Policy/Procedure/Guideline

Data Protection Policy

Version no: 1.0

Issue Status: Approved

Date of Ratification: April 2016

Ratified by: Clinical, Governance & Risk Board

Policy Author: Bradley Woods

Policy Owner: CG&RB

Review Frequency: 2 years

Identifiable Document Code: PTUK028

Last Review: April 2020

Next Review: April 2022

POLICY AWARENESS	
People who need to know this policy in detail	**All staff**
People who need to have a broad understanding of this policy	**All staff**
People who need to know this policy exists	**All staff**

CHANGE CONTROL DETAILS			
Date DD/MM/YY	Version	Description	Reason for changes
11/04/2016	1.0	New policy	New policy

Policy location:
Main Policy Folder in Control Room and Crew Room
On PTUK Server

1.0 Introduction

Anyone who obtains personal information ("data") about other individuals is a 'data controller' and is thus regulated by the Data Protection Act 1998. The Act controls what can lawfully be done with information.

It also gives individuals certain rights to control how information about them is obtained, used, stored and distributed. These rights include the right to find out what information a data controller has about them, and ask for copies of data.
We are necessarily a data controller in relation to all the information that we obtain about you as part of the process of providing you with employment.

2.0 Scope

The policy applies to all staff, permanent, part-time, agency or bank staff and all other computer, network or information users authorized by PTUK or any department thereof. It relates to their use of any PTUK owned facilities (and those leased by or rented or on loan to PTUK), centrally managed or otherwise; to all private systems (whether owned, leased, rented or on loan) when connected to the PTUK network; to all PTUK-owned or licensed data and programs (wherever stored); and to all data and programs provided to PTUK by external agencies (wherever stored). The policy also relates to paper files and records created for the purposes of PTUK business.

In order to manage our business we keep records about our employees that necessarily include the following information:

Name	Date of birth
Sex	Address
Next of kin	Sickness record
Disciplinary record	CV
References	Qualifications
Rate of pay	Bank details
Performance record	Appraisals
Criminal records	

3.0 Roles and responsibilities

3.1 Clinical Governance & Risk Board (CG&RB)

The CG&RB is responsible for defining PTUK's Data Protection Policy and for ensuring it is discharged by all clinical and administrative departments and divisions through Heads of Departments.

3.2 Security Working Group

The Security Working Group acts as a focus for technical and other issues relating to information security and data protection within PTUK. It makes recommendations on strategy and policy matters in relation to data protection, and receives reports from the Data Protection Officer.

3.3 Data Protection Officer

The Data Protection Officer has primary responsibility for PTUK's compliance with the DPA. This comprises:

- maintaining PTUK's notification with the Information Commissioner's Office
- is the point of contact and acts as the Caldicott Guardian for patient data
- ensuring completion of the Annual Survey of Personal Data Holdings
- handling subject access requests and requests from third parties for personal data
- promoting and maintaining awareness of the DPA and regulations, including training
- investigating losses and unauthorised disclosures of personal data.

The DPO is PTUK's main contact for the Information Commissioner's Office.

3.4 Heads of Department / Division

Heads of Department / Division are responsible for ensuring their staff understand the role of the data protection principles in their day-to-day work, through induction, training and performance monitoring, and for monitoring compliance within their own areas of responsibility. They should also ensure Data Protection Coordinators are designated for their departments or divisions, and provided with appropriate training and support.

3.5 Data Protection Coordinators

Coordinators are required to:

- advise staff and students in their departments on the implementation of and compliance with this policy and any associated guidance / codes of practice
- ensure appropriate technical and organisational measures are taken within their departments to ensure against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- support PTUK's notification with the Information Commissioner's Office by maintaining the register of holdings of personal data, including databases and relevant filing systems, and the purposes af processing
- keep the Data Protection Officer informed of changes in the collection, use, and security of personal data within their department
- report any loss of personal data to the Head of Department / Division and the Data Protection Officer

- ensure the proper completion of applications for the data protection registration of new research projects before they are submitted to the Records Office
- confirm compliance with the PCI Data Security Standard in relation to the records of credit card payments made through the department.

