

Nicola Besley Data Protection Policy (DPP) – May 09 2022

<i>Version control</i>	
Document reference and version number	PTUK Registrants Model DPP Framework 2017 V2
Purpose	Model framework for preparing an Operational Data Protection Policy for PTUK registrants and/or their employers.
Status	Finalised
Start date	May 09 th 2022
Date of next review	November 2019-Complete-no changes November 2020-Complete-location and status change November 2012
Approved by	Nicola Besley
Readership	Future employers
Author(s)	Nicola Besley

Ownership	Nicola Besley
-----------	---------------

Contents

1.	Introduction.....	7
1.1	Applicability	7
1.2	Legislative basis.....	8
2.	Conforming to the Data Protection Act.....	9
2.1	Principles.....	9
2.2	Personal data definition	9
2.3	Data Controllers and Data Processors	9
2.4	The Domain of data protection.....	10
2.5	Data Subjects	10
2.6	Informed Consent.....	11
2.7	Data Classes.....	11
2.7.1	Summary of Data Catalogue.....	11
2.8	Recipients.....	12
2.8.1	Recipient groups.....	12
2.8.2	Data release protocols.....	12
2.9	Purposes.....	13
2.9.1	Registrants' Data.....	13
2.9.2	Sharing of registrants' data.....	14
2.9.3	Client Data.....	14
2.9.4	Sharing of registrants' client data.....	15
2.9.5	Other data subjects.....	15
2.10	Sensitive Data.....	16
2.11	Security.....	16
2.12	Emergency situations.....	17
2.12.1	The context.....	17
2.12.2	Principles of data sharing in an emergency	17
2.13	Good practice.....	18
2.13.1	Human responsibilities.....	18
2.13.2	IT security.....	19
2.13.3	Training.....	19
2.14	Subject Access Requests (SARs)	19
2.14.1	SAR Processing Stages	19
3.	Privacy by design	22
3.1	Rationale.....	22
3.2	Situation appraisal	22
3.3	Privacy by design approach.....	26
3.4	PIA Overall results and conclusions	26
3.4.1	Need for a dynamic form	26

3.4.2	Main considerations	26
3.4.2	The Information Flows	27
3.4.3	Main risks to privacy and solutions	27
4.	Anonymisation of data	29
4.1	Introduction.....	29
4.2	Basic principles.....	29
4.4	Risks and mitigation.....	30
4.5	Managing Data Protection Risk.....	30
4.6	Anonymisation and the law	31
4.7	User, processor, controller – roles in the anonymisation process	31
4.8	De-identification and anonymisation	32
4.9	Types of anonymisation	32
4.10	Is anonymisation always possible?	33
4.11	What ‘other’ information is out there?	33
4.12	Ensuring the effectiveness of anonymisation	33
4.13	Freedom of information and personal data	34
4.14	Anonymising qualitative data	34
4.16	Anonymisation techniques low risk.....	34
4.16.1	Aggregation	35
4.16.2	Derived data items and banding	35
4.17	High risk techniques	35
4.18	Pseudonymisation	35
5.	Consent.....	36
5.1	Key points.....	36
5.2	Mental Capacity and Consent	36
5.2.1	Children.....	36
5.2.2	Gilllick and Fraser guidelines.....	36
5.2.3	Adults	37
5.2.4	Mental Capacity Act.....	37
5.2.5	Safeguarding Children and Adults.....	38
5.3	Data Items where consent is required.....	38
5.4	Withdrawal of consent.....	38
5.5	Consent isn’t always required.....	39
5.5.1	Sharing criteria	39
5.5.2	Disclosure myths	39
5.6	Personal data and spatial information.....	40
5.6	Reducing risks to privacy when publishing spatial information	41
5.7	Consent as a layered process	41
6.	Disclosure.....	44
6.1	Key points.....	44
6.2	The use case.....	44
6.3	Different types of anonymised data, different risks	44

6.4	Limited access safeguards.....	45
6.5	Meeting ethical obligations through governance	45
6.5.1	Governance and human resources.....	45
6.5.2	Governance and internal structures	46
6.5.3	Good practice	46
6.5.4	Governance requirements	46
6.6	Deliberate attacks and the data intruder	48
6.7.	Intruder scenarios.....	49
6.8	Prior knowledge and re-identification.....	50
6.9	Types of attack and defences	51
6.9.1	PTUK’s main defence	51
6.9.2	Inference attacks.....	52
6.9.3	Differencing attacks.....	52
6.9.4	Complex attacks	53
6.10	Types of formal disclosure risk assessment.....	53
6.11	Data sharing procedures	53
6.11.1	Data Sharing Agreements	53
6.11.2	Data situations.....	55
6.12	Legal responsibilities in data sharing.....	56
6.12.1	Data status: are my data personal?.....	56
6.12.2	The Single controller model.....	57
6.13	Identifying our stakeholders and methods of communication.....	58
6.14	Incident and breach management.....	58
6.14.1	Current situation	58
6.14.3	Definitions	59
6.14.4	Questions arising from a breach	59
6.14.5	Investigating a suspected breach.....	59
6.14.6	Communicating a breach.....	60
7	The Data Protection Act research exemption	61
7.1	What does the DPA say?	61
7.2	What is ‘research’?	62
7.3	What sort of data is section 33 relevant to?	62
7.4	Section 33 safeguards.....	62
7.5	Incompatibility, retention and subject access	63
7.6	The disclosure of research data	63
Annex 1	– PTUK model consent procedures	65
A1.1	Model Consent Form.....	65
A1.2	Explanatory Notes to be used by the therapist.....	66
Annex 2	– Exemptions to Subject Access Requests	69
A2.1	Introduction.....	69
A2.2	Confidential references	69

A2.3	Publicly available information	70
A2.4	Crime and taxation.....	70
A2.5	Management information.....	71
A2.6	Negotiations with the requester	71
A2.7	Regulatory activity	72
A2.8	Legal advice and proceedings	72
A2.9	Social work records	73
A2.10	Health records.....	73
A2.11	Information held about pupils by schools.....	73
A2.12	SAR exemptions good practice	74
A2.12.1	Withholding or redacting information	74
A2.12.2	Ensuring consistency.....	75
Annex 3	Anonymisation of data.....	76
A3.1	Introduction.....	76
A3.2	Basic principles.....	76
A3.4	Risks and mitigation.....	77
A3.5	Decision framework.....	77
A3.6	Anonymisation and the law	79
A3.7	User, processor, controller – roles in the anonymisation process	80
A3.8	De-identification and anonymisation	80
A3.9	Types of anonymisation	81
A3.10	Is anonymisation always possible?	81
A3.11	What ‘other’ information is out there?	82
A3.12	Ensuring the effectiveness of anonymisation	82
A3.13	Freedom of information and personal data	82
A3.14	Anonymising qualitative data	83
A3.16	Anonymisation techniques low risk.....	83
A3.16.1	Aggregation.....	83
A3.16.2	Derived data items and banding.....	85
A3.17	High risk techniques	85
A3.17.1	Data masking	85
A3.18	Pseudonymisation	85
Annex 4	Cookies - DPP requirements.....	87
A4.1	What are cookies?.....	87
A4.2	Requirements of the legislation.....	88
A4.3	Compliance with the legislation.....	88
A4.4	Types of cookies.....	89
A4.5	PTUK Model Statement.....	90
A4.6	PTUK web site cookie list used.....	90
A4.7	PTUK web site cookie explanations.....	91

1. Introduction

1.1 Applicability

This Data Protection Policy (DPP) applies to Nicola Besley, working therapeutically with children and young persons as a private practitioner/employee. It has been based upon the Play Therapy UK (PTUK) Data Protection Policy (DPP) – August 2016 reference document, which has been positively reviewed by an Information Commissioners Office (ICO) Lead Auditor. The reference document, which is some 130 pages long contains the reasoning for the main points of this policy. Some of the information in the reference document is commercially confidential. Full copies of the PTUK reference document are available to regulatory and statutory organisations upon request. Extracts covering specific enquiries may be obtained from the Registrar of PTUK.

One of the main recipients of our therapist's data is PTUK, so this document also contains information about PTUK's DPP and the methods used to implement it, to show that the data I release to them is in safe hands. This policy also acts as a data sharing agreement with PTUK.

Nicola Besley regards the lawful and correct recording, processing and dissemination of personal information as important to the achievement of my objectives. I therefore strive to ensure that I treat personal information lawfully and correctly.

Nicola Besley's context is more complex than some other organisations. I work mainly with children, who are especially vulnerable to any disclosure of personal information, and their proxies. I am required to supply data for the protection of the public. This is used by PTUK and Clinical Supervisors for revalidation, audit and quality assurance processes. It may also be used for research purposes under strictly controlled conditions.

The policy (DPP) described in this document specifies how data is collected, handled and stored to meet my data protection standards and to comply with the law.

This DPP provides guidance to ensure that Nicola Besley

- Complies with data protection law and follows good practice.
- Protects the rights of their clients and the public.
- Is open about how it stores, processes and uses data.
- Protects against the risk of a data breach.

Our Data Environment includes:

Organisations	Role	Data Protection Policy
Anna Lidzey	Art Therapist Therapist and Clinical Supervisor to Nicola Besley, Play therapist	Anna Lidzey DPP
Private practice/future employers	Play therapist	Nicola Besley DPP
Play Therapy UK	Professional organisation managing the Accredited Register (AR) of Play and Creative Arts Therapists. Data needed for quality assurance, audit and national service evaluation.	Play Therapy UK DPP

APAC	The PTUK accredited training provider of courses for registrants. Data required for student/trainee assessment.	APAC DPP
------	---	----------

1.2 Legislative basis

There are a variety legislative sources that relate to the collection and sharing of personal data that are relevant to the play therapy profession – not just the Data Protection Act 1998 (DPA) – but also the likely revisions required to meet the EU General Data Protection Regulation.

This DPP takes account of a number of legislative references to ensure that the policy balances the privacy rights of individuals with the public interest:

- Human Rights Act 1998
- Freedom of Information Act 2000 (FOIA)
- the Children Act 2004
- Environmental Information Regulations 2004
- Local Government Act 2000
- The Crime and Disorder Act 1998
- The Access to Medical Reports Act 1988
- The Health and Social Care Act 2001
- The Public Health (Control of Diseases) Act 1984
- Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011. (PECED).
- Mental Capacity Act 2005
- Civil Contingencies Act 2004.

The relevance of these is explained in the PTUK reference document.

Other relevant non legislative sources that have been consulted are: the Data Science Ethical Framework, the UKAN Anonymisation Decision-Making Framework and the guidance provided by the ICO upon Privacy by design, Privacy Impact Analysis and anonymization of data.

2. Conforming to the Data Protection Act

2.1 Principles

Nicola Besley endorses and is committed to adhering to the eight data protection principles set out in the Data Protection Act 1998.

- 1 Process personal data fairly and lawfully and, in particular, not process data unless these principles and the rules set out here are followed.
- 2 Obtain personal data only for specified and lawful purposes, and not process data in any manner incompatible with that purpose or those purposes.
- 3 Obtain personal data that is adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- 4 Keep personal data accurate and up to date.
- 5 Not keep personal data for longer than is necessary for their legitimate purposes.
- 6 Process personal data in accordance with the rights of data subjects under the Data Protection Act.
- 7 Take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- 8 Not transfer personal data to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2.2 Personal data definition

The Data Protection Act 1998 (DPA) is concerned with 'personal data'. It says that 'personal data' means: *Data which relate to a living individual who can be identified — (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.*

Personal data has to be about a living person, meaning that the DPA does not apply to mortality or other records about the deceased, although such data could still be protected by confidentiality or other legal rules. PTUK mandates that registrants' client data has to be kept for 100 years or for the lifetime of the client, whichever is the earliest.

2.3 Data Controllers and Data Processors

The DPA defines a data controller as:

... a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

There are two conditions in this definition:

1. That a data controller determines the purposes and manner in which the data are processed.
2. That the data are personal data.

The Data Controller is Nicola Besley, Trainee Therapeutic Play Practitioner. In contrast to a data controller, a data processor does no more than process personal data in the way(s) decided by the data controller. Their processing activities may include for example storing the personal data, providing security, transferring them across the organisation or to another and anonymising them. The Data Processor in this case is the same person as the Data Controller, Nicola Besley.

2.4 The Domain of data protection

The Data Protection Act 1998 (the Act) aims to protect individual's fundamental rights and freedoms, notably privacy rights, in respect of personal data processing balancing this right with public interest needs.

The Act applies to paper and electronic records, including still and moving images, however stored and digital storage systems containing personal data. This is data which relates to individuals who can be identified from the data.

Data protection operates by giving individuals the right to gain access to their personal data, by making a subject access request in which they are entitled to:

- a description of their personal data
- the purposes for which they are being processed
- details of whom they are or may be disclosed to

There are circumstances where the law allows Nicola Besley to disclose data without the data subject's consent; these are:

1. Carrying out a legal duty as authorised by an appropriate legal officer
2. The Data Subject has already made the information public
3. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
4. An emergency situation

All organisations must notify the Information Commissioner of the processing of personal data that is included in a public register. ICO registration number: CSN1642296-ZA327946

2.5 Data Subjects

Data Subjects are defined as being individuals about whom information is held.

- Parents/carers and their children and young persons who are existing, potential and past clients for therapy
- Clinical supervisors
- Complainants, correspondents, enquirers
- Other professionals
- Staff at past present and future places of work

2.6 Informed Consent

Informed consent is when a Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data and then gives their consent.

Nicola Besley will ensure that data is collected within the limits defined in this policy. This applies to data that is collected in person, by completing a form or by digital methods.

When collecting data, I will ensure that the Data Subject:

- clearly understands why the information is needed
- understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
- as far as reasonably possible, grants explicit consent, either written or verbal for data to be processed is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- has received sufficient information on why their data is needed and how it will be used

The PTUK model consent form and explanatory instructions, approved by an ICO Lead Auditor, and which has also been awarded the Plain English Campaign Crystal Mark is mandated for use. Each consent approval and date must be recorded.

2.7 Data Classes

Data classes are the types of data which are being or which are to be processed. The list of data classes used by PTUK's registrants has been substantially reviewed by means of a Privacy Impact Analysis (PIA). This is recorded in an extensive Data Catalogue. *This makes clear the data items which do not fall within the Data Protection Act either because they are not personal or are anonymised/pseudoanonymised and/or their use is for research purposes.*

2.7.1 Summary of Data Catalogue

Table/Source	Fall within the DPA	Storage method
Parent/carer and referrer data	Y	Fortuna
Client activities during sessions	Y	Fortuna
Client attributes	Y	Fortuna
Data from surveys undertaken by therapists	Y	Fortuna
Log of clinical supervision sessions	Y	Fortuna
Organisations' objectives related to play therapy	N	Word processed documents
Questions used in registrants' surveys	N	Fortuna
Therapist's changes of clinical supervisors	Y	Fortuna
SDQ data from parents' observations	Y	Fortuna
SDQ data observed by referrers	Y	Fortuna
Staff matters	Y	Word processed documents
Answers to SEPACTO surveys	N	Fortuna
Cookies	Y	Word processed documents

Emails	Y	Hosted Outlook system
--------	---	-----------------------

2.8 Recipients

2.8.1 Recipient groups

Recipients are individuals or Organisations to whom the data controller intends or may wish to disclose data. This list does not include any person where a data controller may be required by law to disclose in any particular case, for example if required by the police under a warrant.

This list should not be read as a list of those to whom data **will** be disclosed. I am required to make clear all of the possible categories of ‘recipient’ to which we **might** need or wish to disclose data – either in pursuit of their regulatory and public protection functions or in relation to permissions sought from and granted by a data subject or an organisation.

A set of data sharing standards has evolved from the PIA identifying 15 groups to which data may be disclosed: ([29] edit the table as required]

Group	Purposes
1. Data subjects themselves: clients, parent/carers	Requests by parents or those legally responsible as well as the subject.
2. Current, past or future referrers	For purposes that fall within the Act including joined up care, quality assurance and research reports.
3. Associated service delivery channels including healthcare, education, social services and welfare staff, advisors or practitioners	
4. Academic partners including education, training and accrediting establishments and examining bodies	
5. Contractors, suppliers, providers of goods and services	For purposes that fall within the Act including joined up care, and quality assurance reports.
6. Persons making an enquiry or complaint	Requires a Court directive or warrant or in case of an emergency.
7. Child protection services	
8. Civil and criminal Courts	For purposes that fall within the Act including joined up care, and quality assurance reports.
9. Police forces	
10. Private investigators	
11. Local government	Subject to anonymization , aggregation and pseudonymisation
12. Central government	
13. Voluntary and charitable organisations	
14. Ombudsmen	
15. The media	

2.8.2 Data release protocols

A set of protocols, when required, for the release of data to the above groups has also been developed.

Protocol	Description
Purpose limitation	Purpose limitation, ie the data can only be used by the recipient for an agreed purpose or set of purposes;

Training of recipients' staff	Training of recipients' staff with access to data, especially on security and data anonymisation principles;
Personnel background checks	Personnel background checks for those getting access to data;
Controls over the data environment	Controls over the ability to bring other data into the environment, allowing the risk of re-identification by linkage or association to be managed;
Disclosure restrictions	Restriction on the disclosure of the data;
Re-identification measures	Prohibition on any attempt at re-identification and measures for the destruction of any accidentally re-identified personal data;
Security arrangements	Arrangements for technical and organisational security, eg staff confidentiality agreements;
Encryption	Encryption and key management to restrict access to data;
Copy limitation	Limiting the copying of, or the number of copies of the data;
Destruction	Arrangements for the destruction or return of the data on completion of the project;
Penalties	Penalties, such as contractual ones that can be imposed on the recipients if they breach the conditions placed on them.

These protocols are applied selectively to requests from the groups.

2.9 Purposes

Nicola Besley holds a wide range of data types relating to diverse data subjects. At various times the data held in respect of these subjects may be used in relation to some or all of the following purposes, not all of which fall within the Act:

2.9.1 Registrants' Data

PTUK/PTI will use personal information provided by you for the purpose of registration, or gathered for the following purposes:

1. To decide eligibility for entry to the PTUK Accredited Register
2. To enable the general public to search the Register to check your registration status
3. To administer, update and maintain the Register
4. To process and respond to requests, enquiries and complaints received from you or about you
5. To process and respond to requests, enquiries and complaints received about your fitness to practise
6. To provide services requested by you
7. To communicate with you about PTUK/PTI services, events and news
8. To analyse trends and profiles and compile statistics
9. For audit and revalidation purposes
10. To carry out stakeholder satisfaction and other research related to the efficacy, effectiveness and efficiency of play therapy and related interventions
11. To prevent or detect fraud
12. To enable third parties to carry out any of the above on our behalf

We will hold personal information on our systems for as long as is necessary for the purposes set out above and we will remove it when the purposes have been met.

PTUK will make a register entry available to any enquirer as part of the published register. The public can inspect the following information on www.playtherapyregister.org.uk

- Registrant's full name
- Registrant's main registration grades
- Registrant's approximate work location
- Registrant's email address
- Registrant's number
- Any information about the services that provided that have been given to PTUK
- Compliance with PTUK's requirements for registration
- Description of any research undertaken
- The outcomes of any complaints upheld and any sanctions imposed on a registrant as a result of PTUK's disciplinary procedures

The registrant's home address, date of birth and other data are not available to the public unless given to us specifically for that purpose by you.

2.9.2 Sharing of registrants' data

PTUK may share information in the following circumstances:

- Where we are required to do so by law
- When it is in the public interest to do so
- When a Notice of Hearing has been issued to you
- When a data subject has given consent for us to do so

PTUK may share your personal data with:

- Other professional associations
- other Accredited Registers
- statutory health and social care regulators
- academic partners of our accredited training providers
- Disclosure Scotland
- Disclosure and Barring Schemes

2.9.3 Client Data

Nicola Besley and PTUK may use personal information gathered by therapists as originally provided by parents, legal guardians and referrers for the purpose of play therapy interventions, for the following purposes:

1. To assess clients suitability for play therapy or other interventions
2. To record and process data arising from client assessment, meetings and therapeutic sessions for clinical supervision and management reporting
3. To record and process data, suitably anonymised, arising from client assessment, meetings and therapeutic sessions for annual revalidation of registrants by PTUK
4. To record, process and disseminate data, suitably anonymised, arising from client assessment, meetings and therapeutic sessions related to the efficacy, effectiveness and efficiency of play therapy and related interventions and for service evaluation
5. To process and respond to requests, enquiries and complaints received from clients and those responsible for them
6. To process and respond to requests, enquiries and complaints received about my fitness to practise
7. To provide services requested by stakeholders

8. To communicate with stakeholders about the services our registrants offer
9. To analyse trends, service performance and compile statistics
10. For audit purposes
11. To prevent or detect fraud
12. To enable third parties to carry out any of the above on our behalf

Nicola Besley and PTUK will hold personal information in mainly digital but also hard copy form for as long as is necessary for the purposes set out above and we will remove it when the purposes have been met.

2.9.4 Sharing of registrants' client data

Nicola Besley and PTUK may share client information data in the following circumstances:

- Where we are required to do so by law
- When it is in the public interest to do so
- When a Notice of Hearing has been issued
- When the parent or person legally responsible for the child (or a young person/adult client) has given consent for us to do so

2.9.5 Other data subjects

Accounting and auditing

The provision of accounting and related services data for management and auditing purposes.

