Confidentiality, Data Protection & Caldicott Policy

Version	v3.3
Supersedes:	v2.0
Date Ratified by Board:	26.01.2017
Reference Number:	PC24POL1
Title & Department of originator:	Governance Manager, Quality & Patient Safety
Title of responsible committee/department:	Quality & Patient Safety
Effective Date:	24.01.2017
Next Review date:	November 2020 (or when there is a change in Policy)
Target audience:	All PC24 staff or staff working on behalf of PC24
Impact Assessment Date:	05.01.2017
Summary	This policy provides the framework to ensure that PC24 complies with the requirements of the General Data Protection Regulations, Caldicott Principles, the NHS Code of Confidentiality and the Common Law Duty of Confidentiality.

Version	Date	Control Reason	Title of Accountable Person for this Version
v3.0	November 2016	Calidicott policy combined in the Confidentiality & Date Protection Policy. Renamed Policy to include the PC24 Caldicott Policy and Data Protection Impact Assessment.	Governance Administrator & editing by Information Governance Lead.
v3.1	July 2018	Update for GDPR	Data Protection Officer/IG lead
v3.2	November 2019	Update to reflect new IT suite of policies New Appendix 3 to be developed	Data Protection Officer/IG lead
V3.3	Feb 2021	Review to reflect changes in personnel and to check for location specific references in preparation for new OoH contract	DPO/IG lead

Reference Documents	Electronic Locations (Controlled Copy)	Location for Hard Copies
See Sections 16 & 17	Urgent Care 24 Intranet/Policy Documents & Guidance/IG Policies	**Policy File, Wavertree Headquarters**
Consultation: Committees / Groups / Individual		**Date**

SMT, IG Steering Group, Policy Group, Quality & Workforce and Board.	**26.01.2017**

CONTENTS **Page**

1 PURPOSE

This policy provides the framework to ensure that Primary Care 24 (PC24) complies with the requirements of the General Data Protection Regulations (GDPR), Caldicott Principles, the NHS Code of Confidentiality, the Common Law Duty of Confidentiality and its responsibilities in relation to data quality.

2 OBJECTIVES

The objectives of this policy are:

- To ensure any person identifiable data collected and held by PC24 is processed fairly and lawfully and in accordance with the GDPR
- To promote best practice in the processing of person identifiable data
- To ensure that PC24 staff involved in processing person identifiable data understand their responsibilities and obligations
- To ensure that PC24 staff responsible for the processing of person identifiable data are adequately trained to fulfil their responsibilities and obligations
- To ensure the quality of PC24 data in order to promote effective decision making, patient safety, good business management and use of resources for the benefit of patients and staff in line with the organisation's values
- To outline the procedure for reporting and investigation of a suspected breach of Confidentiality and/or Data Protection
- To provide assurance to our patients, staff and others with whom we deal that their person identifiable data is processed lawfully and correctly and held securely at all times

3 SCOPE

The Policy applies to all PC24's employees, Associate GPs, Agency GPs, contractors, suppliers and directors. In this policy reference to PC24 staff includes all those listed here.

PC24 is responsible for its own records under the terms of the GDPR and it has submitted itself as a Data Controller to the Information Commissioner.

This policy covers all identifiable information created, processed and stored by PC24 in any medium on living individuals, patients or staff. Throughout this document, the term 'patient' is used to refer to an individual who has received or is receiving treatment/care from a PC24 service, and this term includes those people who are also known as 'service users', 'clients' and 'carers'.

Although GDPR do not apply to deceased persons, where possible the same level of confidentiality should be provided to the records and information relating to a deceased person as to one who is alive. The issues arising from the processing and provision of access to deceased persons' records can be complex and where these arise advice should be sought from the PC24 Caldicott Guardian or Data Protection Officer.

This policy covers all aspects of information within the organisation, including (but not limited to):

- Patient/staff/service user/carer information
- Person identifiable data
- Organisational information

This policy covers all aspects of handling information, including (but not limited to):

- Structured and unstructured record systems – paper and electronic
- Transmission of information – fax, email, post and telephone
- Information systems managed and/or developed by, or used by PC24

This policy covers all information systems purchased, developed and managed by, or on behalf of, PC24 and any individual, directly or otherwise engaged by the organisation.

4 INTRODUCTION

PC24 is required to meet its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within this policy are primarily based upon the GDPR and the NHS Code of Practice: Confidentiality (Code of Confidentiality). These are two key standards which cover the security and confidentiality of person identifiable data within the NHS, United Kingdom and the European Economic Area.

A definition of person identifiable data and sensitive data is included as **Appendix 1** in this policy.

PC24 holds and processes information about its employees, patients and other individuals for various purposes (e.g. the effective provision of healthcare services or; for administrative purposes such as payroll). To comply with the GDPR, personal identifiable information must be collected and used fairly, stored safely and not disclosed to unauthorised persons. The GDPR and the NHS Code of Confidentiality apply to both manual and electronic data.

This document also mandates the use of Data Protection Impact Assessments (DPIAs), which are to be used to ensure that any new or amended policy, processes, procedure, or activity that involves the use of person identifiable data or sensitive data, is appropriately assessed to establish and record how this impacts on the data subjects and to recommend appropriate action to mitigate this impact. **See Appendix 3.**

DPIAs are now mandatory in England for any new system (IT or otherwise), process, project, policy or technology which involves the processing of personal and/or sensitive data.
PC24 also has a duty to comply with additional guidance issued by the Department of Health and other professional bodies. All PC24 staff have a duty of confidence to patients and colleagues under common law.

The failure of PC24, and or PC24 staff to comply with GDPR could result in a subsequent investigation by the Information Commissioner's Office, with the possible risk of being fined.

Compliance with the policy will provide assurance to PC24 and to individuals that all personal and sensitive data processed by PC24 is dealt with legally, securely, effectively and efficiently, in order to deliver the best possible care to patients.

Compliance will also ensure the quality of data used across the organisation is sufficient to support:

1. Efficient delivery of patient care
2. Robust clinical governance processes
3. Good financial management
4. Performance measurement
5. The review of clinical standards and practice
6. Continuing improvement.

PC24 will establish and maintain policies and procedures to ensure compliance with the requirements contained in the Department of Health Data Protection & Security Toolkit (DPST).

5 DEFINITIONS

Data is any information used to support the functions of PC24, including information relating to patients, carers, employees, including bank, agency, locum or voluntary staff, and other business information. Further information with regard to person identifiable data and sensitive data is set out in **Appendix 1** to this policy.

Data Quality is the assurance that data is fit for its intended use and complies with the Data Quality Standards set out in the PC24 Records Management Policy.