3.6 **Data Owner**

Data Owners are responsible for:

- establishing and monitoring measures, in accordance with this policy and the information security policy, to protect any holdings of personal data for which they are responsible
- ensuring that those holdings are registered as part of the annual survey of personal data holdings

- ensuring that any transfer of personal data to third parties is authorised, lawful and uses appropriate safe transport mechanisms such as encryption.
- authorising the downloading of electronic personal data on to portable devices or the removal of manual personal data from PTUK premises
- informing their departmental Data Protection Coordinator when new holdings of personal data are established or when the purposes of processing change.

3.7 **Data Custodians**

Data Custodians should ensure that their processing of personal data is compatible with the data protection principles, including the security and integrity of data sets.

3.8 **Data Processors**

Data processors have a contractual responsibility to act only on PTUK's instructions and to ensure that their processing of personal data provided by PTUK is carried out in compliance with this policy and in accordance with the eight data protection principles. There should be a written agreement with data processors which adequately addresses these responsibilities.

3.9 **Staff**

All staff are responsible for:

- ensuring that their processing of personal data, including research data, in all formats (e.g. electronic, microfiche, paper, etc.) is compatible with the data protection principles
- raising any concerns in respect of the processing of personal data with the Data Protection Officer
- promptly passing on to the Data Protection Officer all subject access requests and requests from third parties for personal data

- reporting losses or unauthorised disclosures of personal data to the Data Protection Coordinator.

In order that PTUK can continue to comply with the fourth data protection principle, staff should ensure the personal data they provide about themselves is up to date.

4.0 Data Requirement-Personal

It is a requirement under the Act that you consent to our processing data about you. Some data is referred to in the Act as "sensitive personal data". This means personal data consisting of information as to:

- the racial or ethnic origin of the data subject,
- his political opinions,
- his religious beliefs or other beliefs of a similar nature,
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- his physical or mental health or condition,
- his sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

In your contract of employment you expressly consent to our processing data including sensitive personal data about you. With this consent it is lawful for us to process data in order to keep the records about your employment necessary for us to meet the needs of running our business.

Below is a summary of the legal obligations imposed upon us and the rights that you have under the Data Protection Act 1998 together with our policies about those rights and obligations. The Act contains transition periods under which its terms become fully effective over a period of years, however our policy assumes that the Act is fully in force.

4.1 **Our obligations**

The principles for processing of personal data are that data must be:

1. fairly and lawfully processed;
2. processed for limited purposes;
3. adequate, relevant and not excessive;
4. accurate;
5. not kept longer than necessary;
6. processed in accordance with the data subject's rights;
7. secure;
8. not transferred to countries without adequate protection.

We are committed to following these principles and that is why your consent has been obtained so that all our data processing in relation to data of which you are the subject is lawful.

We will process data about you only so far as is necessary for the purpose of managing our business. Data will not be disclosed to anyone else other than our authorised employees, agents, contractors or advisors (except as required by law) unless you expressly authorise its disclosure. We will only obtain data about you that we require for the purpose of managing our business and dealing with you as an employee of that business.

We will take all reasonable steps to ensure that the data we process is accurate. Data will be retained as necessary during the course of your employment and records will be retained for up to six years after the data that you leave the employment in case legal proceedings arise during that period. Data will only be retained for a period of longer than six years if it is material to legal proceedings or should otherwise be retained in our interests after that period.

We will process data in accordance with your rights under the Act.

Data will be kept in a secure system whether manual or computerised to the best of our ability at all times.

The Act prohibits the transfer of data outside the European Economic area to countries that do not have similar protection of data except in some circumstances or with the subject's consent. You have given us your consent to such transfers should they be necessary under your contract of employment. The reason for this is that with the use of the Internet and email data can be transferred to a computer or server in such a country in the course of a transfer between parties within the European Economic area. Also we may have offices or subsidiary companies or agents or contractors in such countries now or in the future and therefore transfers of data could be necessary as part of the management of our business and the performance of your contract of employment.