Administration of complaints processes

The administration of complaint and grievance processes of all kinds, including professional disciplinary processes, and complaints against officers, committees or other subsidiary bodies.

Administration of justice

Data subpoenaed by courts of law or tribunals and for the discharge of court business.

Administration of client records

The administration of client records.

Advertising marketing and public relations for others

We do not allow personal data to be used by external organisations or individuals for these purposes. Only aggregated data, where individuals cannot be identified, is released or for case studies where the client cannot be identified.

Clinical governance and related quality assurance activities

The use of data to monitor safe and effective practice, the production of guidelines, standards of attainment and other advice to improve the quality of care.

Clinical Supervisors

Contact details of clinical supervisors may be listed with their permission

Education and training

The provision of clinical, education, training, accreditation and reaccreditation, supervision and/or research data. Only where individuals cannot be identified, is released or in case studies where the client cannot be identified outside our organisation.

Realising the objectives of Nicola Besley

The provision of services in order to realise my objectives. Only anonymised and aggregated data, where individuals cannot be identified, is released or case studies where the client cannot be identified.

Research

Research in any field, including market, health, lifestyle, scientific or technical research. Only anonymised and aggregated data, where individuals cannot be identified, is released or case studies where the client cannot be identified.

2.10 Sensitive Data

Any data that is identifiable to any client is considered sensitive data that is subject to protection. Each data subject and/or parent/carer has the right to inspect and receive a printout of all sensitive data pertaining to him or her. I will notify any client/parent/carer when I acquire and store any sensitive data from a source other than themselves. The data subjects have the right to petition that any sensitive information held by me be removed for inaccuracy or without a lawful purpose.

Sensitive data includes:

Racial or ethnic origin	Anonymised
Political opinions	Must not be collected
Children's place of residence	Anonymised if released outside our organisation.
Religious or similar beliefs	Must not be collected
Trade union membership	Must not be collected
Physical or mental health including treatment activities, medication and outcome data	Client identity is anonymised
Sexual behaviour	Client identity is anonymised
Criminal record	Must not be collected
Criminal proceedings relating to a data subject's offences	Must not be collected
Complaint proceedings	Collected

Where data is anonymised to suitable standards, such as PTUK's it is not subject to the DPA.

2.11 Security

Nicola Besley operates in a field in which confidentiality and record security is of paramount importance. Our offices and play room are operated on the basis that all material entering the office be regarded as confidential unless otherwise defined. Clear guidelines are laid down for staff with respect to processing and provision of data to data recipients.

In addition, I will ensure that:

1. I have a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection;
2. everyone processing personal information understands that they are contractually responsible for following good data protection practice;
3. everyone processing personal information is appropriately trained to do so;
4. everyone processing personal information is appropriately supervised;

5. anybody wanting to make enquiries about handling personal information knows what to do;
6. I deal promptly and courteously with any enquiries about handling personal information;
7. I describe clearly how we handle personal information;
8. I will regularly review and audit the ways we hold, manage and use personal information;
9. I regularly assess and evaluate our methods and performance in relation to handling personal information;
10. all staff, partners and contractors are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them;
11. I access training when appropriate to support in the role and responsibilities.

2.12 Emergency situations

2.12.1 The context

In the event of the need to respond to an emergency involving Nicola Besley, it is recognised that sensitive information (including personal data) can be shared to respond to the emergency, where explicit consent has not been given, and where the emergency circumstances are incompatible with the initial purposes for which the information (including personal data) was originally collected. Eg bad accident, sudden life threatening illness, disclosure of abuse, severe neglect, dangerous environments or situations, grooming.

Whilst the Data Protection Act 1998 places duties on organisations and individuals to process personal information fairly and lawfully, it is not a barrier to sharing information where the failure to do so would result in a child or vulnerable adult being placed at risk of harm. Similarly, human rights concerns, such as respecting the right to a private and family life would not prevent sharing where there are real safeguarding concerns.

As is the case for sharing personal data about children to prevent or detect a serious crime, it may be entirely proportionate for emergency responders to share personal data to save life or prevent the possibility of serious harm. The absence of agreements should not prevent Nicola Besley from sharing information when responding to an actual emergency.

My starting point is to consider *the risks and the potential harm that may arise if we do not share information*.

2.12.2 Principles of data sharing in an emergency

Although different areas of law apply to data sharing – specifically the Data Protection Act 1998, the European Convention of Human Rights (ECHR) Article 8 and the common law of confidentiality – it is important to recognise that there is overlap between them. The particular rules of the various pieces of legislation cannot be ignored. When considering the issues and to help get to the right decision in an emergency it is acceptable for responders to have in mind some fairly broad-brush and straightforward questions:

- is it unfair to the individual to disclose their information?
- what expectations would they have in the emergency at hand?
- am I acting for their benefit and is it in the public interest to share this information?

Principles:

1. Data protection legislation does not prohibit the collection and sharing of personal data – it provides a framework where personal data can be used with confidence that individuals' privacy rights are respected.

2. Emergency responders' starting point should be to consider the risks and the potential harm that may arise if they do not share information.
3. Emergency responders should balance the potential damage to the individual (and where appropriate the public interest of keeping the information confidential) against the public interest in sharing the information.
4. In emergencies, the public interest consideration will generally be more significant than during day-to-day situations
5. Always check whether the objective can still be achieved by passing less personal data.
6. Therapists should be robust in asserting their requirements to share personal data lawfully in emergency planning, response and recovery situations.
7. The consent of the data subject is not always a necessary pre-condition to lawful data sharing.
8. Therapists should seek advice when in doubt – though prepare on the basis that they will need to make a decision without formal advice during an emergency.

2.13 Good practice

2.13.1 Human responsibilities

- Paper notes must not be misplaced on or off site, for example in personal belongings, left in playrooms, classrooms or meeting rooms.
- Bagged confidential paper waste must not be left unattended outside a building.
- Paper records must be kept in locked cabinets, carried securely and not left in public areas.
- Paper records must not be left visible for unauthorised people to see, for example on unattended receptionist desks, on public transport and in places where staff are working between appointments.
- Take great care that emails are not sent to the wrong people, including replies to circulation lists
- Do not lend keys, entry codes or smart cards (programmed devices which give data access)
- Keys and smart cards must be returned withdrawn when staff leave the organisation. Access codes must be changed
- Passwords must comprise of a mixture of characters, numbers and punctuation marks. They should be changed every three months. They must not be written on sticky notes above computer screens or in other open access places
- Coded door locks must have passcodes changed at least every eight weeks
- Doors to secure areas must not be wedged open, or pass codes written above door locks.
- All lost storage devices and smart cards must be reported and appropriate action taken
- Only encrypted devices must be used for confidential data.
- Unfiltered browsing that potentially allows malware into the system must be prevented
- Passwords must not be shared or re-used as passwords on social media sites
- Nicola Besley must not discuss work responsibilities relating to clients on social media
- Clients' details must not be discussed in public places or with unauthorised personnel.
- Parents/carers should be advised appropriately about how to protect their own data eg copies of reports when discussing it in places where confidentiality cannot be assured.
- Client and therapist files must be stored in locked cabinets in secure areas.

- Computer screens in reception areas must be positioned so that unauthorised people cannot see them.
- Parents' and clients' names or personal details must only be mentioned on the telephone in a private environment
- Use secure envelopes for moving client documents

2.13.2 IT security

PTUK strongly recommends the use of technology for recording and storing client information to move away from paper-based records. It solves many data security issues but, if implemented poorly increases the risk of more serious, large scale data losses. I am using the PTUK Fortuna2017 software to improve the handling of sensitive data but recognise that I will always be reliant upon the good practice my use

The play therapy profession has not, so far, been actively involved in sharing data for integrated patient care systems, which is a pity. We and PTUK are monitoring this situation.

Good practice includes:

- Devices containing personal data including, USB drives, CDs, DVDs, external hard drives and storage devices, must not be left unlocked or unattended at any time.
- Password security: Never use a real name, especially someone close to you or your pet's name. Other "easily-guessed" passwords should also be avoided – your phone number, your favourite song and other "real words" that can be found in a dictionary. Avoid using consecutive or adjacent keyboard letters and number combinations (qwerty, abcde, 12345, 24680). Password cracking algorithms will crack these very quickly. Try to use a mix of upper and lower case letters, numbers and whatever permitted symbols you can to make a complicated string.
- Nicola Besley's logons and passwords should be kept secure at all times. There is no need to share passwords. If there is a need to share data with colleagues, it should be stored in designated shared areas.
- No software must be loaded on to any PC without the prior knowledge of the Nicola Besley who will advise whether or not this is suitable.
- Networked devices are not to be used for unfiltered internet browsing – there's a risk of allowing malware to penetrate the system
- Therapists and staff within the placement environment must be aware of and not respond to links in external emails from untrusted sources; potential spam or phishing attempts; and inadvertently introducing viruses to the network.

2.13.3 Training

Training of our staff will be based on the ICO Training checklist for small and medium sized organisations.

2.14 Subject Access Requests (SARs)

The DPA's sixth data protection principle requires us to process personal data in accordance with the rights the Act gives to individuals. Subject access is one of those rights. We have a 10 stage process to respond to a SAR.

2.14.1 SAR Processing Stages

i) Determine the type of subject access request

Any written request by an individual asking for their personal information is a subject access request. Choose to deal with it in one of two ways: as a routine enquiry, or more formally. I can, treat requests that are easily dealt with as routine matters, in the normal course of business; for example:

- How many sessions has my child attended?
- What is your PTUK registration number?

The following are more likely to be treated formally:

- Please send me a copy of my child's progress report.
- I am a prospective employer of Ms X and request a copy of her clinical outcomes and CPD training records, appropriate authority is enclosed.

ii) Check the requester's identity

Ask the requester for any evidence you reasonably need to check the requester's identity

iii) Identifying what they want?

Ask them **promptly**, within 2 working days, for the other information you reasonably need so you that you can find what they want.

iv) Deciding fees

The maximum fee that can be charged for a straightforward request is £10, at present (August 2016). However this charge is being removed under the new GDPR so we will not make a charge unless there is a second request and this needs more than 30 minutes work to complete. Then the fee will be £30. If requests require more than 30 minutes work, they must be referred to Nicola Besley before acknowledging them.

The 40 calendar days in which we must respond starts when we receive the fee and all the the information that we need to answer the request has also been received.

v) Incomplete information

Do I have all the information that the requester wants? If not tell the requester within two working days.

vi) Currency of information

Will the information be changed between receiving the request and sending the response? I can still make routine amendments and deletions to personal information after receiving a request. However I must not make changes to records as a result of receiving the request, even if the information is inaccurate or embarrassing.

vii) Other people

I do not have to supply the information unless the other people mentioned have given their consent for the disclosure, or it is reasonable to supply the information without their consent. If you decide not to disclose the other people's information, you should still disclose as much information as possible by redacting the references to them.

viii) Obligation to supply information

If all the information that the requester wants is exempt from subject access, then you can reply that you do not hold any of their personal data that you are required to reveal. There are some circumstances when you are not obliged to supply certain information. See Annex 2 for guidance on the exemptions.

ix) Complex terms or codes

Any complex terms or codes must be explained so that the information can be understood.

x) Preparing the response

A copy of the information must be provided in a permanent form unless the individual agrees otherwise, or doing so would be impossible or involve disproportionate effort.

3. Privacy by design

3.1 Rationale

PTUK carried out a review, November 2015 to January 2016 in order to balance the needs for the protection of personal privacy with the public interest and to improve PTUK’s DP standards and those of their registrants. This had been instigated by a Professional Standards Authority seminar on the subject and in addition because of the reasons that some Registrants had given for being unable to supply clinical governance data for revalidation purposes due to their employers’ DP policies.

Having identified the areas for revision PTUK carried out a privacy impact assessment (PIA) according to the guidelines and template issued by the Information Commissioner’s Office (ICO). Particular attention was paid to the ICO’s Anonymisation: managing data protection risk code of practice.

In March 2016 PTUK became aware of the probable changes required by the EU General Data Protection Regulation, which in most experts’ views would not be affected by Brexit. It was decided that another review needed to be made. The reference document version 4 of the PTUK Data Protection Policy - was the outcome. It included PTUK’s registrants’ data environment as well as PTUK’s.

3.2 Situation appraisal

This appraisal is based on the ICO’s principles, reviewed against registrants’ use as well as PTUKs needs. PTUK needs are included in this DPP because they are a significant recipient of registrants’ data.

ICO principles and questions	PTUK	Registrants
Principle 1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless: at least one of the conditions in Schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.		
Have you identified the purpose of the project/policy?	Update of PTUK’s existing DPP	A model DPP for registrants
How will individuals be told about the use of their personal data?	Statements for Registrants to use with parent/carers of clients and referrers. Application forms. Publication of an abridged version of PTUK’s DPP V4_0 on www.playtherapy.org.uk	Parental consent forms and interviews explaining the use of the data
Do you need to amend your privacy	Are being revised to balance privacy with public	

notices?	interest	
Have you established which conditions for processing apply?	Yes – see Data Catalogue and PIA	Yes – see Data Catalogue and PIA
If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?	Depends upon the data item. In general digitally from registrants’ revalidation applications Not collected if consent is withheld Data deleted if reasonable reason given for withdrawal taking into account public interest	Depends upon the data item. Either direct digital input by the registrant or data entered from hard copy forms based on PTUK’s model consent form Not collected if consent is withheld Data deleted if reasonable reason given for withdrawal taking into account public interest
If your organisation is subject to the Human Rights Act, you also need to consider:	No	Maybe
Will your actions interfere with the right to privacy under Article 8?		
Have you identified the social need and aims of the project?	Quality assuring, auditing and service evaluation of therapeutic interventions designed to alleviate children’s social, emotional, behaviour and mental health problems. Building and maintaining a clinical evidence base.	
Are your actions a proportionate response to the social need?	Yes, protection of a vulnerable client group and PTUK’s registrants	
Principle 2		
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.		
Does your policy cover all of the purposes for processing personal data?	Yes	Yes
Have potential new purposes been identified as the scope of the project expands?	Yes – a contribution to employers’ and commissioners’ DP policies to cover therapeutic interventions	

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the information you are using of good enough quality for the purposes it is used for?	Yes – PTUK’s new Fortuna2017 Server software will reduce the chance of errors.
--	--

Which personal data could you not use, without compromising the needs of the project?	None identified
---	-----------------

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?	Yes - with protection against changes as deemed necessary.
---	--

How are you ensuring that personal data obtained from individuals or other organisations is accurate?	Our new Fortuna2017 Server software reduces the chance of data recording errors.	Our new Fortuna2017 User software reduces the chance of data recording errors.
---	--	--

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?	Registrant client data – for the life of the client – 100 years from date of collection
---	---

Registrant training course data – 5 years

Are you procuring software which will allow you to delete information in line with your retention periods?	PTUK produces its own software for this purpose	PTUK’s Fortuna Software is used
--	---	---------------------------------

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?	Yes	Yes
--	-----	-----

If your activities involves marketing, have you got a procedure for individuals to opt out of their	Yes	Yes
---	-----	-----

information being used for that purpose?

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

<p>Are systems protected against the security risks you have identified?</p>	<p>Yes, as at present:</p> <p>Database server not connected to a public network;</p> <p>server only accessed through password protected PCs by office staff and CE and Registrar remotely;</p> <p>software protection of server against unauthorised access (defended successfully against over 1000 attempts);</p> <p>backups of data kept in fireproof locked safe;</p> <p>staff sign contracts forbidding use of non- authorised software, hardware and access to external data;</p> <p>access to solely occupied, detached, premises through a single door which is kept locked until visitors are identified;</p> <p>access to premises outside working hours monitored by security and fire alarm system.</p>	<p>Yes – through password protected PCs/laptops and recommended security software.</p>
--	---	--

<p>What training and instructions are necessary to ensure that staff know how to operate a new system securely?</p>	<p>System User guides</p>	<p>System User guides</p>
---	---------------------------	---------------------------

Principle 8

<p>Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.</p>	<p>Personal data is not transferred outside the EU. Data is received from outside the EU.</p>	<p>Therapists may only use cloud services where servers are based in the EEA (European Economic Area or other countries approved by the EEA. The European Commission has now issued its formal decision</p>
---	---	---

that the Privacy Shield provides adequate protection to allow personal data to be transferred to the US. This scheme became operational from 1 August 2016. A US based service must be a signatory to be acceptable.

Will the project require you to transfer data outside of the EU?	In aggregated and anonymised formats only.	No
If you will be making transfers, how will you ensure that the data is adequately protected?	Encrypted and using servers based in the EU	Encrypted and using servers based in the EU

3.3 Privacy by design approach

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. Although this approach is not a requirement of the Data Protection Act, it helps organisations to comply with their obligations under the legislation. Its adoption helps to upgrade our DPP to a high standard.

Privacy Impact Assessments (PIAs) are an integral part of taking a privacy by design approach. This policy has been informed by a Privacy Impact Analysis (PIA) undertaken by PTUK.

3.4 PIA Overall results and conclusions

3.4.1 Need for a dynamic form

During the PTUK PIA it immediately became apparent that a DPP, including the data catalogue, has to be dynamic to accommodate frequent changes in the type of data being recorded, for example new psychometric measuring instruments and new types of research analysis and dissemination. Consequently the Master PTUK DPP data catalogue is stored by PTUK in its own database.

3.4.2 Main considerations

The following list shows the main considerations taken into account in devising the PTUK DPP reference document:

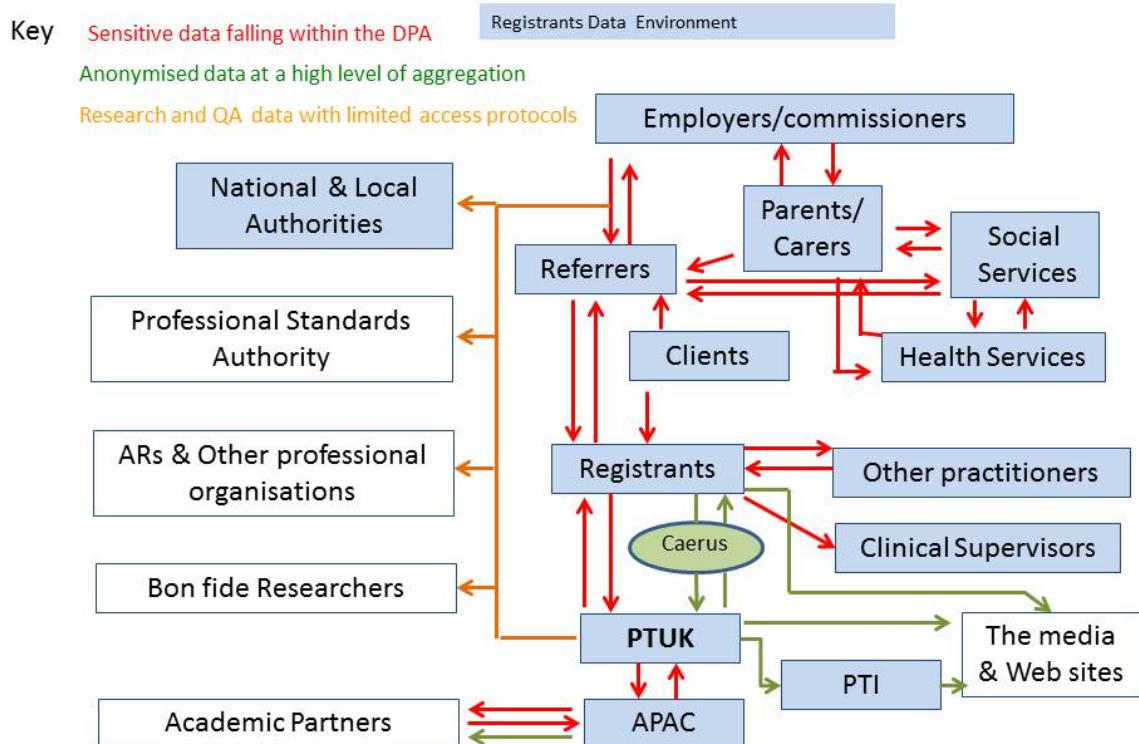
- 1) Balancing the requirements of the DPA, the FOIA and other legislation
- 2) The interchange of data between:
 - Registrants and PTUK
 - Registrants and other parties
- 3) Anonymisation of clients' identities and personal attributes
- 4) Meeting the requirements of PECED ('Cookie Law')
- 5) The protocols required to release data whilst protecting privacy

3.4.2 The Information Flows

The PIA categorises the flows into:

- 1) *Sensitive data falling within the DPA* - the majority of these flows are potentially between registrants and their data environment highlighting the need for sound registrant DPPs
- 2) *Anonymised data at a high level of aggregation* - these flows are mainly between the registrant and PTUK using the Fortuna system. Providing data to the media is also an important area.
- 3) *Quality assurance, audit and service evaluation data with limited access protocols* - these flows are with authorities and individuals concerned with professional matters and research and academic partners (usually universities).

The PTUK & Registrants Data Environment



3.4.3 Main risks to privacy and solutions

The main risk areas relate to individual’s names, contact details and personal attributes. These risks are managed by:

Action	Effect
Adherence to PTUK Ethical principles:	
<ul style="list-style-type: none"> • Fidelity • Autonomy • Beneficence • Non-maleficence • Justice • Self respect 	Guides the decisions and actions of individuals managing data.