Information Assets are defined within the DPST as operating systems, infrastructure, business applications, off-the-shelf products, services, user-developed applications,

records (including paper records) and information. Therefore any reference to information assets includes any method of recording data.

The **General Data Protection Regulations (GDPR)** provide controls on the handling of personal identifiable information for all living individuals. Central to the GDPR is compliance with the six stated principles, designed to protect the rights of individuals about whom personal data is processed whether through a paper or an electronic record, and the duty of accountability for adherence to those principles.

The **Access to Health Records Act 1990** deals with the management and disclosure of health records for deceased patients. The personal representative of a deceased or a person who might have a claim arising from the patient's death can apply for access to a patient's records under this legislation.

The **Caldicott Report 1997 and The Information Governance Review 2013** provide guidance to the NHS and providers of NHS funded care on the use and protection of personal confidential data and sets out the need for controls over the availability of such information and access to it. They make recommendations which are the foundation for the requirement on all NHS organisations and providers of NHS funded care to appoint a Caldicott Guardian who is responsible for compliance with the seven Caldicott confidentiality principles.

The **Common Law Duty of Confidentiality** prohibits use and disclosure of information provided in confidence unless there is a statutory requirement or court order to do so. Where there are no statutory restrictions on disclosure of information, such information may be disclosed only for purposes about which the subject has been informed and the consent of the subject is required. This duty is not absolute, but should only be overridden if the holder of the information can justify that disclosure is in the public interest, for example, to protect the vital interests of the data subjects or another person, or for the prevention or detection of a serious crime.

6 RESPONSIBILITIES & DUTIES

6.1 PC24 has structures in place to deliver information governance to meet its Caldicott, data protection, confidentiality and data quality requirements.

6.2 The Chief Executive

The Chief Executive had responsibility, as the Accountable Officer, for compliance with the GDPR and data quality standards within PC24. This responsibility has been delegated to the Senior Risk Information Owner (SIRO).

6.3 Data Protection Officer (DPO)

The Company Secretary is the Data Protection Officer and has specific responsibilities set out in Article 39 of the GDPR as follows:

- To inform and advise PC24 and its employees about the obligations to comply with GDPR and other data protection laws
- To monitor compliance with GDPR and other data protection laws, and with the organisation's data protection policies, including:
  - Managing internal data protection activities
  - Raising awareness of data protection issues
  - Training staff
  - Conducting internal audits
- To advise on, and to monitor Data Protection Impact Assessments (DPIAs)
- To cooperate with the ICO as the supervisory authority and
- To be the first point of contact for the ICO and data subjects.

In performing that role the DPO will

- Report to the Board
- Be given independence to perform their tasks
- Take account of the risk associated with the various forms of data processing being undertaken, having regard to the nature, scope, data quality, context and purpose of the processing
- Prioritise and focus on the more risky activities, such as the processing of special category data or processes where the impact on individuals could be damaging.

6.4 Senior Information Risk Owner (SIRO)

The Director of Service Delivery is the PC24 SIRO. The responsibilities of this role are:

- To ensure that PC24 achieves monitors and embeds a culture of good information governance, across the organisation and with its business partners
- To work closely with the DPO, IG Lead and Caldicott Guardian
- To attend and Chair the Information Technology and Information Governance Steering Group
- To complete appropriate specialist training for this role
- To understand the organisation's business goals with particular emphasis on the use of, and dependency upon internal and external information assets
- To ensure that there is effective monitoring of data quality within PC24
- To ensure that there is an up to date Information Asset Register
- To ensure PC24's Information Asset Owners (IAOs) understand their role
- To initiate and oversee an information risk awareness/training programme and to communicate the importance and maintain impetus on identifying and managing information risk
- To ensure that any issues identified in relation to data protection matters or data quality are addressed
- To ensure that good information governance assurance practice is shared within PC24 and to learn from good practice developed and practiced within the NHS locally and nationally.

6.5 Caldicott Guardian

This role is undertaken by the Medical Director. The Caldicott Guardian is responsible for agreeing and reviewing processes and procedures governing the transfer and disclosure of personal confidential data within PC24 and with external agencies. They will:

- Develop and maintain knowledge of confidentiality and data protection matters and act as the organisational expert on confidentiality
- Ensure the Caldicott work plan is incorporated into the programme of work managed through the Information Security and Information Governance Steering Group

- Ensure that the Caldicott principles are appropriately reflected in organisational strategies, policies and working practices for staff
- Undertake appropriate specialist training for their role
- Meet regularly with the SIRO and IG Lead, attending the Information Technology and Information Governance Steering Group
- Be the first point contact within PC24 for data protection and Caldicott issues
- Work closely with the IG Lead when information owned by PC24 needs to be transmitted to an external agency
- Ensure adequate governance over the issuing of Smartcards by the Registration Authority
- Oversee patient information audit.

6.6 Information Governance Lead (IG Lead)

The Company Secretary is the Information Governance lead and is responsible for overseeing completion of the DSPT, including those elements pertaining to confidentiality and data protection.

The IG Lead will:

- Lead the co-ordination and implementation of the Data Protection, Confidentiality and Data Quality work programme
- Attend the Information Technology and Information Governance Steering Group
- Monitor and ensure PC24's compliance with the principles contained within the GDPR, Caldicott Report, Confidentiality: NHS Code Of Practice and local processes for monitoring data quality
- Oversee the provision of adequate training and awareness of all staff in relation to their responsibilities for Data Protection, Confidentiality and Data Quality, including specialist training in relation to their role as IG Lead
- Ensure that Information Asset Owners are identified, are aware of their areas of responsibility and attend meetings as required.

6.6 Information Technology and Information Governance Steering Group

The Information Technology and Information Governance Steering Group (ITIGSG) is chaired by the SIRO. The group is responsible for:

- Ensuring that PC24 complies with the GDPR, ongoing NHS guidance and mandatory requirements in relation to information technology, information security and information governance
- Ensuring that PC24 complies with its obligations in relation to the Data Security & Protection Toolkit (DSP Toolkit) and that information to support the submission is appropriately captured
- Developing and monitoring action plans relating to information technology and security identified by the Penetration Test process or any one off audit or review process
- Progressing and embedding information governance processes at PC24
- Allocating actions and work streams to the appropriate personnel
- Developing and monitoring action plans supporting the DSP Toolkit and the development of good practice at PC24
- Ensuring all staff receive training in IG appropriate to their roles and responsibilities
- Discussing matters of concern in relation to information technology, security and governance
- Keeping the relevant policies and Standard Operating Procedures, including this policy, under review
- Monitoring the outcomes of Information Asset Risk assessments, audits and other review processes set out in PC24's policies and SOPs.