PTUK uses the ACCESS AWARE toolkit as prompts for all staff who either process or request data. A copy of which is contained in Appendix 1.

5.0 Your rights under the Act

The Act gives you the following rights as a data subject:

- Access to data

- To be told whether personal data on you is being processed by requesting this in writing and paying a fee currently not to exceed £10.00.

- To be given a description of the data and its recipients and to have a copy of the data within 40 days of the request.

Confidential references given by the employer are excluded from disclosure (but not necessarily references given to the employer). The data subject is entitled to know the source of the data.

The copy should be intelligible and in a permanent form unless to provide it in this form is impossible or would involve disproportionate effort or you agree to accept a non-permanent 'copy'.

If the data controller has previously complied with a request from you then no duty to comply with the request arises until a "reasonable interval" has elapsed between the two. Just what will constitute a "reasonable interval" will depend on the nature of the data, why it is processed and the frequency with which it alters.

To be informed about the logic used to make automated decisions using the data. For example some employers will scan CV's submitted for certain information in order to select candidates for further consideration and this right would entitle the candidate to know what the criteria used was unless this would necessitate divulgence of a trade secret.

The request for access to data must be made in writing if the data controller so requires. The Data controller may also require payment of a fee not exceeding the statutory maximum which is currently £10.00.The data subject must provide the data controller with any information reasonably requested to enable the data controller to be satisfied as to the data subject's identity and in order to locate the information.
Where disclosure of data would necessarily mean that information relating to a third party would be disclosed the data controller may refuse to disclose it unless the third party consents or it is reasonable to disclose the information without such consent.

5.1 **Rectification of data**

You can apply to a court for an order that the data controller rectify, block, erase or destroy inaccurate data and where the court considers it reasonably practicable to do so inform third parties to whom the data has been disclosed of the fact

5.2 **Compensation**

Should you suffer damage as a result of the failure of a data controller to comply with the Act then you may be awarded compensation. Where a data subject suffers distress in certain types of case there may also be an award of compensation for distress as well as damage.

It is a defence in any claim for compensation that the data controller used such care as was reasonably required in all the circumstances to comply with the Act.

6.0 Information

The Act provides that Data will not be fairly processed unless the data controller ensures that as far as reasonably practicable the data subject has or has ready access to:

- The identity of the data controller
- Any representative of the data controller
- The purpose(s) for which the data is intended to be processed
- Any other information necessary to enable the processing to be fair
- We have incorporated this information in of your contract of employment or otherwise given you a notice containing this information (including this policy).

However any data subject whose employer has not notified the Office of the Information Controller that he is a data controller and had these details entered in the public register is entitled to be given (within 21 days of making a written request) "relevant particulars" which are:

- The data controller's name and address;
- The name and address of any representative of the data controller;
- a description of the personal data being or to be processed and the category of data subjects to which they relate;
- a description of the intended purpose of the processing;
- a description of the intended recipients of the data ;
- a list of the countries outside the European Economic area that will or may be in receipt of the data from the data controller.

6.1 Direct Marketing

A data subject has the right to require in writing that the data controller within a reasonable time cease or not begin processing data of which he is the subject for the purpose of direct marketing. Failure to comply by the data controller can lead to a court order that he does so.

6.2 Right to stop data processing

A data subject has the right to require that a data controller cease or not begin data processing where the processing is causing or likely to cause unwarranted and substantial damage or unwarranted and substantial distress to the data subject or another by giving notice in writing specifying why the data processing is or will be the cause of distress or damage and the purpose and manner of processing to which

objection is made. The data controller then has 21 days to respond with a written notice stating either that he has or intends to comply with the request or why he regards the notice as unjustified and the extent to which he has or intends to comply with it. The data subject can make an application to the court if the data controller will not comply. However where the data subject has consented to the data processing or it is necessary for the performance of a contract to which he is a party he requests it with a view to entering a contract or the data controller has a non contractual legal obligation which requires him to carry it out, the data subject has no right under this section to stop the data processing.