Anonymisation of data to de-identify individuals when releasing data outside Nicola Besley's control.

Secure Systems

The use of digital systems is recommended wherever possible with appropriate protection against loss of data and access by unauthorised individuals. Fortuna2017 software colour codes the sensitivity of the data.

Any residual hard copy records must be kept in secure storage.

Guards against identification and re-identification of data subjects

Reduces the chances of unauthorised access and accidental loss or destruction of data over a long period of time.

4. Anonymisation of data

4.1 Introduction

Anonymisation together with the disclosure of data are key issues in our DPP. So often ‘Data protection issues’ have been erroneously used as a reason for not releasing data that is in the public interest. (See also 5.6 concerning the recording and disclosure of spatial/geographic data)

The area of greatest sensitivity is the client clinical data that PTUK collects from registrants. This data has to be provided in an anonymised form. They are almost always shared/released in an aggregated form by PTUK so that the risk of re-identification is minimal.

PTUK has taken the PSA’s advice to refer to Health Research Authority (HRA)’s Differentiating Audit, Service Evaluation and Research document. 3. It has been concluded that PTUK is carrying out both audit and service evaluation so these activities are no longer defined as ‘research’ in this context. PTUK does not undertake original research directly but registrants may do so.

However, there is some contradiction with the broader ICO definition: ‘*Research is a systematic investigation intended to establish facts, acquire new knowledge and reach new conclusions*’. We have resolved this by applying it to the research activities of registrants, such as during the MA stage of their training. This case the ICO definition will be used. This research will normally be fully covered by their University’s review of topic and research proposal, including any need to obtain NHS ethical approval.

4.2 Basic principles

The Information Commissioner has issued its code for anonymization under section 51 of the Data Protection Act ‘. The DPA says good practice includes, but is not limited to, compliance with the requirements of the DPA. This code was also published with Recital 26 and Article 27 of the European Data Protection Directive (95/46/EC) in mind. These provisions **make it clear that the principles of data protection do not apply to anonymised data.**

The DPA does not require anonymisation to be completely risk free – we must be able **to mitigate the risk of identification until it is remote.** If the risk of identification is reasonably likely the information should be regarded as personal data, Clearly, 100% anonymisation is the most desirable position, and in some cases this is possible, but it is not the test the DPA requires.

The term ‘re-identification’ is used to describe the process of turning anonymised data back into personal data through the use of data matching or similar techniques. The ICO’s code’s annexes contain examples of various anonymisation and re-identification techniques and illustrations of how anonymised data can be used for various purposes which PTUK has reviewed to decide which methods should be used.

A distinction has to be drawn between anonymisation techniques used to produce aggregated information, for example, and those – such as pseudonymisation – that produce anonymised data but on an individual-level basis. The latter can present a greater privacy risk, but not necessarily an insurmountable one. There is also a distinction between publication to the world at large and the disclosure on a more limited basis – for example to a particular research establishment with conditions attached. PTUK in the main adopts the latter approach where there is a moderate degree of granularity. In the case of public dissemination, data is aggregated to a safe spatial level, based on a minimum of 250 cases so making identification virtually impossible’ eg ‘77% of boys showed a positive change.’

4.4 Risks and mitigation

PTUK has identified the issues that need to be considered when deciding how to anonymise personal data. The risks considered include:

Risk	Mitigation	
	PTUK	Nicola Besley
<ul style="list-style-type: none"> Information about someone’s private life ending up in the public domain; an anonymised database being ‘cracked’ so that data about a number of individuals is compromised; individuals being caused loss, distress, embarrassment, or anxiety as a result of anonymised data being re-identified; reduced public trust if anonymised data is disclosed unsafely; 	<p>Careful design of the data collection forms and systems design; secure protection measures for digital and hard copy data.</p> <p>PTUK’s data and that received from registrants is kept on a password protected server that is not connected to the Internet. It is in a secured building.</p> <p>Anonymised registrant client ids are used, nor names or addresses.</p> <p>Very little qualitative data is collected by PTUK. It is almost entirely concerned with registrants rather than clients. Some action and learning points issued by clinical supervisors to registrants may relate to specific clients, who cannot be identified by PTUK.</p>	<p>Digital data is stored on a laptop which is password protected.</p> <p>Anonymised registrant client ids are used, not names or addresses of clients, parent/carers, referrers, when data is released outside Nicola Besley</p>
<ul style="list-style-type: none"> legal problems where insufficiently redacted qualitative data is disclosed, for example, under FOIA. 		

4.5 Managing Data Protection Risk

The ICO published its ‘Anonymisation: Managing Data Protection Risk’ code of practice in 2012. Experience provided two main lessons. Firstly, effective anonymisation is possible but it is also possible to do anonymisation ineffectively. Secondly, it isn’t always possible to draw the definitive personal / non-personal data distinction that legal certainty in the field of data protection depends on. As a result our policy also takes into account ‘The Anonymisation Decision-Making Framework’ (ADF) produced by (Mark Elliot, Elaine Mackey Kieron O’Hara and Caroline Tudor published in 2016 by UKAN, University of Manchester. This shows that we have to deploy effective anonymisation techniques and assess re-identification risk *in context*, recognising that there is a wide spectrum of personal identifiability and that different forms of identifier pose different privacy risks.

We have also taken into account the National Data Guardian for Health and Care Review of Data Security, Consent and Opt-Outs - Dame Fiona Caldicott, National Data Guardian June 2016 (Caldicott Review).

The framework recommended by PTUK is underpinned by a relatively new way of thinking about the re-identification problem which posits that we must look at both the data and the data environment to ascertain realistic measures of risk. This is called the data situation approach.

Zero risk is not a realistic possibility if we are to produce useful data: This is fundamental. Anonymisation is about risk management, nothing more and nothing less; accepting that there is a residual risk in all useful data inevitably puts us in the realms of balancing risk and utility. The measures we put in place to manage risk are in our judgement proportional to that risk and its likely impact.

Further details are given in Annex 3.

4.6 Anonymisation and the law

Additional details are given in Annex 3.

Usually, following anonymisation, the original personal data still exist and this means that (except perhaps for the coarsest of aggregate data) the data controller will still be able to identify individuals within the anonymised data (using the original data as a reference) and therefore it would seem that on a literal reading of the definition of personal data the data must still be personal. There are two ways of resolving this paradox:

1. To say that the anonymised data are personal and therefore the question about whether to share or release them depends on whether the DPA provides another get-out (eg whether the share or release constitutes fair processing).
2. To say that the anonymised data are personal for the original data controller but non-personal for other users of the data.

We have adopted the second of these positions as it directly ties the concept of anonymisation to the notion of the context of personal data (in this case, other sources of data that users have access to) and makes a clean separation between the complexities of data protection, such as the (essentially ethical) question of fairness, on the one hand, and the (essentially technical) question of identifiability on the other.

4.7 User, processor, controller – roles in the anonymisation process

Understanding the legal status in respect of particular data is important as it helps us to establish clearly what our responsibilities are *and those of any other stakeholders* during the anonymisation process. It may also be that the design of the process will affect the roles that different agents play.

The DPA defines a data controller as:

... a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

There are two conditions in this definition:

1. That a data controller determines the purposes and manner in which the data are processed.
2. That the data are personal data.

In contrast to a data controller, a data processor does no more than process personal data in the way(s) decided by the data controller. Their processing activities may include for example storing the personal data, providing security, transferring them across the organisation or to another

and indeed anonymising them. The roles of the Data Controller, Data Processor and SIRO (Senior Information Risk Owner) are undertaken in PTUK by the Registrar.

4.8 De-identification and anonymisation

There is a lot of confusion between the two terms *de-identification* and *anonymisation* mostly arising from the fact that the former is usually a necessary but rarely sufficient component of the latter.

De-identification – refers to a process of removing or masking *direct identifiers* in personal data such as a person's name, address, school number or other unique number associated with them. De-identification includes what is called *pseudonymisation*.

Anonymisation – refers to a process of ensuring that the risk of somebody being identified in the data is negligible. This invariably involves doing more than simply de-identifying the data, and often requires that data be further altered or masked in some way in order to prevent statistical linkage.

We can highlight further the difference between anonymisation and de-identification (including pseudonymisation) by considering how *re-identification* might occur:

1. Directly from those data.
2. Indirectly from those data and other information which is in the possession, or is likely to come into the possession, of someone who has access to the data.

The process of de-identification addresses *no more* than the first, i.e. the risk of identification arising directly from data. The process of anonymisation, on the other hand, should address both 1 and 2. Thus the purpose of anonymisation is to make re-identification difficult both directly and indirectly. In de-identification – because one is only removing direct identifiers – the process is unlikely to affect the risk of indirect re-identification from data in combination with other data.

It should be noted that in the description of both processes (i.e. de-identification and anonymisation) the purpose is to make re-identification more *difficult*. Both de-identification and anonymisation are *potentially* reversible; the data environment in which data is shared or released is of critical importance in determining reversibility. In other words, the data environment can either support or constrain reversibility which means that PTUK has had to think very carefully about its environment (and that of our registrants) in which they share or release data. For example, it may be entirely appropriate to release de-identified data in a highly controlled environment such as a secure data lab but not at all appropriate to release them more openly, for example by publishing them in a journal.

4.9 Types of anonymisation

The term 'anonymisation' gets used in a variety of different ways and inevitable communication difficulties arise as a consequence. Elliot et al (2015) have identified four different usages:

1. Formal Anonymisation
2. Guaranteed Anonymisation
3. Statistical Anonymisation
4. Functional Anonymisation - this is PTUK's approach.

4.10 Is anonymisation always possible?

The Information Commissioner recognises that some collections of personal data do not lend themselves well to anonymisation – eg voluminous collections of paper records held in a variety of formats. Although the sensitivity of data will generally decrease with the passage of time, the inappropriate release of records many decades old, eg criminal records, could still have a severely detrimental effect on an individual. That is why the security of data that cannot be anonymised is paramount. It is worth noting that the DPA's section 33 exemption, described later - allows personal data held for research purposes to be retained indefinitely, provided certain conditions are met. PTUK strongly recommends that only digital records are kept by registrants and has developed the Fortuna software to make this feasible.

4.11 What 'other' information is out there?

Determining what other information is 'out there', who it is available to and whether it is likely to be used in a re-identification process can clearly be extremely problematic. The 'other information' needed to perform re-identification could be information available to certain organisations, to certain members of the public or that is available to everyone because it has been published on the internet, for example. Clearly the risk of combining information to produce personal data increases as data linkage techniques and computing power develop, and as more potentially 'match-able' information becomes publicly available.

It is worth stressing that the risk of re-identification through data linkage is essentially unpredictable because it can never be assessed with certainty what data is already available or what data may be released in the future. It is also generally unfeasible to see data return (ie recalling data or removing it from a website) as a safeguard given the difficulty, or impossibility, of securing the deletion or removal of data once it has been published. PTUK's PIA has identified which data may be released outside the PTUK environment and under what conditions. **It is especially important that registrants do not disclose information relating to any client on social media.**

4.12 Ensuring the effectiveness of anonymisation

If the anonymisation of data is ineffective there is the risk of re-identification. PTUK has identified two main issues:

- 1) The risk of the data being obtained by an intruder

We have measures in place and recommendations for therapists to minimise this risk

- 2) The risk of breaking anonymisation by cross referencing data sets

Generally the latter risk scenario is of greater concern for data custodians because of the confidentiality pledges that are often given to those appearing in an anonymised dataset. However, both risk scenarios are relevant and can carry with them different probabilities of re-identification. In either case though it can be difficult, even impossible, to assess risk with certainty. Despite all the uncertainty, re-identification risk can certainly be mitigated by ensuring that only the anonymised data necessary for a particular purpose is released.

PTUK's procedure, which we have adopted, at present relies upon the anonymisation of the client's identity by means of a code. This code can be used in 5 other datasets. PTUK are using different system generated client ID codes in the Fortuna2017 software for each linked dataset to reduce this risk. This protects against re-identification from any lists or reports released or

published. However, lists are only released in response to statutory or legal authorities. Otherwise data is aggregated.

4.13 Freedom of information and personal data

Section 40 of the Freedom of Information Act 2000 (FOIA) introduces a broader concept of risk because its test for deciding whether personal data can be disclosed is whether disclosure to a member of the public would breach the data protection principles. This means that organisations and individual practitioners have to assess whether releasing apparently anonymised data to a member of the public would breach the data protection principles. This is intended to ensure that Data Protection Officers take into account the additional information that a particular member of the public might have that could allow data to be combined to produce information that relates to and identifies a particular individual – and that is therefore personal data.

This risk is managed by restricting the dissemination of anonymised, aggregated data to a limited number of data controllers and through conditions attached to their use.

4.14 Anonymising qualitative data

Much of the anonymised data being created, used and disclosed is derived from clinical and administrative datasets that are essentially statistical in nature. However, the techniques used to anonymise quantitative data are not generally applicable when seeking to anonymise qualitative data, such as the minutes of meetings, case notes, interview transcripts or video footage. Different techniques are needed to do this. We:

- redact individuals' names from documents where permission has not been obtained;
- do not use recordings of audio material;
- change the details in a report that reveal an individual's identity

4.15 Ethics and anonymisation

It is not always immediately obvious why ethical considerations have a role to play in the process of anonymisation. Most readers will understand that the processing of personal data is an ethical issue but once data are anonymised are our ethical obligations not dealt with? This is an understandable confusion which arises in part from a conflation of legal and ethical constraints. Legally, functional anonymisation is sufficient but this might not be true ethically. There two primary reasons why we need to consider ethics beyond the law:

1. Data subjects might not want data about them being re-used in general, by specific third parties or for particular purposes.
2. We are not dealing with zero risk.

There is growing evidence that data subjects are concerned not just about what happens with their personal data but also about the anonymised data derived from their personal data.

There may be many reasons why data subjects object to the reuse of their data. For example I might be unhappy about my data – even anonymised – being reused by a particular type of organisation.

Nicola Besley makes it clear that any data that I hold is not released to any organisation that is not concerned with the emotional well-being of children and young persons and then only for audit, quality assurance or research purposes. Therapists' ethical principles of Fidelity, Autonomy, Beneficence, Non-maleficence and Justice are applied.

4.16 Anonymisation techniques low risk

Covered in detail in Annex 3.

4.16.1 Aggregation

Data is displayed as totals, so no data relating to or identifying any individual is shown. Small numbers in totals are often suppressed through ‘blurring’ or by being omitted altogether.

Recommended by PTUK.

4.16.2 Derived data items and banding

Derived data is a set of values that reflect the character of the source data, but which hide the exact original values. This is usually done by using banding techniques to produce coarser-grained descriptions of values than in the source dataset eg replacing dates of birth by ages or years, addresses by areas of residence or wards, using partial postcodes or rounding exact figures so they appear in a normalised form. Again, this is a relatively low-risk technique because the banding techniques make data-matching more difficult or impossible. The resulting data can be relatively rich because it can facilitate individual-level research but presents relatively low re-identification risk.

Recommended by PTUK.

4.17 High risk techniques

Covered in Annex 3.

4.18 Pseudonymisation

Covered in more details in Annex 3.

Pseudonyms must be used where reference to individual cases is necessary as in academic assignments, published articles, research papers etc. The client’s name must never be used. In disguising it care must be taken not to use the client’s initials. A numeric sequence is preferred. Other attributes that may identify the client such as a combination of geography, age, gender and presenting condition must also be considered carefully.

5. Consent

5.1 Key points

- Consent is generally not needed to legitimise an anonymisation process.
- Even if consent can be obtained it is usually ‘safer’ to use or disclose anonymised data.
- The Information Commissioner’s Office recognises that obtaining consent can be very onerous or even impossible.
- Distinguish registrant data from registrant client data

The Data Protection Act 1998 (DPA) provides various ‘conditions’ or legitimising the processing of personal data, including its anonymisation. Consent is just one condition, and the DPA usually provides alternatives. *The DPA only gives the individual a right to prevent the processing of their personal data where this would be likely to cause unwarranted damage or distress.* In the ICO’s view, it follows therefore that provided there is no likelihood of anonymisation causing unwarranted damage or distress – as will be the case if it is done effectively – then there will be no need to obtain consent as a means of legitimising the processing.

Our policy is that therapists always need to obtain consent from a parent or the person legally responsible for the child for the use of specified data items collected as part of the referral for quality assurance, audit, service evaluation and research purposes. If a registrant cannot obtain consent then their data must not be recorded.

See Annex 1 – PTUK model consent procedures

5.2 Mental Capacity and Consent

Adults and young people ages 16 and 17 are assumed to have capacity to give consent and so a lack of capacity should be clearly evidenced and recorded. Young people under 16 may also have competence depending on their maturity and understanding.

It is important to consider how the personal data was obtained originally by PTUK or a registrant. If, for example, the data was collected as part of a survey and individuals were *told that it would be used for research purposes then clearly there will be no barrier to using the data for that purpose.*

5.2.1 Children

Where the individual to whom the data relates is a child (under the age of 18) and it is determined that the individual has the competency to make decisions regarding the sharing of data he or she has provided in confidence, his or her wishes must be respected. (The ethical principle of autonomy).

Safeguarding issues may arise under the Children Act 2004 in relation to the provision to Children’s Social Care Services and/or the Police of information relating to child abuse and in such cases legal advice should be sought.

In any other cases where the individual does not have the capacity to consent, express consent must be sought from the individual with parental responsibility (parent or guardian).

5.2.2 Gillick and Fraser guidelines

The Gillick competency and Fraser guidelines help us to balance children’s rights and wishes with our responsibility to keep children safe from harm. Gillick competency and Fraser guidelines refer to a legal case which looked specifically at whether doctors should be able to give contraceptive advice or treatment to under 16-year-olds without parental consent. But since then, they have

been more widely used to help assess whether a child has the maturity to make their own decisions and to understand the implications of those decisions.

"...whether or not a child is capable of giving the necessary consent will depend on the child's maturity and understanding and the nature of the consent required. The child must be capable of making a reasonable assessment of the advantages and disadvantages of the treatment proposed, so the consent, if given, can be properly and fairly described as true consent." (Gillick v West Norfolk, 1984)

How is Gillick competency assessed?

Lord Scarman's comments in his judgment of the Gillick case in the House of Lords (Gillick v West Norfolk, 1985) are often referred to as the test of "Gillick competency":

"...it is not enough that she should understand the nature of the advice which is being given: she must also have a sufficient maturity to understand what is involved."

He also commented more generally on parent's versus children's rights:

"parental right yields to the child's right to make his own decisions when he reaches a sufficient understanding and intelligence to be capable of making up his own mind on the matter requiring decision."

Professionals working with children need to consider how to balance children's rights and wishes with their responsibility to keep children safe from harm.

Underage sexual activity should always be seen as a possible indicator of child sexual exploitation. Sexual activity with a child under 13 is a criminal offence and should always result in a child protection referral.

5.2.3 Adults

If it is decided that adults eg parents, lack capacity, in accordance with the Mental Capacity Act 2005 to give informed consent to the sharing of their information, then any decision taken on their behalf must be in their best interests and any previously expressed wishes, or the wishes of anyone who is authorised to act on behalf of the individual.

5.2.4 Mental Capacity Act

A person who lacks capacity at a certain time may be able to make that decision at a later date. Consideration will be given to whether the data needs to be shared now, or could wait until a time when the person is able to consent to the data being shared

The 5 Key Principles¹ in the Mental Capacity Act will be taken into account in coming to a decision about a person's capacity:

1. A person must be assumed to have capacity unless it is established that s/he lacks capacity;
2. A person is not to be treated as unable to make a decision unless all practicable steps to help her/him to do so have been taken without success;
3. A person is not to be treated as unable to make a decision merely because s/he makes an unwise decision;
4. An action taken or decision made, under this Act for or on behalf of a person who lacks capacity must be done, or made, in her/his best interests;

5. Before the action is taken, or the decision is made, regard must be had to whether the purpose for which it is needed can be as effectively achieved in a way that is less restrictive of the person's rights and freedom of action.

Where it is considered that a person does not have capacity, a record will be made of this decision and the steps taken by the registrant to reach a decision about whether data should be shared in their best interests.

The capacity to be able to give consent can be assessed by considering:

- Has the person got the capacity to make this particular decision?
- Have they got the capacity to understand and retain the information relevant to the decision?
- Will they be able to understand the reasonably foreseeable consequences of deciding one way or the other?
- Will they have the capacity to communicate the decision they have come to?

Where professionals request that data supplied by them be kept confidential from the people who use services the outcome of this request and the reasons for taking the decision will be recorded. Decisions of this kind will only be taken on statutory grounds.

The NHS Code of Practice on Confidentiality provides advice and guidance on the legal, ethical and policy conditions affecting the disclosure of confidential patient information. In simple terms, in the absence of a patient's consent, information should only be disclosed where there is a statutory obligation to do so or where the public interest in disclosure is sufficient to override both the duty of confidence owed to an individual and also the public interest in keeping health records confidential. The threshold for disclosure will be a relatively high one. Anonymisation and other procedures need to be taken into account – see section 4.