6.7 All Managers

All managers are responsible for ensuring compliance with policies, that their staff successfully undertake annual mandatory IG training and that incidents, including those with IG implications, are promptly and properly recorded through the Datix system.

6.8 Information Asset Owners

IAO's are Data Custodians and are responsible for ensuring that the data protection and Caldicott Principles are fully observed and complied with by staff within their department or Service Delivery Unit (SDU). IAOs are required to ensure that all data flows and processing of data, for which they are responsible, complies with PC24 Information Governance policies. To this end they will:

- Promote Data Protection and Caldicott Principles on an on-going basis, including posters, articles and local briefings
- Support managers with local induction for new starters and temporary staff to ensure they are given instruction on the Data Protection and Caldicott principles as part of their first week/day
- Ensure all staff know the procedure for reporting IG and IT security incidents
- Be the lead individuals for the completion of their particular aspects of the IG Toolkit
- Attend meetings of the Information Technology and Information Governance Steering Group as invited

Information Asset Administrators will provide support to the IAOs.

6.9 Head of IT

The IT Manager has a particular role in respect of the interface between Information Management & Technology, and the information handled and stored by PC24. The Head of IT will:

- Provide an advisory service to the IGITSG and the IT team
- Monitor and report on the state of Information Management & Technology security within the organisation
- Undertake risk assessments in relation to the information assets for which they have responsibility
- Ensure that information systems are fit for purpose and comply NHS Guidelines and best practice in relation to Data Quality and Governance
- Ensure the Information Security Policy and all Information Technology policies are maintained, up to date and implemented throughout the organisation

- Support the delivery of training in relation to the use of information assets
- Lead on issues with regard to Cyber Security
- Be the lead individual for the completion of the relevant aspects of the DSPT
- Attend the IGITSG.

6.10 Responsibilities of all PC24 staff

- Everyone working in the NHS has a legal duty to keep information about patients, clients and other individuals such as staff or volunteers confidential, and to protect the privacy of individuals. They are required to adhere to confidentiality agreements i.e. common-law of confidentiality, contract of employment, NHS Confidentiality Code of Practice
- PC24 places the utmost importance upon patient confidentiality and data quality
- PC24's patient confidentiality guidance is governed by the NHS Caldicott rules.
- All PC24 staff and visitors are required to sign a confidentiality agreement on commencement of employment with PC24 or on visiting the premises
- In the course of their work PC24 staff may be called upon to handle and process patient-identifiable information whether it is stored on paper or on computer. They are responsible for safeguarding the confidentiality of all personal and corporate information, transmitted or recorded by any means. Such information must not be disclosed, except to authorised personnel.
- All PC24 staff are responsible for the quality of the data they collect and record whether they are in a clinical, technical, clerical or corporate role.
- All notes, memoranda, records and other material in permanent form made or created by PC24 staff relating to the business of PC24 in pursuance of their duties (including all copies) shall be and remain the property of PC24 and must be handed over on demand and in any event at the end of the employment, term of office or contracting relationship
- PC24 staff must not at any time, either during employment, term of office or contracting relationship, or afterwards, use, or divulge to any person, firm or company, except in the proper course of their duties, confidential information relating to the business of any patient or customer of PC24 which may have come to their knowledge as a result of their relationship with PC24

- PC24 staff must not use or divulge any information, relating to or concerning PC24, details of patients, general practitioners, or suppliers of PC24, or any computer programmes and related manuals or documentation, the intellectual property rights of which belong to PC24, or the prices charged or quoted by any such suppliers which they may possess or which may come to their knowledge
- PC24 staff must keep confidential all information entrusted to them which they know, or ought reasonably to know, to be confidential or secret, and not use or attempt to use any such information which they know, or ought reasonably to know, to be confidential or secret, in any manner which may injure or cause loss either directly or indirectly to PC24 or its patients, or may be likely to do so. This restriction will continue to apply at the end of the formal relationship with PC24, save to the extent that any such confidential information shall have come into the public domain.

7 DATA PROTECTION ACT 2018

7.1 Data Protection Act 2018 – Principles and Practices to ensure compliance

The lawful and correct processing of person identifiable data by PC24 is important to successful business operations and to maintaining confidence between PC24 and its patients, staff and others whom we deal with.

Under Article 5(2) of the GDPR, as a data controller, PC24 will be responsible for, and must be able to demonstrate, compliance with the six principles set out in Article 5 (1):

Principle 1 – Lawfulness, fairness and transparency

All personal data shall be processed lawfully, fairly and in a transparent manner in accordance with Principle 1 of the GDPR. Furthermore, PC24 staff are expected to adhere to guidance provided in the Caldicott Report, the Confidentiality: NHS Code of Practice and this policy.

Therefore all staff must:

- have legitimate grounds for collecting and using the personal data

- not use the data in ways that have unjustified adverse effects on the individuals concerned
- be transparent about how data will be used, and give individuals appropriate privacy notices when collecting their personal data
- handle people's personal data only in ways they would reasonably expect and;
- make sure nothing unlawful is done with the data.

Processing is defined as "obtaining, recording or holding information or data, or carrying out any operations or set of operations on the information or data, including (any of the following):

- Organisation, adaptation or alteration of the information or data
- Retrieval, consultation or use of the information or data
- Disclosure of the information or data by transmission, dissemination or otherwise making available"

All PC24 staff must comply with the common law duty of confidentiality: that any person identifiable data given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the individual.

However, research, which includes statistical and historical studies, can be undertaken within lawful processing under GDPR (see Principle 2 below) provided that:

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

If these safeguards are met, then the following exemptions apply:

- personal data can be used for research even if it were not originally obtained for that purpose;
- the data can be retained indefinitely; and
- subject access rights do not apply if the research results are not made public in a form which identifies the research subjects.

The six principles still apply to research data (except data for "historical research").

Principle 2 – Purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes: further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes. The following therefore apply:

- Only the minimum amount of identifiable information required to fulfil the purpose of collection should be recorded and collected. It should be made clear to patients why information is being collected and for what purpose it will be used.
- Personal data that is transferred must only be used for the purpose for which it was originally obtained.

Principle 3 – Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which processing takes place. In practice, this means that PC24 and PC24 staff should ensure that:

- PC24 holds personal data about an individual that is sufficient for the purpose for which it is held in relation to that individual; and
- No more information is held than is needed for that purpose.

This will be monitored by:

- Conducting routine audits as part of good data quality management practice
- Ensuring that relevant records, policies and professional guidelines i.e. information lifecycle, are adhered to.