7.0 Definitions

7.1 Personal Data

”Personal data” means data which relate to a living individual who can be identified:

- from those data, or
- 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

7.2 Sensitive personal data

Information about:

- the racial or ethnic origin of data subjects
- their political opinions
- their religious beliefs or other beliefs of a similar nature
- whether they are members of a trade union

- their physical or mental health or condition
- their sexual life
- the commission or alleged commission by them of any offence, and any proceedings for such offences.

Although the DPA does not define ‘health’, the term should be understood broadly, to include preventative medicine, medical diagnosis, DNA sequences, medical research, provision of care and treatment and the management of healthcare services.

Personal demographic data, such as personal addresses and financial data (including salaries) are not sensitive personal data, but should be treated with similar care.

7.3 Manual Personal Data

Personal data recorded as part of a relevant filing system in paper or other non-electronic format.

7.4 **Processing**

Obtaining, recording or holding personal data. This includes organisation, adaptation or alteration; retrieval, consultation or use; disclosure; and alignment, combination, blocking, erasure or destruction.

7.5 **Relevant Filing System**

Manual personal data structured by reference to individuals in such a way that information relating to a particular individual is readily accessible.

7.6 **Data Holding**

A collection of one or more data sets or files that are being processed for permitted purposes under the direction of a clearly identified member of PTUK staff - the Data Owner.

7.7 **Data Controller**

As the organisation which determines the purposes of the processing, PTUK is the Data Controller for the personal data that it manages.

7.8 **Data Protection Officer**

The PTUK member of staff with lead responsibility for PTUK's compliance with the DPA.

7.9 **Data Owner**

The PTUK member of staff with lead responsibility for permitting and managing the retention and processing of a data holding for which PTUK is the Data Controller. Data Owners delegate responsibility for personal data elements to Data Custodians.

7.10 **Data Custodian**

The individual unit or person identified by the data owner to be responsible for the collection, creation, modification and deletion of specified personal data element(s).

7.11 **System Custodian**

A person appointed by a Head of Department or Division with responsibility and authority to implement the Information Security Policy and supporting policies in respect of a PTUK-wide or departmental system, to ensure that the security measures adopted for systems under his/her control meet the requirements of these policies and to carry out the duties as set out in the associated Codes of Practice. In the case of a large system some duties may be delegated, to named persons whose particular duties are set out in writing, although the Custodian retains overall responsibility for the security of that system.

7.12 **Data Subject**

A living individual who is the subject of personal data

7.13 **Data Processor**

Any third party (other than PTUK staff) who processes personal data on behalf of and on the instructions of the Data Controller.

8.0 Monitoring, Measuring and Review

The system custodian is responsible for the continued monitoring of information requests received. A report is made on bi-annual basis and submitted to the Clinical, Governance & Risk Board for review.

8.0 References

Trade Union and Labour Relations Act 1992

Data Protection Act 1998

Information Commissioners Office
www.ico.org.uk/for_organisations/training/access-aware-toolkit

9.0 Appendices

Appendix 1
Appendix 2
Appendix 3

Appendix 1 – Subject access requests – a guide through the process

Is this a subject access request?
Key points to consider:
• Any written enquiry that asks for information you hold about the person making the request can be construed as a subject access request, but in many cases there will be no need to treat it as such.

• Would you usually deal with the request in the normal course of business? If so, do so – promptly.

• If you are in any doubt how to respond, go back to the individual or their representative and clarify the situation.

Do you have enough information to be sure of the requester's identity?

Key points to consider:
• Often you will have no reason to doubt a person's identity.

• If a person with whom you have regular contact sends a letter from their known address it may be safe to assume that they are who they say they are.

• If you have good cause to doubt the requester's identity you can ask them to provide any evidence you reasonably need to confirm it.