5.2.5 Safeguarding Children and Adults

A number of principles apply in respect of safeguarding children and adults:

- Safeguarding children and adults is everyone's responsibility
- Abuse and neglect of children and adults is never acceptable
- Sharing data appropriately is crucial to protecting children (even when the child or young person does not agree)
- Failure to share appropriate data places children and adults at greater risk

Where the safety or welfare of a child is in doubt, registrants must co-operate with the statutory agencies which can provide protection (Children's Social Care and Police). A number of public bodies are required by the Children Act 2004 to make arrangements for ensuring that their functions are discharged having regard to the need to safeguard and promote the welfare of children. Failure to share relevant data places a child in danger, and leaves staff vulnerable to both professional misconduct and disciplinary consequences.

5.3 Data Items where consent is required

A set of explanatory notes, produced by PTUK, is provided in Annex 1 to explain the data collected and its uses, if asked for.

5.4 Withdrawal of consent

However, there can be problems in an approach based solely on consent, particularly where this involves the publication of personal data. If an individual can give consent, the individual can withdraw it – and may want to do so because of a change in their personal circumstances, for example. Even if the withdrawal of consent stops us from further processing the personal data,

in reality, it may be impossible to remove the data from the public domain. The withdrawal of consent may have little or no effect. It is therefore ‘safer’ to publish anonymised data than personal data, even where consent could be obtained for the disclosure of personal data itself.

5.5 Consent isn’t always required

5.5.1 Sharing criteria

Myth: You always need the consent of the data subject in order to share their personal data. **Fact:** You do not necessarily need consent of the data subject to share their personal data. In terms of compliance with the Data Protection Act 1998 (and the Human Rights Act 1998), consent of the data subject is not a necessary precondition for lawful data sharing. The Data Protection Act 1998 sets out a number of criteria under Schedule 2 for the legitimate processing of personal data (and sharing, like using, is for the most part just another form of processing) and if any one of the criteria is met, the Data Protection Act 1998 test is satisfied.

Consent is simply one of the criteria. Furthermore, consent in relation to personal data does not need to be explicit – it can be implied. More stringent rules apply to sensitive personal data, when consent does need to be explicit if that criterion is used – criteria other than consent can still be used for sensitive personal data. Even without explicit consent for the sharing of sensitive personal data, it is still possible to share the data legitimately if this is necessary in order to exercise any statutory function (as may well be the case for responders to emergencies) or to protect the vital interests of the individual where, for example, consent cannot be given.

One of the lessons identified in the Government’s report on lessons from the 7 July 2005 terrorist attacks related to the management of personal data by local and regional responders. It was apparent that in some parts of the emergency response, the requirements of the Data Protection Act 1998 were either misinterpreted or over-zealously applied.

5.5.2 Disclosure myths

Myth: Personal data collected by one organisation cannot be disclosed to another organisation unless it is for the same (ie ‘compatible’) or a directly related purpose.

Fact: The issue of ‘compatibility’ arises under the second principle of the Data Protection Act 1998. If personal data is collected by one organisation for a particular purpose, then ‘compatibility’ (ie that the information must be used for the same purpose it was collected for) is not a necessary condition. The test is one of incompatibility – ie is the new purpose incompatible with the original purpose? In an emergency response scenario, it is difficult to foresee circumstances where sharing personal data would be incompatible with the purposes for which they were originally collected.

The Data Protection Act 1998 applies to all organisations – including private sector organisations or individuals – which hold or use personal data. A further myth about the DPA is that the private sector cannot be forced to release personal data. The facts are less clear cut. The Data Protection Act 1998 does not, either, enable emergency responders to force the private sector to disclose information. However, it is possible to obtain an order of the court for the private sector to disclose information (including personal data) if this is necessary for a particular purpose and there is a legal basis. The police also have separate powers to compel organisations, including those in the private sector, to provide information for law enforcement purposes. This means that the Data Protection Act 1998 allows for the disclosure of personal information from a private organisation to the police where the latter need the information for their law enforcement functions (which includes preventing or detecting crime and apprehending and prosecuting offenders). Aside from this and court orders, the Data Protection Act 1998 has exemptions that would *allow* private sector organisations to share data in particular situations, but it cannot *compel* them to.

Though the key law governing data protection is the Data Protection Act 1998, *clear legal power to share data is found in secondary legislation made under the Civil Contingencies Act 2004*. The Civil Contingencies Act 2004 (through the regulations made under it) places a duty on emergency responders, on request, to share information relating to emergency preparedness/civil protection work with other Category 1 and 2 responders. This duty relates to the preparedness, response and recovery stages of an emergency.

Civil Contingencies Act 2004 Clear legal power to share data is found in secondary legislation made under the (paragraphs 3.1–3.3). (In the United Kingdom, secondary legislation (also referred to as delegated legislation) is law made by an executive authority under powers delegated from by an enactment of primary legislation, which grants the executive agency power to implement and administer the requirements of that primary legislation.[2] The power to pass delegated legislation is defined and limited by the primary legislation that delated those powers; if the subordinate authority acts beyond its remit, its acts will be invalid or ultra vires ie invalid)

5.6 Personal data and spatial information

There is no simple rule for handling spatial (geographic) information – such as postcodes, GPS data or map references - under the Data Protection Act 1998 (DPA). In some circumstances this will constitute personal data, eg where information about a place or property is, in effect, also information about the individual associated with it. In other cases it will not be personal data.

It is clear, though, that the more complete a postcode - or the more precise a piece of geographical information - the more possible it becomes to analyse it or combine it with other information, resulting in personal data being disclosed. However, where spatial information is being published for a legitimate purpose, the objective should be to achieve the maximum level of detail that can be balanced with the protection of individuals' privacy. PTUK's PIA has taken this into account. In the UK we have considered, the average characteristics of postcodes:

Full postcode = approx 15 households (although some postcodes only relate to a single property)	Only to be used by registrants for postal communication with those responsible for the child. Not to be supplied to PTUK.
postcode minus the last digit = approximately 120/200 households	
postal sector = 4 outbound digits + 1 inbound gives approx. 2,600 households	Rather cumbersome to systematise so not recommended.
postal district = 4 outbound digits approx 8,600 households	PTUK's recommendation for data exported from our registrants' records.
postal area = 2 outbound digits approx 194,000 households	Regarded as too coarse for useful analysis of data.

(‘Outbound’ is the first part of the postcode, ‘inbound’ the second part; for example with the postcode SV3 5AF, the outbound digits are SV3 and the inbound digits are 5AF.)

With information relating to a particular geographical area, there can be a distinction between a “statistical comfort zone” that eliminates almost all risk of identification, and other forms of information that pose a risk of an individual being identified. Small numbers in small geographical areas present increased risk, but this does not mean that small numbers should always be removed automatically. For example, always removing numbers relating to five or 10 individuals or fewer may be a reasonable rule of thumb for minimising the risk of identification in a proactive disclosure scenario, but in the context of a specific freedom of information request a different approach may be possible, based on an application of the tests in the DPA. Our view is that FOI requests of this nature are unlikely.

5.6 Reducing risks to privacy when publishing spatial information

The following methods have been considered:

- | | |
|---|--|
| 1. Increasing a mapping area to cover more properties or occupants; | May be used – normally several towns or areas that contain 100,000 plus populations. |
| 2. Reducing the frequency or timeliness of publication, so that it covers more events, is harder to identify a recent case, or does not reveal additional data such as time or date of the event. | Never less than a year. |
| 3. Removing the final ‘octet’ on IP addresses to degrade the location data they contain; | PTUK and its registrants have no reason to collect this type of data. |
| 4. Using formats, such as heat maps, that provide an overview without allowing the inference of detailed information about a particular place or person; | As 1 above |
| 5. Avoiding the publication of spatial information on a household level. This could constitute the processing of personal data because it is quite easy to link a property to its occupant or occupants – using the publicly available Electoral Register, for example. | This level must not be used. |

Where there are no risks, or they are minimal, or do not fall within the DPA, geographical information should provide as much information as possible, to enable the public to understand issues such as the support needed for children in their area. This can enable communities to engage with agencies such as schools and social services and bring about enhanced accountability.

5.7 Consent as a layered process

In principle consent is a straightforward idea. We ask the data subjects ‘can I do X with your data?’ and they say yes or no. However, in practice the situation is much more complicated than this. Firstly, consent is layered. Secondly, the notion of consent is interlaced with the notion of awareness. This produces what we refer to as a scale of information autonomy. Consider the following questions:

Factor	PTUK recommended procedure
1. Are the data subjects aware that their data have been collected in the first place?	Yes – parental consent form (Depends upon the parent telling the child)
2. Have the data subjects consented to the collection of their data?	Yes – parental consent form The parent is a proxy for the child.
3. Were the data subjects completely free to give consent to the collection of their data or have they agreed to collection because they want something (a good or service) and are required to hand over some data in order to obtain it?	Yes – parental consent form. If consent is refused the play therapy service is still provided

- | | |
|---|---|
| 4. Are the data subjects aware of the original use of their data? | Yes – audit and quality assurance using clinical supervision |
| 5. Have the data subjects consented to the original use of their data? | Yes – parental consent form |
| 6. Have the data subjects consented in general to the sharing of an anonymised version for of their data? | Yes – parental consent form |
| 7. Are the data subjects aware of the specific organisations that you are sharing their anonymised data with? | Yes – parental interview
(By type of organisation eg university) |
| 8. Have they consented to your sharing their data with those organisations? | Yes – parental consent form and interview |
| 9. Are the data subjects aware of the particular use to which their anonymised data are being put? | Yes – parental interview and explanatory notes, if the data subjects accept the invitation to ask these questions |
| 10. Have they consented to those uses? | Yes – parental consent form |

Of course, not all (and possibly none) of the questions have straight yes or no answers. Awareness is a nuanced concept. We are not saying that at this point that we should always be seeking informed consent. Given the current state of the information society this is both impractical and undesirable. Obtaining consent of any sort is complex. Obtaining real informed consent would – just as a starting point – require re-educating the whole populace and even then giving consent for every piece of processing for every piece of data is not something that most, if not all, people are going to engage with consistently. This is not to say that well thought out consent processes do not have their place – they most certainly do – but they are not a panacea.

We argue that the principles of the concept ‘contextual integrity’ can usefully be applied to the flow of anonymised data for the purpose of helping us to make well thought out and ethically sound decisions about how we reuse data.

To untangle this complex notion for practical use we have thought about the terms of roles and relationship between us and the proposed receivers of our anonymised data, and the purpose of the share/release. The complexity of the questions depends on the complexity of the data situation. We use a check list for a simple site-to-site share of data:

1. Do we (the sending organisation) have a relationship with the data subjects?
2. Does the receiving organisation have a relationship with the data subjects?
3. Do we and the receiving organisation work in different sectors?
4. Is our area of work one where trust is operationally important?
5. Is there an actual or likely perceived imbalance of benefit arising from the proposed share or release?

Here the more questions that are answered ‘yes’, the more sensitive the data situation is. Finally, the data themselves can have properties that make the data situation more or less sensitive. Three questions capture the main points:

1. Are some of the variables sensitive?
2. Are the data about a vulnerable population?

3. Are the data about a sensitive topic?

The UK Data Protection Act (1998) identifies a number of topics that are sensitive, two of which are relevant to data held by us: (a) The racial or ethnic origin of the data subject, (e) Their physical or mental health or conditions.

Underlying this notion of sensitivity is one of potential harm. The notion of harm is commonly measured in quantitative/economic terms such as financial loss, which is not relevant to our data, but it is also recognised that it can be felt in subjective ways such as loss of trust, embarrassment or loss of dignity. This is a consideration.

Harm felt subjectively is recognised in law – eg Article 8 of the European Convention of Human Rights stipulates that everyone has the right to respect for his or her private and family life, home and correspondence. Article 12 of the Universal Declaration of Human Rights (1948) goes even further: ‘No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.’ The concept of ‘a right to a private and family life’ encompasses the importance of personal dignity and autonomy and the interaction a person has with others, both in private and in public.

6. Disclosure

6.1 Key points

- Different forms of anonymised data can pose different re-identification risks.
- Publication is more risky than limited access.
- Limited access allows the disclosure of ‘richer’ data.
- Limited access relies on robust governance arrangements.

6.2 The use case

In determining the use cases for our data we have taken three things into account:

1. **Why:** Clarify the reason for wishing to share or release the data
2. **Who:** Identify those groups who will access the data
3. **How:** Establish how those accessing your data might want to use it

Working through these three points helps us with decisions about both *what data we can safely be shared/opened* and *what are the most appropriate means by which to do this*.

Firstly, we need to be clear about our reason(s) for sharing/opening, because our actions will be determined by these.

There are numerous reasons for disseminating data. Perhaps it provides useful information for stakeholders or about our organisation, offers new insights/perspectives on a topic, offers a benefit to particular groups, supports the more effective/efficient use of a service, or maybe we have received an FOI (freedom of information) request. Thinking through why we are disseminating the data automatically brings in the other two questions, the ‘who’ and the ‘how’ of access.

That there will be some benefit to the reuse of data is axiomatic in today’s ‘big data’ climate or PTUK’s ‘data guided organisation’. The demand for data seems insatiable. So clarifying the questions to be answered by our data, or what needs it is hoped they will meet, is a good place to start when thinking about exactly what data to release and how it should be specified.

6.3 Different types of anonymised data, different risks

A problem faced using anonymised data is that on the one hand they want data that is rich and usable enough for their purposes. On the other, they want to ensure that re-identification does not occur. This means that different disclosure options need to be considered.

Different types of anonymised data have different vulnerabilities and pose different levels of re-identification risk. At one end of the spectrum, pseudonymised or de-identified data may be very valuable to researchers because of its individual-level granularity and because pseudonymised records from different sources can be relatively easy to match. However, this also means that there is a relatively high re-identification risk. At the other end of the spectrum, aggregated data is relatively low-risk, depending on granularity, sample sizes and so forth. This data may be relatively ‘safe’ because re-identification risk is relatively low. However, this data may not have the level of detail needed to support the data linkage or individual-level analysis that some forms of research depend on.

Our policy is that pseudonymised data should only be used for case studies published in essays’, dissertations’ and publicity material including presentations, as is the standard procedure in the psychological professions.

The more aggregated and non-linkable the anonymised data is, the more possible it is to publish it. This might be the case for statistics showing the percentage of children in a wide geographical area who have achieved particularly high educational attainment following play therapy, for example, under the Freedom of Information Act 2000, or open data. Here – in reality - there is no restriction on the further disclosure or use of the data and no guarantee that it will be kept secure.

With limited access, eg within a closed community of researchers, it is possible to restrict the further disclosure or use of the data and its security can be guaranteed. Limited access is particularly appropriate for the handling of anonymised data derived from sensitive source material or where there is a significant risk of re-identification.

Our policy is to limit access to research data for specific groups with data governance protocols for each group. There can still be risks associated with limited access disclosure - but these can be mitigated where data is disclosed within a closed community working to established rules. Data minimisation rules will also remain relevant. It could be appropriate that data anonymised from a collection of personal data is published, whilst a record-level version of the data is released in a limited way under an enduser agreement. Our DPP does not permit a record level release of data unless requested by a Court or a police warrant.

6.4 Limited access safeguards

The organisation responsible for the initial disclosure of the data on a limited access basis must put robust safeguards in place before the data can be made available to others. This includes:

1. Purpose limitation, ie the data can only be used by the recipient for an agreed purpose or set of purposes;
2. training of recipients' staff with access to data, especially on security and data minimisation principles;
3. personnel background checks for those getting access to data;
4. controls over the ability to bring other data into the environment, allowing the risk of re-identification by linkage or association to be managed; limitation of the use of the data to a particular project or projects;
5. restriction on the disclosure of the data;
6. prohibition on any attempt at re-identification and measures for the destruction of any accidentally re-identified personal data;
7. arrangements for technical and organisational security, eg staff confidentiality agreements;
8. encryption and key management to restrict access to data;
9. limiting the copying of, or the number of copies of the data;
10. arrangements for the destruction or return of the data on completion of the project;
11. penalties, such as contractual ones that can be imposed on the recipients if they breach the conditions placed on them.

6.5 Meeting ethical obligations through governance

We outline in this section how we go about meeting our ethical obligations whilst maximising the value of the anonymised data.

6.5.1 Governance and human resources

- We have identified a person in our organisation who will be responsible for authorising and overseeing the anonymisation process and ensuring that they have the necessary skills and knowledge to do this. This is our Data Controller who is also the Data Processor SIRO and Registrar

- We will ensure that all relevant staff are suitably trained and understand their responsibilities for data handling, management, sharing and releasing. Because we are a small organisation of an individual person, Nicola Besley, the Data Controller is solely responsible for these functions.

6.5.2 Governance and internal structures

- I have established principles, policies and procedures for acting as a data controller. (Contained in this DPP)
- I have establish principles, policies and procedures for sharing and releasing data including how we will monitor future risk implications for each share (see section 6.14).
- I have a comprehensive record-keeping system across all our therapeutic activities related to our data protection policies and procedures to ensure there is a clear audit trail. The majority of my therapeutic data is stored and processed in an integrated relational database system (Fortuna2017 which incorporates good DP practice (released May 2017).
- Our policy incorporates PTUK's Privacy Impact Assessment (PIA) for all of our data products and/or across our organisation as a whole
- We have established principles, policies and procedures for dealing with data breaches. See section 6.17.

PTUK keeps its registrants up-to-date with any new guidance or case law that clarifies the legal framework surrounding anonymization .

6.5.3 Good practice

If an organisation or individual is involved in the anonymisation and disclosure of data, it is good practice to have an effective and comprehensive governance structure in place that will address the practical issues surrounding the production and disclosure of anonymised data. Having an effective governance structure in place will help if the Information Commissioner's Office (ICO) receives a complaint about the processing of personal data, including its anonymisation, or if they carry out an audit. Enforcement action – including the imposition of monetary penalties - is less likely where an organisation can demonstrate that it has made a serious effort to comply with the Data Protection Act (DPA) and had genuine reason to believe that the data it disclosed did not contain personal data or present a re-identification risk.

6.5.4 Governance requirements

Our governance structure covers the following areas.

- *Responsibility* for authorising and overseeing the anonymisation process. This should be someone of sufficient seniority and with the technical and legal understanding to manage the process. It is the role of our 'Senior Information Risk Owner' (SIRO) to take responsibility for key decisions and to inform our approach to anonymisation. The SIRO will coordinate a corporate approach to anonymisation, drawing on relevant expertise from within and outside an organisation. The SIRO will recommend suitable forms of disclosure, ie publication or limited access.
- *Staff training*: Relevant staff will have a clear understanding of anonymisation techniques, any risks involved and the means of mitigating these. In particular, individual staff members should understand their specific roles in ensuring anonymisation is being done safely.

- *Procedures for identifying cases where anonymisation may be problematic or difficult to achieve in practice:* These could be cases where it is difficult to assess re-identification risk or where the risk to individuals could be significant. It is good practice to have procedures in place to identify these difficult cases and to document how a decision was made as to how, or whether, to anonymise the personal data and how, or whether, to disclose it.

Registrants may consult PTUK on these problem cases.

- *Knowledge management* – this includes any new guidance or case law that clarifies the legal framework surrounding anonymisation. Knowledge management should also extend to new techniques that are available to organisations anonymising data and to intruders seeking to identify individuals within a dataset.
- *A joined up approach with other organisations* in our sector or those doing similar work. Organisations should seek to share information about planned disclosures with other organisations, to assess risks of jigsaw identification. For example it would be helpful for public authority A to know that public authority B is also planning an anonymised disclosure at the same time, one on health and one on welfare, both using similar geographical units. They can then assess the risks collectively and agree mitigation for both datasets.

PTUK encourages a joined up approach with other organisations concerned with welfare of children and other clients. It is important that registrants develop these links and manage disclosure carefully.

- *Transparency.* As anonymised data has no direct effect on any individual, there can be a tendency not to tell individuals about it, or even to be secretive. It may not be necessary, and in many cases will be impossible, to contact individual data subjects. We will explain to the public our organisation's approach to anonymisation as clearly as possible and any consequences of this. In particular:
 - why an individuals' personal data is anonymised and describe in general terms the techniques used to do this;
 - make it clear whether individuals have a choice over the anonymisation of their personal data, and if so how to exercise this – including the provision of relevant contact details. (Note though that the DPA does not give individuals a general right to prevent the processing of personal data about them);
 - say what safeguards are in place to minimise the risk that may be associated with the production of anonymised data. In particular, explain whether the anonymised data will be made publicly available or only disclosed to a limited number of recipients;
 - be open with the public about any risks of the anonymisation being carried out – and the possible consequences of this. You should give them the opportunity to submit queries or comments about this;
 - describe publicly the reasoning process regarding the publication of anonymised data, explaining how we did the 'weighing-up', what factors we took or did not take into account and why, how we looked at identification 'in the round'. This mode of transparency should improve trust as well as lead to improvements in the decision process itself through exposure to public scrutiny and comment.

Whilst it is good practice to be as transparent as possible, data should not be disclosed that would make re-identification more likely. However, excessive secrecy is likely to generate public distrust and suspicion.

- Review the consequences of our anonymisation programme, particularly through the analysis of any feedback you receive about it. Review should be an on-going activity and ‘re-identification testing’ techniques should be used to assess re-identification risk and to mitigate this. It is important to analyse and deal with any complaints or queries you receive from members of the public who believe that their privacy has been infringed.
-
- *Disaster recovery*: our governance procedures also address what we will do if re-identification does take place and individuals’ privacy is compromised. This could involve telling individuals there has been a breach and helping them to take any necessary remedial action. A re-identification incident may lead to the cessation of the anonymisation process or to its modification, eg by using more rigorous anonymisation techniques or disclosure controls.