Principle 4 – Accuracy

Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having

regard to the purposes for which they are processed, are erased or rectified without delay. To comply with these provisions PC24 staff should:

- Take every reasonable step to ensure the accuracy of any personal data obtained, having regard to the purpose(s) for which it has been collected
- Ensure the source of data provided is clear
- Record information accurately
- Regularly check systems to erase or rectify information which is inaccurate or out-of-date without delay.

Principle 5 – Storage limitation

Personal Data must be kept in a form which permits identification of data subjects for no longer than necessary for the purpose for which it is processed; personal data may be stored for longer periods where it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
To comply with these provisions PC24 staff should:

- Adhere to the PC24 Records Management Policy (i.e. information lifecycle)
- Comply with the Department of Health's Records Management: NHS Code of Practice, Part 2 of which provides a comprehensive retention schedule, which is reflected in the PC24 Records Policy.

Principle 6 – Integrity and confidentiality

Personal data must processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In practice, this requires appropriate physical and cyber security to prevent personal data being accidentally or deliberately compromised. In particular, the PC24 Information Security Policy must provide:

- Security which is designed and organised to fit the nature of the personal data held and recognises the harm that may result from a security breach
- Clarity about who is responsible for ensuring information security
- Appropriate control on access to information
- Assurance that PC24 has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff
- A swift and effective system for responding to any breach of security swiftly and effectively.

In addition, PC24 must have an appropriate mobile device policy in place to ensure the physical security of personal data away from its premises.

Any transfer of identifiable information must be carried out securely and with an adequate level of protection given to the data in transit in accordance with current NHS information security standards. In most cases this will require data transferred on portable media or electronically to be encrypted during transit.

In addition to the six principles set out in Article 5 of the GDPR, PC24 should ensure that personal data is not transferred to a country outside the European Economic Area unless that country can ensure an adequate level of protection. In practice, PC24 does not transfer personal or patient identifiable information outside the United Kingdom.

Personal data must be processed in accordance with the rights of the individual

Article 12 of the GDPR sets out the rights of data subjects:

Right 1. The right to be informed.
This encompasses PC24's obligation to provide 'fair processing information' through its privacy notice.

Right 2. The right of access
This sets out the right of a data subject to obtain: confirmation that their data is being processed, access to their personal data and the

information provided in the privacy notice. PC24's process for dealing with such requests is set out in its Standard Operating Procedures. In certain circumstances such a request can be refused, especially where a request is excessive and/or repetitive.

Right 3. The right to rectification

Individuals are entitled to have their personal data rectified if it is inaccurate or incomplete.

Right 4. The right to erasure

The principle underlying this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. There are circumstances within which such a request can be refused.

Right 5. The right to restrict processing

This right restricts processing of personal data, though it can still be stored as long as further processing does not take place. Sufficient information can be retained to ensure that the processing restriction is honoured in the future.

Right 6. The right to data portability

The right to portability allows an individual to obtain and reuse their personal data across different services, particularly to transfer it from one IT environment to another safely and securely.

Right 7. The right to object

An individual has the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling) and
- Processing for the purpose of scientific/historical research and statistics.

Specific restrictions/conditions apply to this right.

Right 8. Rights in relation to automated decision making and profiling

This right provides a safeguard against the risk that a potentially damaging decision is taken without human intervention.

PC24's Subject Access Request Standard Operating Procedures (IG405 & 406) detail the process to be followed to manage a Subject Access Request.

7.2 Data Protection Impact Assessment

Data Protection Impact Assessment (DPIA) is a methodology to identify, assess, mitigate or avoid privacy risks. When changes are proposed, a DPIA should be completed to assess whether those changes give rise to privacy risks.

The DPIA process complies with the Data Protection Act 2018 and the GDPR. A checklist designed for use by staff proposing change including the development or review of a policy, can be found in **Appendix 4**. The Company Secretary's Team should be consulted about the completion of this checklist.

8 CALDICOTT

The Caldicott Report 1997 focused specifically on the protection and processing of patient identifiable information in the NHS. PC24 maintains a commitment to the seven principles set out in the Caldicott Report.

The Caldicott function operates wherever patient identifiable information is involved, that is information that could be used in isolation or in combination with other items of data to identify a patient directly or indirectly and includes such items as:

- Name, address, postcode, phone number
- Pictures, photograph, videos
- NHS number and other identifiable codes

The Medical Director is the Caldicott Guardian for PC24 and oversees the Caldicott function, primarily concerned with upholding and supporting patient confidentiality.

8.1 Caldicott principles for handling patient data

1 Justify the purpose(s)

Every proposed use or transfer of patient identifiable information within PC24 or from another organisation/source should be clearly defined, scrutinised and regularly reviewed by an appropriate guardian. Attention should be paid to any proposed changes to the use of the information.

2 Don't use patient identifiable information unless it is necessary

Personal confidential information data items should not be shared unless it is essential for the specified purpose(s) of the particular information flow. The need for patients to be identified should be considered at each stage of any sharing to ensure the use satisfies the purpose(s) for which the information was provided.

3 Use the minimum necessary patient identifiable information

Where the use of personal confidential data is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information necessary for the specified function to be carried out is transferred or accessible.

4 Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need. This may mean require access controls or the splitting of data flows where one information flow is being used for several purposes.

Access to computer or manual records, for which the member of PC24 staff does not have relevant authorisation, is prohibited. Any staff accessing or attempting to access records they are not authorised to see will be subject to disciplinary procedures.

5 Everyone with access to patient identifiable information should be aware of their responsibilities

Action should be taken to ensure that those handling patient identifiable information – whether clinical and non-clinical staff - are made fully aware of their responsibilities and obligations in respect of patient confidentiality.

6 Understand and comply with the law

Every use of personal confidential data must be lawful. The Caldicott Guardian is responsible for ensuring that PC24 complies with legal requirements

7 The duty to share information can be as important as the duty to protect patient confidentiality

Professionals should, in the patient's interest, share information within this framework. Official policies should support them doing so.

Healthcare professionals should have the confidence to share information in the best interest of their patients within the framework set out by these principles. They should be supported by the relevant PC24 policies, regulators and professional bodies.

The Health & Social Care (Safety & Quality) Act 2015 includes a legal duty requiring health and adult social care bodies to share information where this will facilitate care for an individual.

9 CONFIDENTIALITY

The confidentiality: NHS Code of Practice was published by the Department of Health following major consultation in 2002/2003. The consultation included patients, carers, citizens; other health care providers, professional bodies and regulators. The guidance was drafted and delivered by a working group made up of key representatives from these areas.