Do you need any other information to find the records they want?
Key points to consider:

• You will need to ask the individual promptly for any other information you reasonably need to find the records they want.

• You might want to ask them to narrow down their request.
For example, if you keep all your customers' information on one computer system and your suppliers' information on another, you could ask what relationship they had with you. Or, you couldask when they had dealings with you.

• You have 40 calendar days to respond to a subject access request after receiving any further information you need and any fee you decide to charge.

Do you hold any information about the person?

Key points to consider:

• If you hold no personal information at all about the individual you must tell them this.

• Remember, if you outsource data processing, subject access requests may be sent to a third party. Make sure suppliers are fully aware of their obligations and are trained in handling requests.

Are you going to charge a fee?

Key points to consider:

• If you need a fee you must ask The individual promptly for one. The maximum you can charge is £10 unless medical or education records are involved.

• The 40 calendar days in which you must respond starts when you have received the fee and all necessary information to help you find the records.

Will the information be changed between receiving the request and sending the response?

Key points to consider:
• You can still make routine amendments and deletions to personal information after receiving a request. However, you must not make any changes to the records as a result of receiving the request, even if you find inaccurate or embarrassing information on the record.

Does it include any complex terms or codes?

Key points to consider:
• The information you hold may include abbreviations, codes or technical terms that the individual will not understand. You must make sure that these are explained so the information can be understood.

Does it include any information about other people?

Key points to consider:

• You will not have to supply the information unless the other people mentioned have given their consent, or it is reasonable to supply the information without their consent.

• Even when the other person's information should not be disclosed, you should still supply as much as possible by editing the references to other people. Visit www.ico.gov.uk for more detailed guidance

Are you obliged to supply the information?

Key points to consider:

• There may be circumstances in which you are not obliged to supply certain information.
Visit www.ico.gov.uk for further information regarding exemptions.

• If all the information you hold about the requester is exempt, then you can reply stating that you do not hold any of their personal information that you are required to reveal.

Prepare the response

Key points to consider:

• A copy of the information should be supplied in a permanent form except where the individual agrees or where it is impossible or would involve undue effort. This could include very significant cost or time taken to provide the information in hard copy form.

• An alternative would be to allow the individual to view the information on screen.

For more detailed guidance on responding to subject access requests, visit www.ico.gov.uk or call the ICO helpline on 0303 123 1113.

Appendix 2 - Equality Impact Assessment Tool

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
	Does the policy/guidance affect one group less or more favourably than another on the basis of:		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
	• Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	No	
4.	**Is the impact of the policy/guidance likely to be negative?**	No	
5.	**If so can the impact be avoided?**	N/A	
6.	**What alternatives are there to achieving the policy/guidance without the impact?**	N/A	
7.	**Can we reduce the impact by taking different action?**	N/A	

If you have identified a potential discriminatory impact of this procedural document, please refer it to Human Resources, together with any suggestions as to the action required to avoid/reduce this impact.

Appendix 3 - Checklist for the Review and Approval of Procedural Document

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

	Title of document being reviewed:	Yes/No/ Unsure	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Is the method described in brief?	Yes	
	Are people involved in the development identified?	Yes	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are the references cited in full?	Yes	
	Are supporting documents referenced?	Yes	
6.	**Approval**		

	Title of document being reviewed:	Yes/No/ Unsure	Comments
	Does the document identify which committee/group will approve it?	Yes	
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	Yes	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	Yes	
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8.	**Document Control**		
	Does the document identify where it will be held?	Yes	
	Have archiving arrangements for superseded documents been addressed?	Yes	
9.	**Process to Monitor Compliance and Effectiveness**		
	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	No	
	Is there a plan to review or audit compliance with the document?	Yes	
10.	**Review Date**		
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so is it acceptable?	Yes	
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	Yes	

Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name	Bradley Woods	Date	18.04.2020
Signature			
Committee Approval			
If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name	William Corbett	Date	18.04.2020
Signature