6.6 Deliberate attacks and the data intruder

In disclosure control, the agent who attacks the data is usually referred to as the *data intruder*. As soon as we consider such a character as a realistic possibility rather than a shady abstraction, several questions immediately arise such as who might they be and what might they be trying to achieve by their intrusion? PTUK has considered such questions as who, how and why and developed a classification scheme, which we will use, as follows:

Inputs

- *Motivation*: What are the intruders trying to achieve?
- *Means*: What resources (including other data) and skills do they have?
- *Opportunity*: How do they access the data?
- *Target Variables*: For a disclosure to be meaningful something has to be learned; this is related to the notion of sensitivity.
- *Goals achievable by other means*? Is there a better way for the intruders to get what they want than attacking your dataset?
- *Effect of Data Divergence*: All data contain errors/mismatches against reality. How will that affect the attack?

Intermediate outputs (used in the risk analysis)

- *Attack Type*: What is the technical aspect of statistical/computational method used to attack the data?
- *Key Variables*: What information from other data resources is going to be brought to bear in the attack?

Final outputs (the results of the risk analysis)

- *Likelihood of Attempt*: Given the inputs, how likely is such an attack?
- *Likelihood of Success*: If there is such an attack, how likely is it to succeed?
- *Consequences of Attempt*: What happens next if they are successful (or not)?

- *Effect of Variations in the Data Situation:* By changing the data situation can we affect the above?

6.7. Intruder scenarios

Clearly, some sorts of data will be more attractive to a ‘motivated intruder’ than others. The sources of attraction to an intruder in the case of our data include:

<i>Motivation</i>	1 Finding out personal data about someone else, for nefarious personal reasons such as child custody issues;	2 the possibility of causing mischief by embarrassing others such as divorce evidence or professional jealousy;	3 political or activist purposes, eg as part of a campaign against a particular organisation or person;	4 curiosity, eg a local person’s desire to find out which parents have children requiring play therapy	5 potential for grooming a child for sexual abuse
<i>Means:</i>	Local knowledge	Local knowledge	Broad knowledge	Local knowledge	Local knowledge
<i>Opportunity:</i>	Usually low technical skills	Usually low technical skills	High technical skills	Usually low technical skills	Varying levels of technical skills
<i>Target Variables:</i>	Registrants systems – high	Registrants systems – high	Registrants systems – low	Registrants systems – high	Registrants systems – low
<i>Goals achievable by other means?</i>	PTUK systems - low	PTUK systems - low	PTUK systems - low	PTUK systems - low	PTUK systems - low
<i>Effect of Data Divergence</i>	Usually	Usually	Almost certainly	Usually	Almost certainly
<i>Attack Type</i>	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely
<i>Key Variables:</i>	Physical access to records	Physical access to records	Physical access to records	Physical access to records	Physical access to records
	Talking to other persons who know the child	Talking to other persons who know the child	Talking to other persons who know the child Systems intrusion	Talking to other persons who know the child	Talking to other persons who know the child

<i>Likelihood of Attempt:</i>	Moderate	Moderate	Low	Low	Low
<i>Likelihood of Success:</i>	Low probability	Low probability	Very low probability	Low probability	Very low probability
<i>Consequences of Attempt</i>	Moderate impact on parties concerned	Moderate impact on parties concerned	Serious impact on the play therapy profession	Moderate impact on parties concerned	Very serious impact on the play therapy profession
<i>Effect of Variations in the Data Situation:</i>	No	No	No	No	No

The most sensitive data, a client’s name and address and related details, are not collected by PTUK. The Fortuna2017 software ensures that these data items are stored in a separate sub-system, with separate security arrangements.

6.8 Prior knowledge and re-identification

Re-identification problems can arise where one individual or group of individuals already knows a great deal about another individual, for example a family member, colleague, therapist, clinical supervisor, teacher or other professional. These individuals may be able to determine that anonymised data relates to a particular individual, even though an ‘ordinary’ member of the public or an organisation would not be able to do this. eg a clinical supervisor knowing that an anonymised case study in a journal relates to a registrant that she is treating.

When considering re-identification risk, it is useful to draw a distinction between recorded information, established fact and personal knowledge. There must be a plausible and reasonable basis for non-recorded personal knowledge to be considered to present a significant re-identification risk.

Even if public authorities cannot rely on the ‘personal data’ exemption in FOIA to prevent the release of information like this, they may be able to rely on other exemptions, bearing in mind that the public interest may favour disclosure where an exemption is not absolute. Organisations that *are not public authorities should also adopt an approach of balancing the risk that disclosure may pose to an individual or group of individuals against the benefit that might result from the disclosure.*

In order to make sense of this scenario-classification scheme we take into account a set of basic concepts: key variables, data divergence, and response knowledge.

We also consider *uniqueness*, one of the fundamental concepts in disclosure risk assessment, which underpins much of the research on disclosure risk analysis. A record is unique on a set of key variables if no other record shares its combination of values for those variables.

For disclosure risk purposes we need to examine two types of uniqueness on a set of key variables: population uniqueness—a unit is unique in the population (or within a population data file such as a census); and sample uniqueness—a sample unit is unique within the sample file.

In one form or another, these two concepts – sample and population uniqueness –form the basis of many of the disclosure risk assessment methods for microdata (files of records about individuals). If a unit is population unique then disclosure will occur if an intruder *knows* it is

population unique. Much of the methodology in this area concerns whether sample information can be used to make inferences about population uniqueness.

In essence, identification means we find a person; attribution means we learn something new about them. Although the two processes often occur simultaneously, they can in fact occur separately.

Formally, a disclosure happens when an attribution is made, not when a re-identification happens. Accurate re-identification typically (but not always) leads to attributions, but attributions can happen without re-identification.

In the UK, the ICO has made it clear that reliable attribution does count as re-identification in their interpretation of the DPA: *Note that ‘identified’ does not necessarily mean ‘named’. It can be enough to be able to establish a reliable connection between particular data and a known individual.* UK: Information Commissioner’s Office (2012a p 21).

The key takeaway message is that any form of statistical disclosure counts as re-identification from the point of view of the DPA. So making data non-disclosive (in the context of its environment) will ensure that our processing is compliant with the DPA.

6.9 Types of attack and defences

6.9.1 PTUK’s main defence

The presupposition is that a data intruder has access to some information which contains formal identifiers for population units and a set of *key variables* which are also present on the target dataset. The key variables are then used to link the identifiers to the target information—in principle, this could be any information not already known to the data intruder but in practice, in the scenario framework, we assume that the information has some value in terms of their goal.

This is why PTUK uses different randomly generated IDs for different data sets that enabling linking but prevent disclosure of a client’s identity.

Diagram illustrating the use of randomly generated IDs in storing and processing client information received from registrants.

Key:

Data retained on registrants' systems. Not sent to PTUK	Data sent by registrants to PTUK	Data generated by PTUK
---	----------------------------------	------------------------

Person Contact details

Unique ID	Name	Address etc	Rand ID 1	Rand ID 2	Rand ID 3	Rand ID 4	Rand ID 5	PTUK S ID
-----------	------	-------------	-----------	-----------	-----------	-----------	-----------	-----------

Client Attributes

Ethnicity	Gender	Age etc	ID
-----------	--------	---------	----

Location of therapy

School name	Address	Borough	Type etc	ID
-------------	---------	---------	----------	----

Psychometric measures

Type	Pre item	Pre Item score	Post Item	Post Item score etc	ID
------	----------	----------------	-----------	---------------------	----

Hopes & expectations

Source	Objective	Pre	Post	Review stage	Notes	ID
--------	-----------	-----	------	--------------	-------	----

Session activities

Session no.	Presenting condition	Therapist	type of session	Activity	% time	Notes	ID
-------------	----------------------	-----------	-----------------	----------	--------	-------	----

However lists of individual data items are only used internally within PTUK or returned to the registrant. In all other cases, when client data is released outside of PTUK it is in aggregated sets of a minimum size of 250 records and with restricted geographic identification (see section 5.6)

Formal risk assessment for microdata releases usually requires us to understand the probability of the data intruder being able to make such linkages correctly. PTUK believes that the procedures described above make such linkages extremely unlikely.

6.9.2 Inference attacks

Low cell counts constitute a risk. Although it may not be possible, without external information about the population represented in a table, to make inferences about any given individual with certainty. However, this will change if a conversation is overheard about someone talking about the variable in relation to themselves. PTUK's recommended defence is to advise registrants not to talk about their data outside a professional audience.

6.9.3 Differencing attacks

A difference attack is possible with variables for which there are multiple different plausible coding schemes for a variable, where the categories in those coding schemes are not nested but instead overlap. This situation may occur where there are separate requests for tables or maps

with different codings potentially allowing more information to be revealed about those in the overlaps than intended from a single table. Although it could happen with any variable the issue most commonly comes up with geography. The end result of this is that whilst a table may be considered safe in isolation, this may not be the case for multiple tables when overlain with one another. PTUK's procedures governing the use of geographic variables makes the success of this type of attack extremely unlikely.

6.9.4 Complex attacks

The attacks mentioned above are the simple ones. There are more complex operations that a sophisticated intruder can try, often with lurid names that can confuse and befuddle: *table linkage, mashing attacks, fishing attacks, reverse fishing attacks* and so forth. All of these involve bringing together multiple data sources. In practice if one covers the simple attacks, in the way described above then the complex ones also become more difficult to execute. However, we have taken account that in releasing multiple data products from the same personal data source into the same environment there could be an increased risk. To mitigate this we do not release microdata samples and aggregate whole population from the same underlying dataset.

Fishing attacks should not be confused with Phishing. Phishing is fraudulently obtaining personal authentication information (usually passwords) by pretending to be a third party (often a bank). PTUK does not process this type of data. A fishing attack on the other hand is the identification of an unusual record in a dataset and then attempting to find the corresponding entity in the world.

To reiterate, we and PTUK take care, mostly through the extent of aggregation, when considering releasing multiple data products from the same data source.

6.10 Types of formal disclosure risk assessment

Broadly speaking there are two types of disclosure risk assessment: Data Analytical Risk Assessment (DARA) and penetration testing. The two approaches have complementary advantages and disadvantages. PTUK considers that the DARA approach is not practical so we have chosen the penetration test method.

There are three core advantages of intruder testing as a risk assessment method compared to DARA approaches:

1. It mimics more precisely what a motivated intruder could do.
2. It will explicitly take account of data divergence.
3. It is based on real data gathering and real external data.

In other words it is *grounded*. Against this, we recognise that it has one important disadvantage: it will be tied very tightly to one particular exercise and therefore does not necessarily represent all of the things that could happen. This disadvantage is the flip-side of its advantages and indeed is an issue with all testing regimes: one trades off groundedness against generality.

6.11 Data sharing procedures

Our overall objective, in applying the framework is to disseminate *safe useful data*.

6.11.1 Data Sharing Agreements

We will prepare data sharing agreements, for each case as required, setting out a common set of rules to be adopted by the organisations/persons involved in the share. Our framework is illustrated by two examples:

Factor	Organisations/persons (recipients)	
	PTUK	A university student undertaking research
Data situation	Simple share with secondary controlled release. 4 environments	Simple share with secondary controlled release. 3 or 4 environments
Purpose(s) of the share	Quality assurance and audit of registrants' work. Service evaluation at a national level.	Data to be included, as part of an MA dissertation
Recipients of the share and the circumstances in which they will have access and the model used	Professional Standards Authority; British Council for Therapeutic Interventions With Children; PTUK/PTI registrants; professional journals and magazines. All data sets are aggregated and anonymised. Case studies are pseudonymised.	University staff and recipients of dissertation.
Data to be shared	<p>Model 2: Pluralistic control</p> <p>Anonymised client attributes</p> <p>Anonymised location of therapy</p> <p>Therapy session data</p> <p>Psychometric and other measures of pre and post therapy scores</p> <p>Clinical supervision data</p> <p>Therapist's CPD plan and activities</p>	<p>All data sets are aggregated and anonymised. Case studies pseudonymised</p> <p>Model 1: Single controller</p> <p>Clinical data related to topic</p>
Data security	<p>Clinical outcomes (client IDs anonymised)</p> <p>All data kept in secure IT systems</p>	<p>Clinical data (Clients' IDs anonymised – data aggregated)</p> <p>All data kept in secure IT systems</p>
Retention of shared data	100 years	For period of research project + 10 years
Sanctions for failure to comply with the agreement	Sanctions dependent upon the impact of the failure ranging from a condition imposed by the ICO to rectify the situation and fine by the ICO	Sanctions dependent upon the impact of the failure ranging from a condition to rectify the situation to suspension/ removal from PTUK's Accredited Register and fine by the ICO

6.11.2 Data situations

In applying our data environment we recognise that data in one environment may be considered sufficiently anonymised (for example the de-identified data in a secure setting), but in a different environment (such as a researcher’s publication) this may no longer be the case at all. The model that we use is the *Simple share with secondary controlled release*.

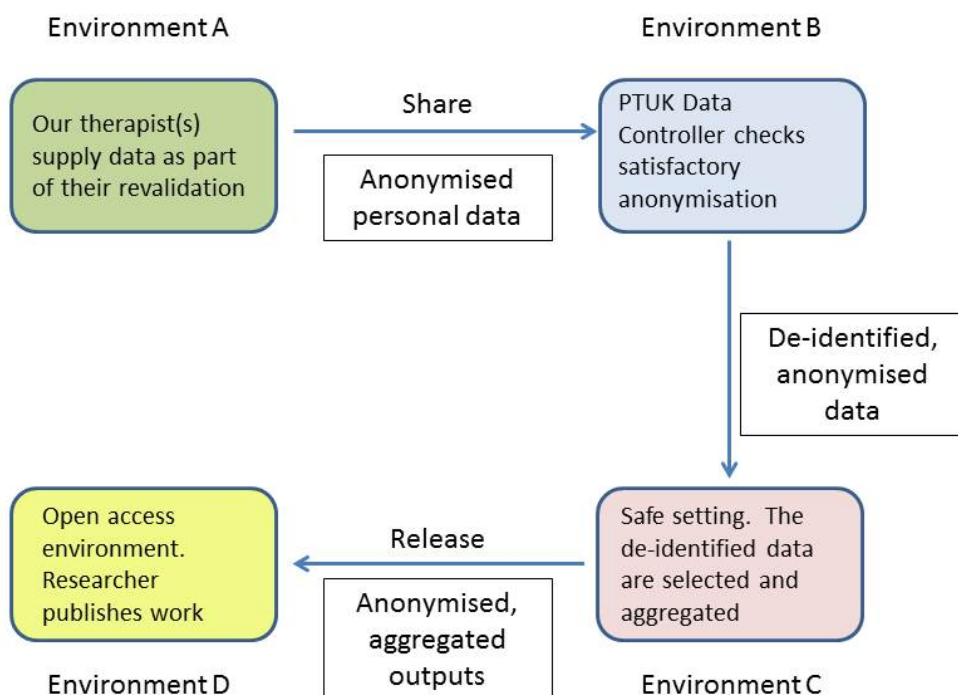
This applies to data flow across environments involving personal and de-identified data. The data share is formalised under a data sharing agreement which stipulates both ourselves and the recipient as data controllers in common for those data. This means both organisations have full data protection responsibilities as shown in the diagram below where our organisation is A.

A recipient, such as PTUK, as part of its remit to revalidate our therapist(s), uses a de-identified subset of the data and makes it available within a secure setting for re-use by approved accredited researchers. The recipient (PTUK) is environment B.

The secure setting within B is designed in such a way as to ensure that the de-identified data are functionally anonymous. It places restrictions on who can access the data, on how they can be accessed, and on what auxiliary information can be brought in and out of C’s secure environment eg a PTUK training provider’s academic partner - environment C.

An approved accredited researcher carries out a data analysis in environment C producing statistical output, such as regression models, that will need to be written up for her/his research. These outputs are first checked by environment C staff, to ensure that they are not disclosive, so they are passed as ‘safe’. The researcher duly writes up and openly publishes her research, which contains some of the analytical output. The publication of the research is a fourth environment, D.

Our Data Sharing Environment



6.12 Legal responsibilities in data sharing

The movement of data across multiple environments complicates the question of who is responsible for data and more specifically: what is our role in respect of those data? Are we a data controller, processor or user in a particular context? The key to resolving this is to: (i) *know where the data have come from* and under what conditions and (ii) *know where they are going* and under what conditions. The ‘conditions’ we take account of are:

1. The status of the data in each data environment in the data situation, whether they are personal, de-identified or anonymous data.
2. The data provenance, i.e. who decided to collect the data (including what data and who it is about), established the legal grounds for doing so and determined the means for processing it.
3. The enabling conditions for the share or release of the data (in an anonymised form), i.e. how is that processing fair and lawful?
4. The mechanism for a data share or release, eg a data sharing agreement or contract, or an end user or open licence.

Despite the complexity of the questions here, many situations can be subsumed under two common models of processing responsibilities.

6.12.1 Data status: are my data personal?

Personal data are data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Article 29 Working Party’s 2007 opinion on ‘personal data’ identifies four main building blocks underpinning this description. It is worth looking briefly at these building blocks as they make explicit some of the inherent ambiguities that stem from applying an abstract concept to real world situations.

Any information – The Working Party notes, with which we concur, is that this phrasing calls for a wide interpretation, and includes any sort of statement about an individual. The statement may be objective, such as someone’s health, employment status or qualifications, or subjective, such as an opinion or assessment like ‘John Smith is a good practitioner’. *For information to be personal data it need not be true or proven.*

Relating to – This means the information is about an individual. The relation may be direct, for example their exam transcript in their certification data, SDQ scores in their clients’ records or a CV in their staff file. This is clear, but when the relation is indirect it can become complicated. Data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated’ (Article 29 Data Protection Working Party 2007:10).

Identified and identifiable – A person is considered to be identified if within a group of persons they can be distinguished from all others in the group eg a Play Therapist in Todcaster. A person is identifiable where the conditions exist to identify them. In considering whether a person is identifiable or not, context is the main issue.

Lastly, the concept of *natural persons* – The protection afforded by the rules of the Directive applies to natural persons (that is, to human beings) and more specifically living persons. In some circumstances, there are two further legal considerations that extend this in the UK. The first

concerns the Statistics and Registration Services Act (2007), which expands the protection to include any body corporate for the purposes of official statistics. The second concerns medical records of deceased persons. As we know the DPA protects the personal data of living persons only, as deceased persons under the Act are no longer considered data subjects. Although there are no clear legal obligations of confidentiality to deceased persons in the UK, for medical data the Department of Health and the General Medical Council have deemed that there is an ethical obligation to ensure that confidentiality continues to apply to these data after death. This is supported by the Scottish Freedom of Information Act (2002, section 38) which classes medical records of deceased persons as personal data. We adhere to both these rulings and use the life of the data subject as well as the data owner eg child, therapist – whichever is the longer, as the period in which data is stored and processed.

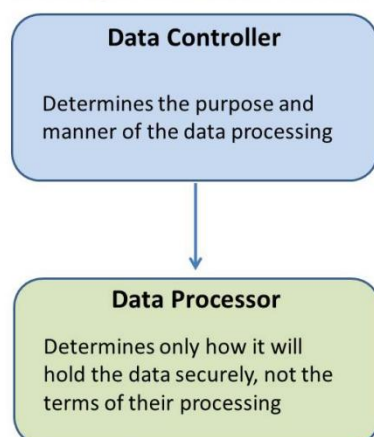
6.12.2 The Single controller model

This is the simplest model of data processing responsibilities and the one that we have adopted. The DPA requires that when a controller discloses personal data to a data processor it uses a written contract rather than a data sharing agreement. This is so only the controller can exercise control over the purpose for which and the manner for which personal data can be processed.

In the diagram below Nicola Besley is the data controller, having determined the manner in which, and the purposes for which, the data are processed. As such it retains overall responsibility for the data. The recipient's responsibilities are related to ensuring it does not breach the conditions of its contract with us and particularly its data security undertakings. However the legal responsibility for compliance with the DPA falls directly upon us (the data controller), not the recipient (the data processor). We cannot pass on our responsibility to the recipient and have a duty to ensure that the recipient's security arrangements are at least equivalent to our own as well as taking reasonable steps to ensure that these are maintained.

In terms of enforcement, even if the recipient were considered negligent because, for example, it did not follow agreed security measures, the ICO cannot take action against it, although we could pursue a civil action for breach of contract. On the other hand, if the recipient were to deliberately use the data for purposes not covered by our agreement, it would become a data controller in its own right and is likely to be in breach of the first principle of the DPA and the ICO could take enforcement action against it (see UK: Information Commissioner's Office (2014a) *Data Controller and Processor Guidance*).

The Single Controller Model



6.13 Identifying our stakeholders and methods of communication

Nicola Besley recognises that effective communication can help build trust and credibility, both of which are critical to difficult situations where we need to be heard, understood and believed. I will be better placed to manage the impact of a disclosure if we have developed a good working relationship with our stakeholders

Our data users are of course not the only group with an interest in our activities. Others who may be affected include data subjects, the general public, partner organisations, the media, funders and special interest groups. We have identified our main stakeholders as:

- Our clients, including parents, carers, employers and other professionals
- Our professional organisation, in this instance PTUK
- Regulatory authorities including [OFSTED, PSA and ICO]
- National and local government departments and agencies concerned with any aspect of children’s well-being; mainly education, health and social services including their research departments
- Professional, academic and general interest media
- All members of the public with an interest in children’s welfare and community groups

The main methods that we use for communicating data protection matters are:

- Emails – individual and bulk
- Personal visits and presentations by our staff and therapists
- Group meetings with parents

6.14 Incident and breach management

6.14.1 Current situation

Nicola Besley is an individual with limited resources to deploy in managing breaches.