The Code of Practice is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patient's consent to the use of their health records. This document uses the term 'staff' a convenience to refer to all those to whom this code of practice should apply. Whilst directed at NHS staff, the Code is also relevant to anyone working in and around health services and includes those staff working in integrated teams, private and the voluntary sector.

This document:

- Introduces the concept of confidentiality
- Describes what a confidential service should look like
- Provides a high level description of the main legal requirements
- Recommends a generic decision support tool for sharing/disclosing information;
- Lists examples of particular information disclosure scenarios

A summary of the key confidentiality issues can be gained by reading the main body of the document (pages 1 – 12), while the supporting annexed provide detailed advice and guidance on the delivery of a confidential service. The full document can be accessed here.

10 STANDARDS TO BE FOLLOWED BY ALL STAFF

10.1 Access to Records

- Access to computer or manual records, for which the member of staff does not have relevant authorisation, is prohibited.
- Any staff accessing or attempting to access records they are not authorised to see will be subject to disciplinary procedures.
- Requests from patients, or their representatives, to their health records should be handled in accordance with the guidance contained in the PC24 Subject Access Request SOP for the relevant service.

10.2 Transfer of Identifiable Information

- Any transfer of identifiable information must be carried out securely and with an adequate level of protection given to the data in transit in accordance with current NHS information security standards. In most cases this will require data transferred on portable media or electronically to be encrypted during transit.
- Patient identifiable data is not to be transferred outside the UK unless arrangements are in place to ensure that the requirements of GDPR, the Data Protection Act 2018 and Department of Health (DH) guidelines are fully complied with.
- Where a process requires that patient identifiable information is to be sent outside PC24, including by email from the PC24 domain, the Information Asset

Owner of that information should seek advice from the DPO and SIRO who will risk assess the process in advance.

- Where a Subject Access Request has been made the recipient is entitled to receive the response electronically. Where the recipient of the information does not have an appropriately secure email address, steps must be taken to protect that information such as password protection. Any password must be transmitted to the recipient by a means other than email.
- PC24 does not process personal or patient identifiable information outside the United Kingdom.

10.3 Clinical Research

- The DPO, or in their absence the SIRO, and the Caldicott Guardian should be consulted prior to the undertaking of clinical research, for the purposes of risk assessment and assurance that the use of data is lawful within GDPR and the DPA.
- The outcome of that consultation must be documented.

10.4 Collecting Information

- Only the minimum person identifiable information required for the specified purpose should be recorded and collected. The purpose for which information is to be collected and processed must be made clear to the information subjects concerned.
- All records, reports or printed matter containing person identifiable information must be treated as confidential and kept secure at all times. identifiable information must be kept securely whether stored electronically on devices that have adequate security measures in place, or stored in hard format - see PC24 Information Security Policy
- All data, manual or system held, should be periodically reviewed to ensure that the information is accurate, up to date and complete
- All data, manual or system held, should not be kept for longer than is necessary. Timescales are set out in PC24 Records Management policy which provides a schedule showing the normal retention periods for data and the recommended disposal methods. This policy also assures the quality of information.

- All reports, printouts or other printed material containing person identifiable information must be disposed of securely. Third party contractors used to dispose of such information on behalf of PC24 must be accredited to the required NHS standards and provide certification of disposal
- The disposal of computer equipment or devices capable of storing information must be carried out through the IT department to ensure all data is removed before disposal and equipment disposal meets the NHS required standards.

11 DISCLOSURE OF INFORMATION

Care must be taken to ensure any disclosure of personal or sensitive data is accompanied by appropriate consent or is for an identified lawful purpose under GDPR and the DPA.

Where there is any doubt, the DPO and SIRO, or one of these should both not be available, should be consulted prior to any disclosure. Written outcome of the consultation should be provided and disclosure should then be in accordance with that advice. Where patient information is involved the DPO/SIRO should seek advice from the Caldicott Guardian.

Any request to access/view a patient health record should be made in accordance with GDPR, DPA or Access to Health Records 1990. In accordance with the SOP the IG Lead, or their deputy, should be informed and should appropriately document, and monitor compliance with, that request.

Any requests for patient or staff information from external bodies such as the Police should be directed to the DPO/IG Lead who will liaise with the SIRO/Caldicott Guardian where necessary and ensure that disclosure is with in ‘lawful purpose’ as set out in the GDPR/DPA.

In all cases, as stipulated by GDPR/DPA, only the minimum necessary information to meet the identified need should be provided. The subject of the request should be notified of the disclosure unless it would defeat the purpose of the disclosure (eg Police investigation) or put the subject or any other party at risk.

Where the parameters of a subject access request are unclear, PC24 will seek clarification of the request, though this does not extend the response time limit. If the request is one of a number from the same individual or is particularly complex, the time limit can, within 1 month of receipt of the request, be extended for a further month upon notification to the data subject with the reason for the extension.

11.1 Disclosing Information against the Subject's wishes

The responsibility to withhold or disclose information without the data subject's consent rests with the DPO, IG lead and SIRO and cannot be delegated. Circumstances where the subject's right to confidentiality may be overridden are rare, examples could include:

- Where the subject's life may be in danger, or cases in which she/he may not be capable of forming an appropriate decision
- Where there is a serious danger to other people or where the rights of others may supersede those of the subject, for example a risk to children or the serious misuse of drugs
- Where there is a serious threat to the healthcare professional or other staff
- Where there is a serious threat to the community
- In other exceptional circumstances, based on professional consideration and consultation.

The following are examples where disclosure without consent is required:

- Births and deaths – National Health Service act 1977
- Notifiable communicable diseases – Public Health (Control of Diseases) Act 1984.
- Poisonings and serious accidents are the workplace – Health & Safety at Work Act 1974
- Child abuse – Children's Act 1989 and The Protections of Children Act 1999
- Drug Addicts – Drugs (Notification of Supply to Addicts) Regulations 1973
- Road traffic accidents – Road Traffic Accident 1988

- Prevention/detection of a serious crime e.g. terrorism, murder – The Crime and Disorder Act 1998

If in doubt, seek guidance in confidence from the DPO, SIRO and Caldicott Guardian.

11.2 Non-Disclosure of person identifiable data

An individual requesting access to their data may be refused access to parts of the information if, on consultation with the DPO, Caldicott Guardian, SIRO and any appropriate clinicians as appropriate, exposure to the information could cause physical or mental harm to the data subject or a third party. The reasoning for any non-disclosure must be set down in writing and those providing advice should be prepared to justify their reasons in a court of law if necessary.

Information related to third parties, other than health care professionals providing information as part of their duty of care, should be redacted from the record before disclosure unless consent for the release has been received from the third party concerned or it is reasonable to comply with the request without the consent of the third party.