The detection of surreptitious attacks on information recorded on paper is more difficult. I am confident that my office and safe storage facilities are good.

Attacks might come from four main groups:

Group	Probability	Defence need
National government agencies eg cyber warfare	Virtually nil – my data is of no interest	No complete protection is possible if data is to remain usable
Criminals seeking money by reselling data or ransom	Medium – as with any other organisation. The larger the size the bigger the risk. Individual PCs have been attacked.	PC and other mobile device protection
Amateur Hackers seeking personal satisfaction		Server and database protection Data transmission protection
Individuals seeking to redress a perceived wrong caused in		Mainly for paper records containing client data.

some way by actions of one of our staff. Low

Physical access to premises and out of office situations.

Our incident management policy is being developed. This will set out:

- how I would recognise and report an incident;
- how incidents would be logged and investigated;
- the need to report an incident to the ICO and notify the data subjects concerned, where appropriate; and
- how to implement any ‘lessons learned’ following an incident.

The following headings indicate our approach which needs to be refined and tested over the next two years.

6.14.3 Definitions

A Data Breach (breach) is a security incident that involves the intentional or unintentional access, disclosure, manipulation or destruction of data.

A Security incident is an event that violates our regulatory, legislative or contract obligations.

A breach may be related to paper records or IT systems.

6.14 .4 Questions arising from a breach

In order to identify and deal with a breach the following items will be collected, where possible:

1. Nature of the incident
2. Who detected the incident?
3. How was the incident discovered?
4. When was the incident discovered?
5. When was it reported? How? To whom?
6. Who knows about the incident? Who needs to know?
7. Is there any information involved that is protected by regulatory or legislative requirements?
8. What is the scope of the incident? Number of systems/records, type of data
9. What actions have been taken?
10. Are there any third parties involved?
11. What data is available from logs? Network firewall, VPN, host, application; database; others?
12. What are the objectives of the investigation?
13. Are there recent vulnerability assessments?
14. What is the retention period of log data?
15. Has any intelligence been received that may be relevant to the incident?

6.14.5 Investigating a suspected breach

There are four key questions:

Infiltration: How did the perpetrators gain access?

Propagation: How did the perpetrators move from the point of entry to the location of the targeted data or system?

Aggregation: How did the perpetrators access and harvest the targeted data or control of the targeted system?

Exfiltration: How did the perpetrators move the harvested data to a system controlled by the attackers?

6.14.6 Communicating a breach

No matter how strong an organisation's defences, a data breach can still occur. Therefore cyber resilience – the ability to become strong, healthy or successful again after something bad happens – is critical and only comes from preparation. Our action plan will include:

Before a crisis

- Examining our Cyber Scope, based on our data environment
- The role of social media
- The speed imperative
- The potential use of additional resources
- The appropriate chain of command
- Training
- Use of crisis simulations to test plans
- Developing a Guiding Light strategy

During a crisis

Manage the three stages:

- Access
- Resolve
- Control

After a crisis

We will review:

- The Discovery-to-Notification time gap
- Adequacy of safeguards in place
- Appropriateness of the data held

7 The Data Protection Act research exemption

7.1 What does the DPA say?

The use of data for quality assurance and research is a main consideration in our DPP. Section 33 of the Data Protection Act 1998 (DPA) provides an exception to those engaged in historical or other research, and in the preparation of certain statistics, to some of the eight data protection principles contained in the DPA. There are conditions:

- (i) that the data are not processed to support measures or decisions with respect to particular individuals, and
- (ii) that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

The exemption is, however, quite narrow and only affects the three data protection principles relating to the purpose for which data were obtained (the second data protection principle); the duration for which they can be kept (the fifth data protection principle); and the data subject's access provisions (relating to a data subject's right of access under s.7 DPA).

- 1 So Section 33 does not give a blanket exemption from all the data protection principles which apply to personal data provided and/or used for research purposes. Researchers wishing to use personal data should be aware that most of the data protection principles will still apply (notably the requirement to keep data secure).
- 2 For the purposes of the second data protection principle, the further processing of personal data only for research purposes in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which they were obtained.
- 3 Personal data which are processed only for research purposes in compliance with the relevant conditions may, notwithstanding the fifth data protection principle, be kept indefinitely.
- 4 Personal data which are processed only for research purposes are exempt from section 7 if:
 - (a) they are processed in compliance with the relevant conditions, and
 - (b) the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them.
- 5 For the purposes of subsections (2) to (4) personal data are not to be treated as processed otherwise than for research purposes merely because the data are disclosed:
 - (a) to any person, for research purposes only,
 - (b) to the data subject or a person acting on his behalf,
 - (c) at the request, or with the consent, of the data subject or a person acting on his behalf, or
 - (d) in circumstances in which the person making the disclosure has reasonable grounds for believing that the disclosure falls within paragraph (a), (b) or (c).

Section 33(2) provides that the further processing of personal data only for research purposes will not breach the second data protection principles (i.e. personal data must not be processed in a manner which is incompatible with the purpose for which the data were obtained) if the processing complies with the ‘relevant conditions’.

Provided that the ‘relevant conditions’ have been complied with, personal data may be further processed for research purposes:

1. *even if the data were originally obtained for a different purpose eg revalidation compliance (therefore exempt from the second data protection principle);*
and
2. the personal data may be kept indefinitely for the specific research purposes for which they are being used (therefore exempt from the fifth data protection principle);
and
3. the personal data will be exempt from the data subject’s rights of access where ‘the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them’ (section 33(4)).

7.2 What is ‘research’?

The DPA does not define ‘research’. Therefore the Information Commissioner uses an ordinary meaning of ‘research’ when determining whether personal data is being processed for research purposes: **research is a systematic investigation intended to establish facts, acquire new knowledge and reach new conclusions**, which are the purposes of our and PTUK’s research policies. The DPA makes it clear that ‘research purposes’ include statistical or historical research, but other forms of research, for example market, social, commercial or opinion research, could also benefit from the exemption. This is inconsistent with the PSA’s advice but not with the research carried out by PTUK registrants. PTUK have agreed with the PSA to distinguish data used for audit, quality assurance and service evaluation from research. However we consider that the analyses that we undertake using the PTUK clinical evidence base falls under the ICO meaning.

In our view the research undertaken by our therapists using aggregated and anonymised data exempts it from the principles of the DPA as shown above.

7.3 What sort of data is section 33 relevant to?

The exemption is clearly of most relevance where personal data – rather than anonymised data – is being used for research. The exemption is as applicable to sensitive personal data, eg data about someone’s health being processed for medical research – as it is to ‘ordinary’ personal data. It provides important - though limited - assistance to those seeking to use personal data for research purposes. As explained elsewhere in the code, it is not always possible to use anonymised data for research purposes. Therefore researchers should be aware of the useful features that this exemption contains and the protection for individuals that it provides. The exemption can apply to data collected primarily for research purposes and to cases where research is a secondary purpose.

7.4 Section 33 safeguards

For the exemption to apply, certain conditions must be satisfied:

- the data must not be processed to support measures or decisions with respect to particular individuals.

- the data must not be processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

Where anonymisation is carried out effectively, neither the production nor the publication of the anonymised data *will have any effect on any particular individual*. Provided that this is the case, the research exemption's conditions will have been satisfied.

7.5 Incompatibility, retention and subject access

Provided the data is only processed for research purposes, and the conditions are satisfied, then:

- the data may be processed for research purposes without falling foul of the DPA's prohibition on processing data for an 'incompatible' purpose. *This puts it beyond doubt that personal data obtained for one purpose can also be used for research purposes;*
- the data may be retained indefinitely. This is important in contexts such as historical research or longitudinal studies because the data protection principles usually require that personal data is not kept for longer than is necessary. Note that the data protection principles do not apply to anonymised data;
- the data will be exempt from the right of subject access – provided the data is not published in a form which identifies any individual or individuals. This means that organisations can avoid the administrative issues associated with dealing with individuals' requests. It is good practice though to grant individuals access to personal data held for research purposes even if the exemption does apply.

Clearly the research exemption provides important benefits for researchers and important safeguards for individuals. However, it is good practice to plan for the publication of anonymised data as early in the data life cycle as is practicable. This will help to minimise, or will negate, the risk to individuals. It also means that researchers will not need to be concerned with the parts of the DPA from which section 33 does not provide exemption, eg the requirement to process personal data fairly and lawfully.

7.6 The disclosure of research data

The section 33 exemption can still be relied on even if research outputs are published in a form which identifies individuals, but the exemption from providing subject access will be lost. However, depending on the circumstances, the publication of personal data for research purposes could still breach other provisions of the DPA.

This would not normally apply to our therapists because we do not identify individuals.

There is a particular incentive to anonymise sensitive personal data, eg data about someone's health or criminal convictions. This is because this type of personal data is subject to relatively stringent data protection restrictions. In particular, it could be difficult to find an alternative to seeking the data subject's consent as a means of legitimising the processing of sensitive data about their health. (In some cases an organisation may, as a matter of policy, decide to always obtain data subjects' consent for the anonymisation of personal data about them, but the DPA provides alternatives to this.) Our policy is that anonymisation should occur at the earliest opportunity – ideally by the data controller anonymising the personal data prior to processing, disclosing or using it for research purposes.




The DPA does not necessarily prohibit the disclosure of research data in a form which identifies individuals and the benefit of the section 33 exemption will not necessarily be lost if this happens. However, even if a researcher needs personal data to carry out research, it is arguably a breach of the DPA to publish or disclose data for research purposes in a form which identifies individuals where there is an alternative to this.

Remember that an organisation that receives personal data from a researcher will take on its own data protection responsibilities as the data controller for that data. This could mean informing the individuals concerned that your organisation has obtained personal data about them. If an individual consents to the use or disclosure of personal data about them for research purposes then there will be no need to rely on the DPA's research exemption. However, it can be impossible for organisations or individuals to exercise control over personal data once it has been published. An obvious problem might be where an individual who once consented to the use or disclosure of their personal data decides to revoke consent, eg because of a change in their personal circumstances.

Therefore our policy is to use and disclose anonymised data rather than personal data for research and other purposes - even where consent could be obtained. (It is rare for research outputs to be published in the form of personal data and consent for this would not normally be sought for this type of disclosure.)

Annex 1 – PTUK model consent procedures

A1.1 Model Consent Form

Play therapy – parent’s permission			
---	--	---	---

Child’s name:

I understand that any information or personal details you collect about me, my child or family during play therapy are confidential, and that neither my name, address, nor any other information that identifies me or my child will be released or published outside the organisation/agency/school.

(During the course of therapy we will be recording information about your son or daughter but we will not reveal your child’s name and address in any information we share with anyone else, unless it is for medical or legal reasons. We use all information in line with the Data Protection Act. Please ask us if you would like details of the information that we collect and how we use it.)

I agree that my child can attend therapeutic play or play therapy sessions.	Yes <input type="checkbox"/>	No <input type="checkbox"/>
I agree that the information you collect will be used for monitoring and review purposes, as part of the therapist’s supervision.	Yes <input type="checkbox"/>	No <input type="checkbox"/>
I agree that clinical information that does not identify my child may be used for research purposes and for case studies. I understand that any information used will remain confidential, and that no information that identifies me or my child will be used or published.	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If I do not agree to you using information as above, this will not affect any care my child receives.		
Parent’s signature:	Date:	
Please print your full name:		

Nicola Besley ICO UK Data Protection Register number:ZA327946
 Play Therapy UK Data Protection Register number: CSN1642296

A1.2 Explanatory Notes to be used by the therapist

The purpose of these notes is to help you and us meet the requirements of UK data-protection legislation.

Remember that parents may be stressed, deeply concerned, defensive and possibly angry if their child has been referred by somebody else for play therapy, so only use these explanations if the parent or carer asks for them.

Use language that is appropriate to the parent's or carer's understanding of English (or the language being used).

Ask frequently 'Is that OK?' or 'Is that clear?', and 'Would you like any more information?'

Only answer the questions asked.

Substitute the first name of the client for 'your child'.

Only use 'mental health' if appropriate for the severity of the issue.

Adapt the answers if your employer's policies or procedures are different.

Explain that parents have a right to ask to see the personal information that we keep about them and their child at any time.

I How we will use your details

a. Your personal contact details (your name, address, phone number and email address)

We will only use this information to contact you or for reporting the progress and results of the therapy for quality assurance purposes. We will only share these details outside of our organisation for medical or legal purposes.

b. Your child's age, sex, ethnic background and why they have been referred for play therapy

We will use this information in reports circulated within our organisation. We use it to assess how effective and efficient the service is for different types of children. If the details contain your or your child's name, we will mark them as 'confidential' and store them securely. If we send this information outside the organisation, we will make it anonymous so that neither you nor your child can be traced.

c Measures based on the results of questionnaires

You or the person who referred your child for play therapy will fill in these questionnaires. We will use the questionnaires to assess how severe any emotional well-being, behaviour or mental-health issues are so that we can decide how many sessions your child needs and who they should see. We may also use the questionnaires after therapy has started and definitely at the end of therapy to see what changes have happened. If any reports contain your child's name, we will mark them as 'confidential' and store them securely. If we send the reports outside the organisation, we will make the information in them anonymous so that it can't be linked to your child or yourself

d The activities your child does during the sessions

We use this information to review your child's progress. We also use it to see which activities help improve children's emotional well-being and mental health so that we can improve the quality of our therapists' practice, including their training. If any reports contain your child's name we will mark them as confidential and store them securely. If we send reports outside the organisation we will make the information in them anonymous so that it can't be linked to your child or yourself.

Clinical information may also be used in case studies that are used to assess the quality of play therapists work. We may circulate this information more widely to help other therapists improve their practice. Your child will not be able to be identified from any information used for this purpose.

2 Supervision and quality assurance

All practitioners on the Register of Play and Creative Arts Therapists, managed by Play Therapy UK and accredited by the Professional Standards Authority, must have a set number of hours of clinical supervision. The therapist makes a verbal report on each child to a clinical supervisor who is very experienced in working in therapy with children. The child's progress, including their problems, what they do in the sessions, any significant themes in their play and anything else that is relevant, is discussed. The clinical supervisor assesses and reviews a therapist by providing support and advice, identifying any problem areas and, if necessary, suggesting action to be taken.

Notes may be taken during the discussions between the therapist and supervisor. If these notes contain your or your child's name, we will mark them as confidential and store them securely. If we send any part of these notes to anyone else or another organisation, we will make your or your child's personal details anonymous so that you can't be traced.

3 Play Therapy UK

Play Therapy UK is my professional organisation. It uses information about your child and their play therapy activities to check the quality of therapists' service, and to update the clinical evidence base (see below) and other research projects which are aimed at improving the quality of therapists' practice for the benefit of the children they work with.

The clinical evidence base is kept in a secure computer database managed by PTUK. It is used to compare the results of therapy with a child's characteristics (such as their age, sex, ethnic background and the condition they have been referred with), the number and type of sessions and the therapy activities that have taken place. Doing this helps Play Therapy UK to set guidelines of good practice, and to identify any areas of risk or where further investigation (through research) is needed. Play Therapy UK makes all the information anonymous so that a child cannot be identified in any reports that are produced. When information is analysed and reported on, it is based on groups of a minimum number of 200 cases and does not identify any child.

Play Therapy UK therapists have to revalidate each year. They do this by providing the following information.

- Your child's age, sex, ethnic background and the condition they were referred to us with
- Measures they have taken based on information from questionnaires
- The therapy activities carried out by the child during the sessions

Your name and contact details and those of your child are not passed on to Play Therapy UK.

Fortuna2017

Fortuna2017 is a system that Play Therapy UK recommends that therapists use from May 2017 onwards. Within Fortuna, information is encrypted as well as password-protected. Only encrypted information is passed to Play Therapy UK. When therapists submit information, a series of randomly allocated client-identity numbers are used. This allows Play Therapy UK to link the items of information for analysis without revealing your child's identity. This information is kept in a secure database system which is not connected to the internet. In the unlikely event of security being at risk it is almost impossible to identify you or your child.

Your rights

You have a right to see any information that we hold about you or your child. We may charge a small fee for this service.

For details of information held by your service provider, therapist or clinical supervisor, please contact:

{56}.....]

For details of information held by Play Therapy UK, please contact:

Jeff Thomas
Registrar & Data Controller
Play Therapy UK
The Coach House
Belmont Road
Uckfield TN25 1BP.

Phone: 01825 761143

Annex 2 – Exemptions to Subject Access Requests

A2.1 Introduction

The Data Protection Act 1998 (DPA) recognises that in some circumstances there might be a legitimate reason for not complying with a subject access request (SAR), so it provides a number of exemptions from the duty to do so. Where an exemption applies to the facts of a particular request, PTUK may refuse to provide all or some of the information requested, depending on the circumstances. It is a matter for us to decide whether or not to use an exemption – the DPA does not oblige us to do so, so PTUK is free to comply with a SAR even if we could use an exemption.

Certain restrictions (similar to exemptions) are also built into the DPA's subject access provisions. For example, there are restrictions on the disclosure of personal data about more than one individual in response to a SAR.

Not all of the exemptions apply in the same way, and we should look at each exemption carefully to see how it applies in a particular SAR. Some exemptions apply because of the nature of the personal data in question, eg information contained in a confidential reference. Others apply because disclosure of the information would be likely to prejudice a particular function of the organisation to which the request is made. The DPA does not explain what is meant by 'likely to prejudice'. However, the Information Commissioner's view is that it requires there to be a substantial chance (rather than a mere risk) that complying with the SAR would noticeably damage the discharge of the function concerned. If challenged, PTUK must be prepared to defend to the Information Commissioner's Office or a court our decision to apply an exemption. It is therefore good practice to ensure that such a decision is taken by the Chief Executive or Registrar and that we document the reasons for it.

A2.2 Confidential references

From time to time we may give or receive references about an individual, eg in connection with their contracting or employment, or for educational purposes. Such references are often given 'in confidence', but that fact alone does not mean the personal data included in the reference is exempt from subject access. The DPA distinguishes between references you give and references you receive.

References you give are exempt from subject access if you give them in confidence and for the purposes of an individual's education, training or employment or the provision of a service by them. There is no such exemption for references you receive from a third party. If you receive a SAR relating to such a reference, you must apply the usual principles about subject access to decide whether to provide some or all of the information contained in the reference.

Example: Company A provides an employment reference for one of its employees to company B. If the employee makes a SAR to company A, the reference will be exempt from disclosure. If the employee makes the request to company B, the reference is not automatically exempt from disclosure and the usual subject access rules apply.

It may be difficult to disclose the whole of a reference to the individual it relates to without disclosing some personal data about the author of the reference – most obviously, their identity. If the reference was not provided in confidence, this difficulty should not prevent disclosure. However, if a question of confidentiality arises, you should contact the author to find out

whether they object to the reference being disclosed and, if so, why. Even if the provider of a reference objects to its disclosure in response to a SAR, you will need to supply the personal data it contains to the requester if it is reasonable to do so in all the circumstances. You will therefore need to weigh the referee's interest in having their comments treated confidentially against:

- the requester's interest in seeing what has been said about them. Relevant considerations are likely to include:
- any clearly stated assurance of confidentiality given to the referee;
- any reasons the referee gives for withholding consent;
- the likely impact of the reference on the requester;
- the requester's interest in being able to satisfy himself or herself that the reference is truthful and accurate; and
- any risk that disclosure may pose to the referee.

A2.3 Publicly available information

If an enactment requires an organisation to make information available to the public, any personal data included in it is exempt from the right of subject access. The exemption only applies to the information that the organisation is required to publish. If it holds additional personal data about an individual, the additional data is not exempt from the right of subject access even if the organisation publishes it.

A2.4 Crime and taxation

Personal data processed for certain purposes related to crime and taxation is exempt from the right of subject access. These purposes are:

- the prevention or detection of crime;
- the capture or prosecution of offenders; and
- the assessment or collection of tax or duty.

Example The police process an individual's personal data because they suspect him of involvement in a serious crime. If telling the individual they are processing his personal data for this purpose would be likely to prejudice the investigation (perhaps because he might abscond or destroy evidence), then the police do not need to do so. However, the exemption applies, in any particular case, only to the extent that complying with a SAR would be likely to prejudice the crime and taxation purposes set out above. We need to judge whether or not this is likely in each case – we should not use the exemption to justify denying subject access to whole categories of personal data if for some individuals the crime and taxation purposes are unlikely to be prejudiced.

Example A taxpayer makes a SAR to Her Majesty's Revenue and Customs (HMRC) for personal data they hold about him in relation to an ongoing investigation into possible tax evasion. If disclosing the information which HMRC have collected about the taxpayer would be likely to prejudice their investigation, eg because it would make it difficult for them to collect evidence, HMRC could refuse to grant subject access to the extent that doing so would be likely to prejudice their investigation. If, however, the taxpayer does not make the request until some years later when the investigation (and any subsequent prosecution) has been completed, it is unlikely that complying with the SAR would prejudice the crime and taxation purposes – in which case HMRC would need to comply with it.