PC24 is not required to disclose the requested information:

- If a specific exemption applies
- The request is manifestly unfounded or
- The request is excessive.

The reasons behind any non-compliance must be documented so that it can be explained to both the data subject and the Information Commissioner.

12 ACCESS TO INORMATION TECHNOLOGY SYSTEMS

Access to IT systems is controlled in accordance with guidance provided in the PC24 Information Security Policy (PC24POL6). Key standards within the policy are:

- Restrict access to the level appropriate to the user's role

- Access should only be gained by means of a restricted login and, where necessary, a security password or PIN, issued when the appropriate training has been received and the relevant level of access authorised and gained
- Passwords must be kept secure and never shared with other users. Failure to comply is treated seriously and may lead to disciplinary action
- Users must log-off or lock their screen when the computer is not in use
- No computer should be placed in such a position that unauthorised persons can view patient or other confidential information. If this proves to be impossible, the IT team should be consulted about the possibility of purchasing a privacy filter
- Access to VPNs, and portable IT devices that may contain confidential information is subject to the same restrictions as listed above.

13 BREACHES

13.1 Breach of Policy

Line Managers and Heads of Department should ensure that their staff comply with PC24 policies and procedures. Line Managers should ensure that staff are aware of key documents related to their work and have undertaken the required mandatory training.

Non-compliance with a PC24 policy may result in disciplinary action.

13.2 Breaches of Confidentiality and Data Protection

- Failure to manage information securely places PC24 at risk of breaching confidentiality and data protection legislation. If person identifiable information is deliberately or accidentally divulged the DPA and NHS Caldicott Guidelines could be breached
- As well as placing PC24 at risk of prosecution, breaches of confidentiality lead to a lack of trust from patients and public, and adverse publicity for PC24. Disciplinary action may be taken if an unauthorised disclosure of person identifiable data is made and, if deliberate, an individual may be liable to prosecution

- All suspected breaches of confidentiality or Data Protection policies should be reported on Datix and reported to IG Lead, the Senior Information Risk Owner and the individual's Line-Manager
- Breaches will be presented to the Information Governance & IT Steering Group monthly and reviewed to ensure learning is captured and all reportable breaches have been appropriately reported.
- A report will be made bi-monthly to the Quality & Workforce Committee as part of the Regulatory Compliance Report.
- Some breaches will be deemed, following investigation, to warrant disciplinary action, this will be the responsibility of the individual's Line Manager and/or the Human Resources Manager
- Serious breaches will be reported through the Data Security & Protection Toolkit which will, where appropriate, automatically refer matters to the Information Commissioner.
- Where a breach may result in legal action or adverse publicity for PC24, briefing will be provided for the appropriate CCG communication officers and PC24's legal advisors as appropriate.

14 MONITORING COMPLIANCE AND EFFECTIVENESS

The compliance and effectiveness of this policy will be monitored by a combination of:

- Analysis of incidents and reported breaches to identify common themes of failure in process or procedure
- Audits at all sites to assess the adequacy of information security measures and staff understanding of their responsibilities relating to Data Protection and Confidentiality
- The work of the Information Governance & IT Steering Group
- The annual review of Information Governance compliance through completion of the Data Protection & Security Toolkit.
- Completion and review of Data Protection Impact Assessments
- Annual Information Governance mandatory training for all staff, monitored by the training team and the Information Governance & IT Steering Group

- Annual performance review of all staff.

15 TRAINING

15.1 As part of the PC24 mandatory training programme, each member of PC24 staff will undertake Information Governance training using the approved training tool, on an annual basis. This training will be recorded by the training department. Managers have a responsibility to ensure all their staff are up to date with mandatory training requirements. See Training Needs Analysis is **Appendix 2.**

15.2 Policies and procedures supporting Data Protection and Confidentiality are available and accessible on the local PC24 intranet.

16 FINANCIAL IMPACT & RESOUCE IMPLICATIONS

PC24 is required to be compliant with the Data Protection & Security Toolkit.
Failure to maintain this would render PC24 ineligible to tender for new business.

The Information Commissioner's Office monitors all serious breaches of the personal identifiable data and/or confidentiality requirements of the DPA, and could impose a statutory fine.

17 EQUALITY & HEALTH INEQUALITIES STATEMENT

PC24 is committed to an environment that promotes equality and embraces diversity in its performance as an employer and service provider. It will adhere to legal and performance requirements and will mainstream equality and diversity principles through its policies, procedures and processes. This policy has been implemented with due regard to this commitment. To ensure that the implementation of this policy does not have an adverse impact in response to the requirements of the Equality Act 2010 this policy has been screened for relevance during the policy development process and a full equality impact analysis conducted where necessary. PC24 will take remedial action when necessary to address any unexpected or unwarranted disparities and monitor practice to ensure that this policy is fairly implemented.

18 DATA PROTECTION IMPACT STATEMENT

PC24 is committed to an environment that protects person identifiable data in the development of any policy. When proposing change to a policy there is a requirement for policy writers to investigate whether the policy complies with the data protection principles set out in GDPR and the Data Protection Act 2018. All individuals with responsibility for reviewing/writing policies should consider Data Protection Impact Assessment compliance and undertake assessments as necessary. In cases where there is a change in process, the Data Protection Officer must also be consulted.

This policy complies with the Data Protection Act 2018, therefore no Data Protection Impact Assessment is necessary.

19 POLICY REVIEW

This policy will be subject to regular planned review and all staff will be alerted to any new version. The latest version can be accessed via the staff intranet.

20 ASSOCIATED DOCUMENTATION

All PC24's Information Technology and Information Governance Policies and SOPs are accessible to all staff from the intranet and include:

- Information Security Policy
- Email and Internet Policy
- Records Management Policy
- Subject Access Request SOPs
- Clear Desk & Screen SOP
- Sending Information by fax SOP
- Sending Information by post SOP
- Transporting Information SOP
- Guidance on Handling Patient Identifiable Information

21 REFERENCES

- Data Protection Act 2018
- General Data Protection Regulations
- The Caldicott Report 1997
- The Information Governance Review 2013
- The Human Rights Act 1998
- The Equality Act 2010
- Common Law Duty of confidence
- Confidentiality: NHS Code of practice
- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf
- https://www.england.nhs.uk/ourwork/tsd/ig/
- NHS Codes of Practice:
    - Confidentiality
    - Records Management
    - Information Security Management

APPENDIX 1 Personal data and special category personal data

Personal data is defined in Article 4 of the GDPR as 'any information relating to an identified or identifiable natural person (the data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Category personal data is defined as personal data which is more sensitive and therefore needs more protection. This includes:

- the racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- genetics
- biometrics (when used for ID purposes)
- physical or mental health or condition
- sex life
- sexual orientation.

The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data. In particular, if you are processing sensitive personal data you must satisfy one or more of the conditions for processing which apply specifically to such data, as well as one of the general conditions which apply in every case. The nature of the data is also a factor in deciding what security is appropriate. Please see Article 9(2) of the GDPR and the section of this guide on the ***conditions for processing.***

The categories of sensitive personal data are broadly drawn so that, for example, information that someone has a broken leg is classed as sensitive personal data, even though such information is relatively matter of fact and obvious to anyone seeing the individual concerned with their leg in plaster and using crutches. Clearly, details about an individual's mental health, for example, are generally much more "sensitive" than whether they have a broken leg.

APPENDIX 2 Training Needs Analysis

Training requirement	Frequency	Course length	Delivery method	Facilitators	Recording Attendance	Strategic & Operational Responsibility
Information Governance	On appointment	N/A	e-learning	N/A	Training Dept.	
Information Governance Refresher	Annually	N/A	e-learning	N/A		
Data Protection Officer	Annually					
Senior Information Responsible Owner Training	Annually					
Information Asset Owner	Annually					
Caldicott Training	Annually					
Staff Groups	**Target Audience**					
Integrated Urgent Care SDU	All staffing					
Primary Care SDU	All staffing					
Corporate	All staffing					
SIRO	Yes					
Data Protection Officer	Yes					
Information Asset Owners	Yes					

Data Protection Act 2018

DATA PROTECTION IMPACT ASSESSMENT

(DPIA)

Compliance Checklist

Data Protection Act 2018

PRIVACY IMPACT ASSESSMENT (PIA)

Compliance Checklist

Privacy

Privacy has become a much larger consideration for business and government in recent years. New information technologies have increased public concerns about intrusion into their privacy.

Beyond the recognition of privacy as a human right, specific laws have been introduced to deal with particular areas of concern. Much of the legislative attention to date has been focused on information about people that is collected, stored, used and disclosed by organisations. The handling of personal data is regulated by the Data Protection Act 2018, which the Information Commissioner's Office oversees.

Privacy impact assessment

Privacy Impact Assessment (PIA) is a process which enables organisations to anticipate and address the likely impacts of new initiatives, foresee problems, and negotiate solutions. Risks can be managed through the gathering and sharing of information with stakeholders. Systems can be designed to avoid unnecessary privacy intrusion, and features can be built in from the outset that reduces privacy intrusion.

This Privacy Impact Assessment (PIA) aims to assist Primary Care 24 when proposing change to investigate whether the personal information aspects of their project comply with the data protection principles in the Data Protection Act (DPA).

The checklist has been designed for use by any employee proposing change. The Quality & Patient Safety Team should be consulted about the completion of this checklist.

It should be noted that many terms used in the **principles** have meanings specific to the **Data Protection Act**, and it would be prudent to refer to the Act for definition for those terms. Another useful reference is the specific guidance on the Information Commissioner's website **https://ico.org.uk/**

A) BASIC INFORMATION - New or existing Project, System, Technology or Legislation

1 Lead Directorate and project name	
Directorate	
Department	
Project	

2 Contact position and/or name, telephone number and e-mail address. (This should be the name of the individual most qualified to respond to the PIA questions)	
Name	
Title	
Phone Number	
E-Mail	

3 Description of the programme / system / technology / legislation (initiative) being assessed.
If this is a change to an existing project, system, technology or legislation, describe the current system or programme and the proposed changes. *(N.B. if the initiative does **not** collect, use or disclose personal data* - see definition and statement below).*

4 Purpose / objectives of the initiative (if statutory, provide citation/reference).	
Purpose	

5 What are the potential privacy impacts of this proposal?

IF THERE IS NO PERSONAL DATA INVOLVED,
GO TO SECTION C DPA COMPLIANCE - CONCLUSIONS (on the last page)

***IMPORTANT NOTE:**
'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.

(Data Protection Act 2018)

B) DATA PROTECTION PRINCIPLES (DPPs) (General Data Protection Regulations (GDPR))

PRINCIPLE 1 **LAWFUL AND FAIR PROCESSING**	
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless – (a) at least one of the conditions in Chapter 2 GDPR is met, and (b) in the case of sensitive personal data, at least one of the additional conditions is also met	
1.1 Preliminary	
What type of personal data are you processing?	Personal Confidential Data of the deceased and of the living
1.2 Conditions relevant for purposes of the first principle: processing of any personal data	
Describe the purposes for which you will be processing personal data.	
List which of the grounds you will be relying on as providing a legitimate basis for processing personal data.	
1.3 Conditions relevant for purposes of the first principle: processing of any *sensitive* personal data	
If this project does not involve the processing of sensitive personal data, please go to section 1.4	
Identify the categories of *sensitive personal data* that you will be processing.	
Identified *the purposes* for which you will be processing *sensitive personal data*.	
Identify which of the grounds you will be relying on as providing a legitimate basis for processing *sensitive personal data*?	
1.4 Obtaining consent	
Are you relying on the individual to provide consent to the processing as grounds for lawful and fair processing?	Delete as appropriate Yes No
If yes, when and how will that consent be obtained?	.

For the processing of *sensitive personal data*, are you relying on *explicit* consent?	Delete as appropriate Yes No
If yes, when and how will that consent be obtained?	
1.5 Lawful processing	
How is compliance with the Human Rights Act being assessed?	Via this PIA Review and the Data Sharing Agreement - Information is limited to a need to know and informed consent is provided to ensure no breach of Human Rights occurs.
Are you assessing whether your processing is subject to any other legal or regulatory duties?	Delete as appropriate Yes No
If yes, how is that assessment being made? If no, please indicate why not.	
1.6 Fair processing	
How are individuals being made aware of how their personal data is being used?	
How individuals are offered the opportunity to restrict processing for other purposes?	
When is that opportunity offered?	
1.7 Exemptions from the first principle	
The Act requires that in order for personal data to be processed fairly, a data controller must provide the data subject with the following information:- 1. the identity of the data controller 2. the identify of any nominated data protection representative, where one has been appointed 3. the purpose(s) for which the data are intended to be processed 4. any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair *Data Protection Act:* ***https://ico.org.uk/for-organisations/guide-to-data-protection/exemptions***	
Do you provide individuals with all of the information in the box above?	Delete as appropriate Yes

	No
If no, which exemption to these provisions is being relied upon?	