Nor would the exemption justify withholding all the personal data to which the request relates when only part of the personal data would be likely to prejudice those purposes.

Example In the previous example about an ongoing investigation into possible tax evasion, HMRC would be entitled to refuse subject access to personal data that would be likely to prejudice their investigation. However, this would not justify a refusal to grant access to other personal data they hold about the taxpayer.

Personal data that:

- is processed for the purpose of discharging statutory functions; and
- consists of information obtained for this purpose from someone who held it for any of the crime and taxation purposes described above

is also exempt from the right of subject access to the extent that providing subject access to the personal data would be likely to prejudice any of the crime and taxation purposes. This prevents the right applying to personal data that is passed to statutory review bodies by law-enforcement agencies, and ensures that the exemption is not lost when the information is disclosed during a review.

Example The Independent Police Complaints Commission (IPCC) begins an investigation into the conduct of a particular police force. Documents passed to the IPCC for the purposes of the investigation contain personal data about Mr A that the police force would not have been obliged to disclose to Mr A in response to a SAR – because doing so would be likely to prejudice its criminal investigation. If Mr A then makes a SAR to the IPCC, he has no greater right of access to the personal data in question.

Section 29(4) of the DPA provides an additional exemption from the right of subject access that is designed to prevent the right being used to force relevant authorities to disclose information about the operation of crime detection and anti-fraud systems, where such disclosure may undermine the operation of those systems.

A2.5 Management information

A further exemption applies to personal data that is processed for management forecasting or management planning. Such data is exempt from the right of subject access to the extent that complying with a SAR would be likely to prejudice the business or other activity of the organisation.

Example The senior management of an organisation are planning a re-organisation. This is likely to involve making certain employees redundant, and this possibility is included in management plans. Before the plans are revealed to the workforce, an employee makes a SAR. In responding to that request, the organisation does not have to reveal its plans to make him redundant if doing so would be likely to prejudice the conduct of the business (perhaps by causing staff unrest in advance of an announcement of the management's plans).

A2.6 Negotiations with the requester

Personal data that consists of a record of your intentions in negotiations with an individual is exempt from the right of subject access to the extent that complying with a SAR would be likely to prejudice the negotiations.

Example An individual makes a claim to his insurance company. The claim is for compensation for personal injuries he sustained in an accident. The insurance company dispute the seriousness of the injuries and the amount of compensation they should pay. An internal paper sets out the company's position on these matters and indicates the maximum sum they would be willing to pay to avoid the claim going to court. If the individual makes a SAR to the insurance company, they would not have to send him the internal paper – because doing so would be likely to prejudice the negotiations to settle the claim.

A2.7 Regulatory activity

Some organisations may use an exemption from subject access if they perform regulatory activities. The exemption is not available to all organisations, but only to those that have regulatory functions concerning the protection of the public or charities, or fair competition in business. Organisations that do have such functions may only apply the exemption to personal data processed for these core regulatory activities, and then only to the extent that granting subject access to the information concerned would be likely to prejudice the proper discharge of those functions.

A2.8 Legal advice and proceedings

Personal data is also exempt from the right of subject access if it consists of information for which legal professional privilege (or its Scottish equivalent, 'confidentiality in communications') could be claimed in legal proceedings. The English law concept of legal professional privilege encompasses both 'legal advice' privilege and 'litigation' privilege. In broad terms, the former applies only to confidential communications between client and professional legal adviser, and the latter applies to confidential communications between client, professional legal adviser or a third party, but only where litigation is contemplated or in progress.

The Scottish law concept of confidentiality of communications provides protection both for communications relating to the obtaining or providing of legal advice and for communications made in connection with legal proceedings. Information that comprises confidential communications between client and professional legal adviser may be withheld under the legal privilege exemption in the same way that information attracting English law 'legal advice' privilege may be withheld. Similarly, the Scottish law doctrine that a litigant is not required to disclose material he has brought into existence for the purpose of preparing his case protects information that, under English law, would enjoy 'litigation' privilege.

Where legal professional privilege cannot be claimed, you may not refuse to supply information in response to a SAR simply because the information is requested in connection with actual or potential legal proceedings. The DPA contains no exemption for such information; indeed, it says the right of subject access overrides any other legal rule that limits disclosure. In addition, there is nothing in the Act that limits the purposes for which a SAR may be made, or which requires the requester to tell you what they want the information for.

It has been suggested that case law provides authority for organisations to refuse to comply with a SAR where the requester is contemplating or has already begun legal proceedings. The Information Commissioner does not accept this view, but he recognises that:

- the courts have discretion as to whether or not to order compliance with a SAR; and
- if a court believes that the disclosure of information in connection with legal proceedings should, more appropriately, be determined by the Civil Procedure Rules (the courts' rules on disclosure),

- it may refuse to order personal data to be disclosed.

Nevertheless, simply because a court may choose not to order the disclosure of an individual's personal data does not mean that, in the absence of a relevant exemption, the DPA does not require you to disclose it. It simply means that the individual may not be able to enlist the court's support to enforce his or her right.

A2.9 Social work records

Special rules apply where providing subject access to information about social services and related activities would be likely to prejudice the carrying out of social work by causing serious harm to the physical or mental health or condition of the requester or any other person. These rules are set out in the Data Protection (Subject Access Modification) (Social Work) Order 2000 (SI 2000/415). Their effect is to exempt personal data processed for these purposes from subject access to the extent that its disclosure would be likely to cause such harm.

A further exemption from subject access to social work records applies when a SAR is made by a third party who has a right to make the request on behalf of the individual, such as the parent of a child or someone appointed to manage the affairs of an individual who lacks capacity. In these circumstances, personal data is exempt from subject access if the individual has made clear they do not want it disclosed to that third party.

A2.10 Health records

The exemptions that may apply when a SAR relates to personal data included in health and education records.

To apply this exemption, there clearly needs to be an assessment of the likelihood of the disclosure causing serious harm. Unless you are a health professional, you must consult the health professional who is responsible for the clinical care of the individual concerned before deciding whether the exemption applies. This requirement to consult does not apply if the individual has already seen or knows about the information concerned.

A further exemption from subject access to information about an individual's physical or mental health applies where a SAR is made by a third party who has a right to make the request on behalf of the individual, such as the parent of a child or someone appointed to manage the affairs of an individual who lacks capacity. In these circumstances, personal data is exempt from subject access if the individual has made clear they do not want it disclosed to that third party.

A2.11 Information held about pupils by schools

A pupil, or someone acting on their behalf, may make a SAR in respect of personal data held about the pupil by a school. If the school is in England, Wales or Northern Ireland, the SAR should be dealt with by the school. If the school is in Scotland, the SAR should be dealt with by the relevant education authority or the proprietor of an independent school.

There are two distinct rights to information held about pupils by schools. They are:

- the pupil's right of subject access under the DPA; and
- the parent's right of access to their child's 'educational record' (in England, Wales and Northern Ireland this right of access is only relevant to maintained schools – not independent schools, English academies or free schools. However in Scotland the right extends to independent schools).

Although this code is only concerned with the right of subject access, it is important to understand what is meant by a pupil's 'educational record'. This is because there is an overlap between the two rights mentioned above. The statutory definition of 'educational record' differs between England and Wales, Scotland and Northern Ireland. Broadly speaking, however, the expression has a wide meaning and includes most information about current and past pupils that is processed by or on behalf of a school. However, information kept by a teacher solely for their own use does not form part of the educational record. It is likely that most of the personal information a school holds about a particular pupil will form part of the pupil's educational record. However, it is possible that some of the information could fall outside the educational record; eg, information about the pupil provided by the parent of another child is not part of the educational record.

Unlike the distinct right of access to the educational record, the right to make a SAR is the pupil's right. Parents are only entitled to access information about their child by making a SAR if the child is unable to act on their own behalf or has given their consent. If it is not clear whether a requester has parental responsibility for the child or is acting on their behalf, you should clarify this before responding to the SAR.

In deciding what information to supply in response to a SAR, you need to have regard to the general principles about exemptions from subject access described elsewhere in the ICO code. Examples of information which (depending on the circumstances) it might be appropriate to withhold include:

- information that might cause serious harm to the physical or mental health of the pupil or another individual;
- information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
- information contained in adoption and parental order records; and
- certain information given to a court in proceedings concerning the child.

A2.12 SAR exemptions good practice

An organisation that makes appropriate use of the exemptions in the DPA might have the following indicators of good practice:

A2.12.1 Withholding or redacting information

If information is withheld in reliance on an exemption, the response explains, to the extent it can do so, the fact that information has been withheld and the reasons why. The explanation is given in plain English, and does more than simply specify that a particular exemption applies.

Information to be redacted is approved before source material is copied in a redacted form. It is then subject to at least one quality review by a manager to confirm that all data has been excluded appropriately. A copy of the disclosure bundle showing the redactions and the reasons behind them is retained for reference. Once approved, redaction is either carried out manually using black marker which is then photocopied, or electronically using Adobe Acrobat or bespoke redaction software.

A2.12.2 Ensuring consistency

Advice on applying the exemptions most likely to be relevant to the organisation's activities is included in SAR guidance for staff. Quality assessments are carried out to ensure that exemptions are applied consistently.

Annex 3 Anonymisation of data

A3.1 Introduction

Anonymisation together with the disclosure of data are key issues in our DPP. So often ‘Data protection issues’ have been erroneously used as a reason for not releasing data that is in the public interest.

The area of greatest sensitivity is the client clinical data that PTUK collects from registrants. This data has to be provided in an anonymised form. They are almost always shared/released in an aggregated form by PTUK so that the risk of re-identification is minimal.

PTUK has taken the PSA’s advice to refer to Health Research Authority (HRA)’s Differentiating Audit, Service Evaluation and Research document. 3. It has been concluded that PTUK is carrying out both audit and service evaluation so these activities are no longer defined as ‘research’ in this context. PTUK does not undertake original research directly but registrants may do so.

However, there is some contradiction with the broader ICO definition: ‘*Research is a systematic investigation intended to establish facts, acquire new knowledge and reach new conclusions*’. We have resolved this by applying it to the research activities of registrants, such as during the MA stage of their training. This case the ICO definition will be used. This research will normally be fully covered by their University’s review of topic and research proposal, including any need to obtain NHS ethical approval.

A3.2 Basic principles

The Information Commissioner has issued its code for anonymization under section 51 of the Data Protection Act ‘. The DPA says good practice includes, but is not limited to, compliance with the requirements of the DPA. This code was also published with Recital 26 and Article 27 of the European Data Protection Directive (95/46/EC) in mind. These provisions **make it clear that the principles of data protection do not apply to anonymised data.**

The DPA does not require anonymisation to be completely risk free – we must be able **to mitigate the risk of identification until it is remote.** If the risk of identification is reasonably likely the information should be regarded as personal data, Clearly, 100% anonymisation is the most desirable position, and in some cases this is possible, but it is not the test the DPA requires.

The term ‘re-identification’ is used to describe the process of turning anonymised data back into personal data through the use of data matching or similar techniques. The ICO’s code’s annexes contain examples of various anonymisation and re-identification techniques and illustrations of how anonymised data can be used for various purposes which PTUK has reviewed to decide which methods should be used.

A distinction has to be drawn between anonymisation techniques used to produce aggregated information, for example, and those – such as pseudonymisation – that produce anonymised data but on an individual-level basis. The latter can present a greater privacy risk, but not necessarily an insurmountable one. There is also a distinction between publication to the world at large and the disclosure on a more limited basis – for example to a particular research establishment with conditions attached. PTUK in the main adopts the latter approach where there is a moderate degree of granularity. In the case of public dissemination, data is aggregated

to a safe spatial level, based on a minimum of 250 cases so making identification virtually impossible’ eg ‘77% of boys showed a positive change.’

A3.4 Risks and mitigation

PTUK has identified the issues that need to be considered when deciding how to anonymise personal data. The risks considered include:

Risk	PTUK	Mitigation [40].....]
<ul style="list-style-type: none"> • Information about someone’s private life ending up in the public domain; • an anonymised database being ‘cracked’ so that data about a number of individuals is compromised; • individuals being caused loss, distress, embarrassment, or anxiety as a result of anonymised data being re-identified; • reduced public trust if anonymised data is disclosed unsafely; 	<p>Careful design of the data collection forms and systems design; secure protection measures for digital and hard copy data.</p> <p>PTUK’s data and that received from registrants is kept on a password protected server that is not connected to the Internet. It is in a secured building.</p> <p>Anonymised registrant client ids are used, nor names or addresses.</p>	<p>[41)]</p> <p>Anonymised registrant client ids are used, not names or addresses of clients, parent/carers, referrers, when data is released outside [42)],</p>
<ul style="list-style-type: none"> • legal problems where insufficiently redacted qualitative data is disclosed, for example, under FOIA. 	<p>Very little qualitative data is collected by PTUK. It is almost entirely concerned with registrants rather than clients. Some action and learning points issued by clinical supervisors to registrants may relate to specific clients, who cannot be identified by PTUK.</p>	

A3.5 Decision framework

The ICO published its ‘Anonymisation: Managing Data Protection Risk’ code of practice in 2012. Experience provided two main lessons. Firstly, effective anonymisation is possible but it is also possible to do anonymisation ineffectively. Secondly, it isn’t always possible to draw the definitive personal / non-personal data distinction that legal certainty in the field of data protection depends on. As a result our policy also takes into account ‘ The Anonymisation Decision-Making Framework’ (ADF) produced by (Mark Elliot, Elaine Mackey Kieron O’Hara and Caroline Tudor published in 2016 by UKAN, University of Manchester. This shows that we have to deploy effective anonymisation techniques and assess re-identification risk *in context*, recognising that there is a wide spectrum of personal identifiability and that different forms of identifier pose different privacy risks.

We have also taken into account the National Data Guardian for Health and Care Review of Data Security, Consent and Opt-Outs - Dame Fiona Caldicott, National Data Guardian June 2016 (Caldicott Review).

As at April 2010, the European Commission has made positive findings of adequacy in relation to the following countries outside the European Economic Area (EEA) : Argentina, Canada, Guernsey, Isle of Man, Switzerland, Jersey, Faroe Islands and the USA.

The framework recommended by PTUK is underpinned by a relatively new way of thinking about the re-identification problem which posits that we must look at both the data and the data environment to ascertain realistic measures of risk. This is called the data situation approach.

Some privacy models such as differential privacy and k-anonymity do attempt to assess and control risk by comparing it to some theoretically parameterised environment – there is however nothing intrinsic in these models that requires engagement with the actual data environment and therefore are not being used by PTUK or ourselves.

PTUK is following the ADF's total system approach which consists of ten components:

1. Describing our data situation through our data catalogue and data environment scenario
2. Describing our legal responsibilities
3. Demonstrating a knowledge of our data
4. Understanding the use case
5. Demonstrating how our ethical obligations are met
6. Specifying the processes needed to assess disclosure
7. Specifying the disclosure control processes needed
8. Identifying who our stakeholders are and planning how we will communicate
9. Planning what happens once our data has been shared or released
10. Planning what we will do if things go wrong

In developing these components we have adopted the five principles upon which the ADF is founded:

1. We cannot decide whether data are safe to share/release or not by looking at the data alone.
2. But we still need to look at the data.
3. Anonymisation is a process to produce safe data but it only makes sense if what we are producing is safe *useful* data.
4. Zero risk is not a realistic possibility if we are to produce useful data.
5. The measures we put in place to manage risk should be proportional to the risk and its likely impact.

Zero risk is not a realistic possibility if we are to produce useful data: This is fundamental. Anonymisation is about risk management, nothing more and nothing less; accepting that there is a residual risk in all useful data inevitably puts us in the realms of balancing risk and utility.

The measures we put in place to manage risk are in our judgement proportional to that risk and its likely impact.

A3.6 Anonymisation and the law

Anonymisation is a process to allow data to be shared or disseminated ethically and legally, thereby realising their huge social, environmental and economic value, whilst preserving confidentiality.

There are four possible types of data:

About People	Non-Identifiable data	Identifiable data
Yes	Anonymised Data	Primary Personal data
No	Apersonal Data	Secondary Personal Data

The term *apersonal* is used here rather than *non-personal*. The point is to distinguish between data that are not to do with people from those that are to do with people but have been anonymised so that they are non-personal. So *apersonal* data are always non-personal but not vice versa.

So, are anonymised data non-personal?

Usually, following anonymisation, the original personal data still exist and this means that (except perhaps for the coarsest of aggregate data) the data controller will still be able to identify individuals within the anonymised data (using the original data as a reference) and therefore it would seem that on a literal reading of the definition of personal data the data must still be personal. There are two ways of resolving this paradox:

1. To say that the anonymised data are personal and therefore the question about whether to share or release them depends on whether the DPA provides another get-out (eg whether the share or release constitutes fair processing).
2. To say that the anonymised data are personal for the original data controller but non-personal for other users of the data.

We have adopted the second of these positions as it directly ties the concept of anonymisation to the notion of the context of personal data (in this case, other sources of data that users have access to) and makes a clean separation between the complexities of data protection, such as the (essentially ethical) question of fairness, on the one hand, and the (essentially technical) question of identifiability on the other.

Now, given that we are assuming perfect anonymisation, most of the principles of the DPA are clearly met. For example, principle 7 concerning data security, is intrinsically met directly by the anonymisation process. Principle 5 will be met as soon as the purpose that the original personal data were collected has been achieved (and the original data are destroyed rendering the anonymised data non-personal for everyone) and principles 3, 4 and 6 can only be meaningfully applied to the original data. This leaves us with principles 1, 2 and 8.

Principle 8: Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data is potentially relevant to any open data release as open data if it is globally published via the Internet and therefore

available in all countries regardless of their DP laws and practices. Our policy is not to publish personal data on the Internet.

Principle 2: *Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes*
The justification for an anonymised share or release would usually be either: (i) it is necessary for administering justice, or for exercising statutory, governmental, or other public functions or (ii) that it is in accordance with the legitimate interests of the data controller or (iii) for the exercise of any other functions of a public nature exercised in the public interest by any person. In the vast majority of cases where release or sharing of anonymised data is being considered one of those justifications will apply. Our policy clearly meets (ii) and (iii) and also accord with the Caldicott Review.

PTUK has identified two categories of data in this context:

- i) That collected for the auditing of registrants' individual practice and the quality assurance of the PTUK overall programme – our clinical evidence base is included for the purpose of setting standards and issuing guidelines
- ii) The release of data from the clinical evidence base for research purposes. In this instance data is aggregated to a minimum of 250 cases, meeting our spatial controls and without the names or addresses of individuals, rendering re-identification almost impossible.

A3.7 User, processor, controller – roles in the anonymisation process

Understanding the legal status in respect of particular data is important as it helps us to establish clearly what our responsibilities are *and those of any other stakeholders* during the anonymisation process. It may also be that the design of the process will affect the roles that different agents play.

The DPA defines a data controller as:

... a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

There are two conditions in this definition:

1. That a data controller determines the purposes and manner in which the data are processed.
2. That the data are personal data.

In contrast to a data controller, a data processor does no more than process personal data in the way(s) decided by the data controller. Their processing activities may include for example storing the personal data, providing security, transferring them across the organisation or to another and indeed anonymising them. The roles of the Data Controller, Data Processor and SIRO (Senior Information Risk Owner) are undertaken in PTUK by the Registrar.

A3.8 De-identification and anonymisation

There is a lot of confusion between the two terms *de-identification* and *anonymisation* mostly arising from the fact that the former is usually a necessary but rarely sufficient component of the latter.

De-identification – refers to a process of removing or masking *direct identifiers* in personal data such as a person’s name, address, school number or other unique number associated with them. De-identification includes what is called *pseudonymisation*.

Anonymisation – refers to a process of ensuring that the risk of somebody being identified in the data is negligible. This invariably involves doing more than simply de-identifying the data, and often requires that data be further altered or masked in some way in order to prevent statistical linkage.

We can highlight further the difference between anonymisation and de-identification (including pseudonymisation) by considering how *re-identification* might occur:

1. Directly from those data.
2. Indirectly from those data and other information which is in the possession, or is likely to come into the possession, of someone who has access to the data.

The process of de-identification addresses *no more* than the first, i.e. the risk of identification arising directly from data. The process of anonymisation, on the other hand, should address both 1 and 2. Thus the purpose of anonymisation is to make re-identification difficult both directly and indirectly. In de-identification – because one is only removing direct identifiers – the process is unlikely to affect the risk of indirect re-identification from data in combination with other data.

It should be noted that in the description of both processes (i.e. de-identification and anonymisation) the purpose is to make re-identification more *difficult*. Both de-identification and anonymisation are *potentially* reversible; the data environment in which data is shared or released is of critical importance in determining reversibility. In other words, the data environment can either support or constrain reversibility which means that PTUK has had to think very carefully about the environment in which they share or release data. For example, it may be entirely appropriate to release de-identified data in a highly controlled environment such as a secure data lab but not at all appropriate to release them more openly, for example by publishing them in a journal.

A3.9 Types of anonymisation

The term ‘anonymisation’ gets used in a variety of different ways and inevitable communication difficulties arise as a consequence. Elliot et al (2015) have identified four different usages:

1. Formal Anonymisation
2. Guaranteed Anonymisation
3. Statistical Anonymisation
4. Functional Anonymisation - this is PTUK’s approach.

A3.10 Is anonymisation always possible?

The Information Commissioner recognises that some collections of personal data do not lend themselves well to anonymisation – eg voluminous collections of paper records held in a variety of formats. Although the sensitivity of data will generally decrease with the passage of time, the inappropriate release of records many decades old, eg criminal records, could still have a severely detrimental effect on an individual. That is why the security of data that cannot be anonymised is paramount. It is worth noting that the DPA’s section 33 exemption, described later - allows personal data held for research purposes to be retained indefinitely, provided certain conditions

are met. PTUK strongly recommends that only digital records are kept by registrants and has developed software to make this feasible.

A3.11 What ‘other’ information is out there?

Determining what other information is ‘out there’, who it is available to and whether it is likely to be used in a re-identification process can clearly be extremely problematic. The ‘other information’ needed to perform re-identification could be information available to certain organisations, to certain members of the public or that is available to everyone because it has been published on the internet, for example. Clearly the risk of combining information to produce personal data increases as data linkage techniques and computing power develop, and as more potentially ‘match-able’ information becomes publicly available.

It is worth stressing that the risk of re-identification through data linkage is essentially unpredictable because it can never be assessed with certainty what data is already available or what data may be released in the future. It is also generally unfeasible to see data return (ie recalling data or removing it from a website) as a safeguard given the difficulty, or impossibility, of securing the deletion or removal of data once it has been published. PTUK’s PIA has identified which data may be released outside the PTUK environment and under what conditions. **It is especially important that registrants do not disclose information relating to any client on social media.**

A3.12 Ensuring the effectiveness of anonymisation

If the anonymisation of data is ineffective there is the risk of re-identification. PTUK has identified two main issues:

3) The risk of the data being obtained by an intruder

We have measures in place and recommendations for therapists to minimise this risk

4) The risk of breaking anonymisation by cross referencing data sets

Generally the latter risk scenario is of greater concern for data custodians because of the confidentiality pledges that are often given to those appearing in an anonymised dataset. However, both risk scenarios are relevant and can carry with them different probabilities of re-identification. In either case though it can be difficult, even impossible, to assess risk with certainty. Despite all the uncertainty, re-identification risk can certainly be mitigated by ensuring that only the anonymised data necessary for a particular purpose is released.

PTUK’s procedure, which we have adopted, at present rely upon the anonymisation of the client’s identity by means of a code. This code can be used in 5 other datasets. PTUK are investigating the feasibility of using different client ID codes in the Fortuna2017 for each dataset to reduce this risk. This protects against re-identification from any lists released or published. However lists are only released in response to statutory or legal authorities. Otherwise data is aggregated.

A3.13 Freedom of information and personal data

Section 40 of the Freedom of Information Act 2000 (FOIA) introduces a broader concept of risk because its test for deciding whether personal data can be disclosed is whether disclosure to a member of the public would breach the data protection principles. This means that organisation and individual practitioners have to assess whether releasing apparently anonymised data to a member of the public would breach the data protection principles. This is intended to ensure that Data Protection Officers take into account the additional information that a particular member of

the public might have that could allow data to be combined to produce information that relates to and identifies a particular individual – and that is therefore personal data.

This risk is managed by restricting the dissemination of anonymised, aggregated data to a limited number of data controllers and through conditions attached to their use.

A3.14 Anonymising qualitative data

Much of the anonymised data being created, used and disclosed is derived from clinical and administrative datasets that are essentially statistical in nature. However, the techniques used to anonymise quantitative data are not generally applicable when seeking to anonymise qualitative data, such as the minutes of meetings, case notes, interview transcripts or video footage. Different techniques are needed to do this. We:

[43) ...]

- redact individuals' names from documents where permission has not been obtained;
- only uses videos of training sessions which are erased after use (typically 48 hours);
- do not use recordings of audio material;
- change the details in a report that reveal an individual's identity

A3.15 Ethics and anonymisation

It is not always immediately obvious why ethical considerations have a role to play in the process of anonymisation. Most readers will understand that the processing of personal data is an ethical issue but once data are anonymised are our ethical obligations not dealt with? This is an understandable confusion which arises in part from a conflation of legal and ethical constraints. Legally, functional anonymisation is sufficient but this might not be true ethically. There two primary reasons why we need to consider ethics beyond the law:

1. Data subjects might not want data about them being re-used in general, by specific third parties or for particular purposes.
2. We are not dealing with zero risk.

There is growing evidence that data subjects are concerned not just about what happens with their personal data but also about the anonymised data derived from their personal data.

There may be many reasons why data subjects object to the reuse of their data. For example I might be unhappy about my data – even anonymised – being reused by a particular type of organisation.

[44)] makes it clear that any data that we hold is not released to any organisation that is not concerned with the emotional well-being of children and young persons and then only for audit, quality assurance or research purposes. Our therapists' ethical principles of Fidelity, Autonomy, Beneficence, Non-maleficence and Justice are applied.

A3.16 Anonymisation techniques low risk

A3.16.1 Aggregation

Data is displayed as totals, so no data relating to or identifying any individual is shown. Small numbers in totals are often suppressed through 'blurring' or by being omitted altogether.

Recommended by PTUK.

Variants:

- Cell suppression - if data is from a sample survey then it may be inappropriate to release tabular outputs with cells which contain small numbers of individuals, say below 30. This is because the sampling error on such cell estimates would typically be too large to make the estimates useful for statistical purposes. In this case, suppression of cells with small numbers for quality purposes acts in tandem with suppression for disclosure purposes.

Recommended by PTUK.

- Inference Control – Some cell values (eg small ones such as 1-5) in statistical data can present a greater risk of re-identification. Depending on the circumstances, small numbers can either be suppressed, or the values manipulated (as in Barnardisation). If a large number of cells are affected, the level of aggregation could be changed. For example, the data could be linked to wider geographical areas or age-bands could be widened.

Recommended by PTUK.

- Perturbation – such as Barnardisation - is a method of disclosure control for tables or counts. It involves randomly adding or subtracting 1 from certain cells in the table. This is a form of perturbation.

Not recommended by PTUK – too complex for our purposes.

- Rounding – rounding a figure up or down to disguise precise statistics. For example if one table may have a cell with value of 10,000 for all people doing some activity up to the present date. However, the following month, the figure in that cell rises to 10,001. If an intruder compares the tables it would be easy to deduce a cell of 1. Rounding would prevent this.

Recommended by PTUK, where appropriate.

- Sampling - in some cases, when very large numbers of records are available, it can be adequate for statistical purposes to release a sample of records, selected through some stated randomized procedure. By not releasing specific details of the sample, data holders can minimise the risk of re-identification.

May be used by PTUK but difficult for registrants because of the small size of datasets.

- Synthetic data - mixing up the elements of a dataset – or creating new values based on the original data - so that all of the overall totals and values of the set are preserved but do not relate to any particular individual.

Difficult to implement

- Tabular reporting – a means of producing tabular (aggregated) data, which protects against re-identification.

Recommended by PTUK.

These are relatively low risk techniques because it will generally be difficult to find anything out about a particular individual by using aggregated data. This data cannot support individual-level research but can be sufficient to analyse social trends on a regional basis, for example.

A3.16.2 Derived data items and banding

Derived data is a set of values that reflect the character of the source data, but which hide the exact original values. This is usually done by using banding techniques to produce coarser-grained descriptions of values than in the source dataset eg replacing dates of birth by ages or years, addresses by areas of residence or wards, using partial postcodes or rounding exact figures so they appear in a normalised form. Again, this is a relatively low-risk technique because the banding techniques make data-matching more difficult or impossible. The resulting data can be relatively rich because it can facilitate individual-level research but presents relatively low re-identification risk.

Recommended by PTUK.

A3.17 High risk techniques

A3.17.1 Data masking

This involves stripping out obvious personal identifiers such as names from a piece of information, to create a data set in which no person identifiers are present.

Variants:

- **Partial data removal** – results in data where some personal identifiers, eg name and address have been removed but others such as dates of birth, remain.

Anonymisation is necessary.

- **Data quarantining** - The technique of only supplying data to a recipient who is unlikely or unable to have access to the other data needed to facilitate re-identification. It can involve disclosing unique personal identifiers – eg reference numbers – but not the ‘key’ needed to link these to particular individuals.

Recommended by PTUK where appropriate.

These are relatively high risk techniques because the anonymised data still exists in an individual-level form. Electoral roll data, for example, could be used to reintroduce names that have been removed to the dataset fairly easily. However, this type of data is also relatively ‘rich’ in terms of allowing an individual to be tracked as part of a longitudinal study for example.

A3.18 Pseudonymisation

De-identifying data so that a coded reference or pseudonym is attached to a record to allow the data to be associated with a particular individual without the individual being identified. Deterministic modification is a similar technique. ‘Deterministic’ here means that the same original value is always replaced by the same modified value. This means that if multiple data records are linked, in the sense that the same name (or address, or phone number, for example) occurs in all those records, the corresponding records in the modified data set will also be linked in the same way. This facilitates certain types of data analysis. This is also a relatively high risk technique, with similar strengths and weaknesses to data masking.

Pseudonyms be used where reference to individual cases is necessary as in academic assignments, published articles, research papers etc. The client’s name must never be used. In disguising it care must taken not to use the client’s initials. A numeric sequence is preferred.

Other attributes that may identify the client such as a combination of age, gender and presenting condition must also be considered carefully.

Annex 4 Cookies - DPP requirements

Acknowledgement: A significant part of the content in this annex is based upon material published by [Optanon](#) who provide cookie consent and audit services and also upon guidance developed by the UK International Chamber of Commerce.

A4.1 What are cookies?

Almost all websites use cookies - little data files - to store information in peoples' web browsers. Some websites contain hundreds of them.

Cookies are pieces of data, normally stored in text files, that websites place on visitors' computers to store a range of information, usually specific to that visitor - or rather the device they are using to view the site - like their browser or mobile phone.

They were created to overcome a limitation in web technology. Web pages are 'stateless' - which means that they have no memory, and cannot easily pass information between each other. So cookies provide a kind of memory for web pages.

Cookies allow you to login on one page, then move around to other pages and stay logged in. They allow you to set preferences for the display of a page, and for these to be remembered the next time you return to it.

Cookies can also be used to watch the pages you visit between sites, which allows advertisers to build up a picture of your interests. Then when you land on a site that shows one of their adverts - they can tailor it to those interests. This is known as 'behavioural advertising'.

Almost all websites use cookies in some way or another, and every page you visit in those sites writes cookies to your computer and receives them back from it.

Cookies are incredibly useful – they allow modern websites to work the way people have come to expect – with every increasing levels of personalisation and rich interactive functionality.

However, they can also be used to manipulate your web experience in ways you might not expect, or like. It could be to your benefit, or the benefit of someone else – even a business or organisation that you have never had any direct contact with, or perhaps heard of.

It is impossible to tell just by looking at them, whether particular cookies are benefitting you or another party. You have to rely on the website you are visiting to tell you how it uses cookies

There are other technologies, like Flash and HTML5 Local Storage that do similar things, and these are also covered by the legislation, but as cookies are the most common technology in use, it has become known as the Cookie Law.

Cookies are a kind of short term memory for the web. They are stored in your browser and enable a site to 'remember' little bits of information between pages or visits.

They are widely used to make the web experience more personal, which is generally seen as a positive thing. However, some cookies collect data across many websites, creating 'behavioural profiles' of people. These profiles can then be used to decide what content or adverts to show you. This use of cookies for targeting in particular is what the law was designed to highlight. By requiring websites to inform and obtain consent from visitors it aims to give web users more control over their online privacy.

To find out lots more about cookies in general and the different types, take a look at Cookiepedia - a leading information resource all about cookies.

A4.2 Requirements of the legislation

The 'Cookie Law' refers to a piece of privacy legislation that requires websites to get consent from visitors to store or retrieve any information on a computer, smartphone or tablet.

It was designed to protect online privacy, by making consumers aware of how information about them is collected and used online, and give them a choice to allow it or not. It started as an EU Directive that was adopted by all EU countries in May 2011. The Directive gave individuals rights to refuse the use of cookies that reduce their online privacy. Each country then updated its own laws to comply. In the UK this meant an update to the Privacy and Electronic Communications Regulations.

All websites owned in the UK or targeted towards EU citizens, are now expected to comply with the law. The key elements of the requirements can be summarised as:

1. Information should be sufficiently complete to enable users to understand the purpose/uses of the cookies.
2. The site should take into account the likely audience of the site when explaining the uses of cookies, avoiding terminology that would be difficult for the average site visitor to understand.
3. They advise also that sites should assume knowledge about the uses of cookies and how to manage them is limited.
4. Information about cookies and how to manage them can be layered, but must always be accessible, even after consent has been obtained. A specific 'Cookie Policy' link is advised over a generic 'Privacy Policy'.
5. There must be information on how to revoke consent after it has been obtained.
6. Information should distinguish between first and third party cookies, and identify the third party organisations that are setting cookies.

If you don't comply you risk enforcement action from regulators, which in the UK means The Information Commissioners' Office (ICO). In exceptional cases this can mean a fine.

However, non-compliance could also have other, perhaps more serious consequences than enforcement. There is plenty of evidence that consumers avoid engaging with websites where they believe their privacy is at risk, and there is a general low level of trust about web tracking by the use of cookies.

A4.3 Compliance with the legislation

Compliance with the cookie law comes down to three basic steps:

1. Work out what cookies your site sets, and what they are used for, with a cookie audit
2. Tell your visitors how you use cookies.
3. Obtain their consent and give them some control.

Your cookie audit should tell you:

- the attributes and values of each cookie used on your site
- their purpose and use categories
- the 3rd parties setting cookies on your site, and what they do with them
- how best to inform your visitors according to guidance developed by the UK International Chamber of Commerce.

A4.4 Types of cookies

Uses	Consent
<p>1: Strictly necessary cookies</p> <p>These cookies are essential in order to enable you to move around the website and use its features, such as accessing secure areas of the website. Without these cookies services you have asked for, like shopping baskets or e-billing, cannot be provided.</p> <p>These cookies are used by PTUK</p>	<p>User consent is not required for the delivery of those cookies which are strictly necessary to provide services requested by the user. However, it is important to give users the opportunity to understand these cookies and the reasons they are used.</p> <p>The ‘strictly necessary’ category is narrowly defined in the UK due to the wording of the law. The view of the ICO is that only a small range of activities can be categorised as ‘strictly necessary’ and the use of the cookie must be related to a service provided on the website that has been explicitly requested by the user.</p> <p>These cookies will not be used:</p> <ul style="list-style-type: none"> • To gather information that could be used for marketing to the user. • To remember customer preferences or user ID’s outside a single session (unless the user has requested this function).
<p>2: Performance cookies</p> <p>These cookies collect information about how visitors use a website, for instance which pages visitors go to most often, and if they get error messages from web pages. These cookies don’t collect information that identifies a visitor. All information these cookies collect is aggregated and therefore anonymous. It is only used to improve how a website works.</p> <p>These cookies are used by PTUK.</p>	<p>These cookies are used to remember visitor selections that change the way the site behaves or looks. It might also include cookies that are used to deliver a specific function, but where that function includes cookies used for behavioural/targeted advertising networks they must be included in category 4 as well as this category.</p> <p>Obtaining consent by functional use:: “By using our [website][online service], you agree that we can place these types of cookies on your device.”</p>
<p>3: Functionality cookies</p> <p>These cookies allow the website to remember choices you make (such as your</p>	<p>As these cookies are site specific and are linked to user choices for using a site, consent</p>

user name, language or the region you are in) and provide enhanced, more personal features. For instance, a website may be able to provide you with local weather reports or traffic news by storing in a cookie the region in which you are currently located. These cookies can also be used to remember changes you have made to text size, fonts and other parts of web pages that you can customise. They may also be used to provide services you have asked for such as watching a video or commenting on a blog. The information these cookies collect may be anonymised and they cannot track your browsing activity on other websites.

These cookies are used by PTUK.

4: Targeting cookies or advertising cookies

These cookies are used to deliver adverts more relevant to you and your interests. They are also used to limit the number of times you see an advertisement as well as help measure the effectiveness of the advertising campaigns. They are usually placed by advertising networks with the website operator's permission. They remember that you have visited a website and this information is shared with other organisations such as advertisers. Quite often targeting or advertising cookies will be linked to site functionality provided by the other organisation.

for use of these types of cookies may be obtained in a number of ways, for instance when the user changes the settings for the site or selects an option, eg language or country. The method used will depend on the nature of the website, and the precise function of the cookies involved.

Targeting or advertising cookies are placed for the benefit of website operators, either by third parties at the direction of website operators or alternatively by website operators using third-party functionality on their website. Careful analysis of your cookie audit will be required to establish the correct position.

PTUK does not use this category of cookie. Our strong recommendation is that registrants should also avoid their use.

A4.5 PTUK Model Statement

'Cookies are essential to the proper functioning of our site. To improve your experience, we use cookies to remember log-in details and provide secure log-in, collect statistics to optimize site functionality and performance, and deliver content tailored to your interests. Click Agree and Proceed to accept cookies to go directly to the site or click on Set preferences to see detailed descriptions of the types of cookies and choose whether to accept certain cookies while on the site.' (To be implemented)

A4.6 PTUK web site cookie list used

Also, the cookies that the site uses are to enable the site to function effectively. They do not track users.

ASPXANONYMOUS	RequestVerificationToken	dnnSitePanel-SMTP
DOTNETNUKE	atuvc	dnnTabs-dnnHostSettings
LastPageId	eventqueue	dnnTabs-dnnSiteSettings
Panel-Appearance	jsuid	dnn_IsMobile

ClientResourceManagement	authentication	language
SWS Cookie Message	StayInEditMode	
dnnSitePanel-PortalAliases	dnnSitePanel-Appearance	

A4.7 PTUK web site cookie explanations

DotNetNuke uses a number of cookies, the most important of which are the forms authentication cookie (created when a user logs in) and the portalroles cookie, which stores what roles a user has access to in the current portal.

The forms authentication cookie are by default temporary (session) cookies and are not persistent cookies, however users can make them persistent by checking the "remember me" checkbox on the login control. This can be removed via the UI or a setting

The portals role cookie is persistent but it only exists for 1 minute - and it's contents are encrypted as well as containing a portalid to make sure that they only apply for that portal. We use the expiry here as we want to be sure to refresh the users portal roles to pick up any alterations that may have occurred eg if an admin has added the user to new roles. There is no way to disable this in the application currently, but you can create an alternative membership provider and alter the logic as you see fit- the relevant code can be found in `library/httpmodules/membership/membershipmodule.cs` (or `.vb` if using a version prior to 6.0)

Please note, that whilst session cookies are typically preferred as this cookie has a short expiration of 1 minute (to ensure role identification is valid), having it as a session cookie would have a longer lasting cookie (by default of 30 minutes since the last period of activity) so a persistent cookie is a better option in this case.

DotNetNuke can also create a cookie to track affiliates (used to allow sites to track and reward vendor affiliates). Whilst this (little used) function cannot be disabled by a setting, sites that do not allow persistent cookies can safely remove these by editing `default.aspx.cs` (or `.vb`), go in to the `ManageRequest` function and removing the `request.cookies("affiliateid")` block.

Another cookie is used if you choose to install and use the `usersonline` module as it creates cookies to track when an anonymous user logs in so that it does not miscount active users. To avoid this cookie log in as host and go to `host->host` settings and ensure "enable users online" is unchecked (this is the default).

A cookie is created called "language" stores the current language - in a monolingual install this is simply the browser default language, but if the site supports multiple languages then this may be different, based on the language selected by clicking in the languages skin object.

The cookie with the name ".ASPXANONYMOUS" is also created by `asp.net` anonymous authentication. This can be disabled by setting `enabled=false` in the `anonymousIdentification` node in `web.config`.

Using the mobile redirection capabilities (added in 6.1.0 for PE/EE, and 6.1.5 for all editions), two optional cookies may be created. The cookies are called "disablemobileredirect" (which disables redirects when a mobile device is detected) and "disabledirectpresist" sic which stores a cookie with a lifetime of 20 minutes to indicate that redirects are not allowed.

The `DNNPersonalization` cookie is used to store personalization data (such as tab expansion) for anonymous users. Authenticated users personalization data is stored in their profile.

Two cookies in the form "_ContainerSrc" and "_SkinSrc" can be used to read and set the portal specific container and skin - these are both read only cookies.

If you are using the stylesheet widget (or relocation widget or style scrubber widget's which can the stylesheet widget) then two cookies are created StyleSheetWidget_SizeWidget which stores the width, and StyleSheetWidget_TextSizeWidget which stores the text size. These values can then be consumed if you provide alternative stylesheets.

Tabs controls create a cookie to store the last selected tab eg if you visit admin->site settings and click on the "advanced settings" tab it will create a cookie called "dnnTabs-dnnSiteSettings" and store the tabIndex (1). This is read back when the page is revisited and the previously selected tab is then selected.

Panels controls apply a similar logic to tab controls eg if you visit admin->site settings, click on "advanced settings" and expand "security settings" it will create a cookie called "dnnSitePanel-SecuritySettings" and store the value "true". This is read back when the page is revisited and the previously expanded panel is correctly expanded.

Also, because we show youtube videos on the front page the site references the youtube site, however these are embedded using the privacy-enhanced mode.