PRINCIPLE TWO: THE PURPOSE OR PURPOSES FOR PROCESSING PERSONAL DATA		
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.		
2.1 Use of personal data within the organisation		
What procedures are in place for maintaining a comprehensive and up-to-date record of use of personal data?		
Is any data processing carried out on your behalf (e.g. by a subcontractor)?	Delete as appropriate Yes No	
If yes, please identify		
2.2 Use of existing personal data for new purposes		
Does the project involve the use of existing personal data for new purposes?	Delete as appropriate Yes No	
If no, go to section 2.3		
If yes, How is the use of existing personal data for new purposes being communicated to:- *a) the data subject:* b) *the Data Protection Officer (responsible for Notification)*	a)	
	b)	
2.3 Disclosure of data		
How individuals / data subjects are made aware of disclosures of their personal data?		
PRINCIPLE 3: DATA MINIMISATION		
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.		
3.1 Adequacy and relevance of personal data		
How is the *adequacy* of personal data for each purpose determined?		
How is an assessment made as to the *relevance* (i.e. no more than the minimum required) of personal data for the purpose for which it is collected?		
What procedures are in place for periodically checking that data collection procedures are adequate, relevant and not excessive in		

relation to the purpose for which data are being processed?		
PRINCIPLE 4: ACCURATE AND UP TO DATE		
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. Every reasonable step must be taken to rectify or erase inaccurate or incomplete data.		
4.1 Accuracy of personal data		
How often is personal data being checked for accuracy?		
How is the accuracy of the personal data being checked with the Data Subject?		
4.2 Keeping personal data up to date		
How is personal data evaluated to establish the degree of damage to: (a) the data subject or (b) the data controller That could be caused through being out of date?	a)	
	b)	
PRINCIPLE 5 NO LONGER THAN NECESSARY		
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.		
5.1 Retention policy		
Is the project subject to any statutory / sectorial requirements on retention?	Delete as appropriate Yes No	
If yes please state relevant requirements		
5.2 Review and deletion of personal data		
When data is no longer necessary for the purposes for which it was collected: a) How is a review made to determine whether the data should be deleted? b) How often is the review conducted? c) Who is responsible for determining the review? d) If the data is held on a computer, does the application include a	a)	
	b)	
	c)	
	d)	

facility to flag records for review / deletion?	
If yes, please explain	
Are there any exceptional circumstances for retaining certain data for longer than the normal period?	Delete as appropriate Yes No
If yes, please provide justification	

PRINCIPLE 6 INTEGRITY & CONFIDENTIALITY (SECURITY OF PERSONAL DATA)	
Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures**.**	
6.1 Security Policy	
Is the level of security appropriate for the type of personal data processed?	Delete as appropriate Yes No
If yes please explain	
6.2 Unauthorised or unlawful processing of data	
Describe security measures that are in place to prevent any unauthorised or unlawful processing of: a) Data held in an automated format e.g. password controlled access to PCs b) Data held in a manual record e.g. locked filing cabinets	a) b)
Is there a higher degree of security to protect *sensitive personal data* from unauthorised or unlawful processing?	Delete as Appropriate Yes No
If yes, please describe the planned procedures. If no, please indicate why not.	
Describe the procedures in place to detect breaches of security (remote, physical or logical)? **logical (such as hacking etc.)*	
6.4 Destruction of personal data	

Describe the procedures in place to ensure the destruction of personal data no longer necessary?		
6.5 Contingency planning		
Is there a contingency plan to manage the effect(s) of an unforeseen event?	Delete as Appropriate Yes No	
If yes, please give details		
Describe the risk management procedures to recover data (both automated and manual) which may be damaged/lost through: a) human error b) computer virus c) network failure d) theft e) fire f) flood g) other disaster.	a)	.
	b)	
	c)	
	d)	
	e)	
	f)	
	g)	
6.6 Choosing a data processor		
How do you ensure that the Data Processor complies with these measures?		
SUBJECTS RIGHTS/SUBJECT ACCESS		
Personal data shall be processed in accordance with the rights of data subjects under this Act.		
7.1 Subject access		
How do you locate all personal data relevant to a request (including any appropriate 'accessible' records)?		
7.2 Withholding of personal data in response to a subject access request		
Are there any circumstances where you would withhold personal data from a subject access request?	Delete as appropriate Yes No	
If yes, on what ground. If no, go to 7.3		
How are the grounds for doing so identified?		
If yes, please provide justification		
7.3 Processing that may cause damage or distress		
Do you assess how to avoid causing unwarranted or substantial damage or unwarranted and substantial distress to an individual?	Delete as appropriate Yes No	

If yes, please specify proposed procedures. If no, please indicate why not.	
Do you take into account the possibility that such damage or distress to the individual could leave your organisation vulnerable to a compensation claim in a civil court?	Delete as appropriate Yes No If yes, please explain
7.4 Right to object	
Is there a procedure for complying with an individual's request to prevent processing for the purposes of direct marketing?	Delete as appropriate Yes No N/A Other
If yes, please explain	
7.7 Automated decision	
Are any decisions affecting individuals made solely on processing by automatic means?	Delete as appropriate Yes No
If yes, what will be the procedure(s) for notifying an individual that an automated decision making process has been used?	
7.6 Rectification, blocking, erasure and destruction	
What is the procedure for responding to data subject's notice (in respect of accessible records) or a court order requiring: a) rectification; b) blocking; c) erasure or; d) destruction of personal data?	a)
	a)
	b) .
	c)
OVERSEAS TRANSFER (OUTSIDE OF THE EEA)	
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.	
8.1 Adequate levels of protection	

Are you transferring personal data to a country or territory outside of the EEA[1]? [1] The European Economic Area (EEA) comprises the 27 EU member states plus Iceland, Liechtenstein and Norway.	Delete as appropriate Yes No
If no, go to Part III If yes, where?	
What types of data are transferred? (e.g. contact details, employee records)	
Is *sensitive personal data* transferred abroad?	Delete as appropriate Yes No
If yes, please give details	
Are measures in place to ensure an adequate level of security when the data are transferred to another country or territory?	Delete as appropriate Yes No
If yes, please describe. If no, please indicate why not.	
Have you checked whether any non-EEA states to which data is to be transferred have been deemed as having adequate protection?	Delete as appropriate Yes No
If yes, please give details	

C) DPP COMPLIANCE - CONCLUSIONS

Please provide a summary of the conclusions that have been reached in relation to this project's overall compliance with the DPPs. This could include indicating whether some changes or refinements to the project might be warranted.

IG Manager Name:

IG Manager Signature: **Date:**

Project Manager:

Project Manager Signature: **Date:**

END OF POLICY