7.03 Confidentiality and Data Protection Policy

Title: 7.03 Confidentiality and Data Protection Policy	
Published Date: September 2019	**Version number:** V3.0
Ratified by: SMT September 2019	**Expiry date:** September 2022
Suggested earliest review date: March 2022	**Author:** MF
Date of previous versions and brief details of amendments made *Versions prior to 2015 are available through archives and may be requested.* V2.0 – May 17 Suite of policies relating to Information Governance have been developed and ratified for use within St Anne's following the introduction of new IT systems and several contract compliance issues around security of information. V3.0 – August 19 - Updated to meet DPA 2018 and GDPR changes. Includes changes around Police requests for Data and Privacy Impact Assessments. Change of number to policy and full suite of IT / IG policies. All policies in Section 9 of the Staff Manual have moved back to Section 7 to use up numbers within the Staff Manual.	
Equality Impact Assessment completed:	Yes

Introduction

At St Anne's Community Services (St Anne's), we process personal information about our staff, Clients, visitors, trustees and others to support the delivery of services and the operation of our business. We recognise the need for effective controls around the collection, creation, use, retention and destruction of personal data, as well as our duties under data protection laws, in particular our obligations under Article 5 of General Data Protection Regulation (GDPR) and processing activity requirements as set out in the Data Protection Act 2018 (DPA).

This policy forms part of our Information Governance Management Framework, which demonstrates how we comply with relevant legislation and guidance, including: the DPA, the Access to Health Records Act 1990, the Human Rights Act 1998, the Caldicott Principles/guidance, the Confidentiality Code of Practice Department of Health (2003), the Information Commissioners Office (ICO) Statutory Data Sharing Code of Practice and the ICO's Anonymisation Code of Practice, the Health and Social Care Information Centre's 'A Guide to Confidentiality in Health and Social Care' and the National Data Guardian's ten data security standards, as well as observing the common law duty of confidentiality.

All applicable legal and best practice standards are brought together in the Data Security and Protection Assurance Framework for Health and Social Care. St Anne's will conduct an annual self-assessment of its compliance with this Framework through the Data Security and Protection Toolkit process.

This policy outlines the requirements of the DPA and confidentiality regarding the collection, use, transfer and security of personal data by or on behalf of St Anne's. Our Privacy Notice contains more detail about the processing activities we undertake, as well as the categories of personal data we process.

Purpose

This policy is in place to ensure that St Anne's staff are aware of their responsibilities for the safeguarding of confidential information held both manually (non-computer in a structured filing system) and the potential consequences of breaches of confidentiality for the organisation, individual data subjects and themselves.

For the purpose of this and all other St Anne's Information Governance policies, the term 'St Anne's staff' refers to St Anne's employees, members of the SMT Team, St Anne's Board, temporary staff, contractors / agency staff, consultants, students and other individuals working on behalf of St Anne's.

Scope

This policy applies to all St Anne's staff and all identifiable information created, processed and stored by St Anne's, including information about St Anne's staff and our partner organisations. All St Anne's staff who will have access to confidential data will be subject to a confidentiality agreement, which will be incorporated into the contractual terms and conditions of all employees and included in contracts for services or contained in standalone documents as appropriate. The Information Governance Manager will provide further advice and guidance on this.

This policy is primarily concerned with confidentiality in relation to personal data. However, the principles of confidentiality should also be applied to sensitive business activities (e.g. tendering processes, commissioning new services, performance management).

All staff should meet the standards outlined in this policy as well as their terms of employment, any relevant professional code of practice and the St Anne's Code of Practice. **Failure by any employee of St Anne's to adhere to this policy may result in disciplinary action.**

Key Legislation and Definitions

The Access to Health Records Act 1990 provides controls on the management and disclosure of health records for **deceased** patients.

Clients: past and present clients and tenants of St Anne's.

The DPA and **GDPR** provide controls on the handling of personal identifiable information for all living individuals.

Personal Confidential Data (PCD): a term used in the Caldicott Information Governance Review, in this policy it describes all personal information about identified or identifiable individuals which should be kept private or secret, incorporating the DPA definition of 'personal data', i.e. 'any information relating to an identified or identifiable living individual' and including dead as well as living people. It includes both information 'given in confidence' and that which is owed a 'duty of confidence'.

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Safe Haven: a location (or in some cases a piece of equipment) situated within premises where arrangements and procedures are in place to ensure PCD can be held, received and communicated securely and confidentially.

Sensitive Information: includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation (referred to in the DPA as 'special categories of personal data') as well as personal data relating to criminal convictions and offences or related security measures.

Duties and Responsibilities

Chief Executive Officer

The Chief Executive Officer is responsible for ensuring that:

- St Anne's staff are aware of the need to comply with the GDPR/DPA, in particular the rights of data subjects wishing to access personal information
- St Anne's staff are aware of requirements of the common law duty of confidence and
- Arrangements with third parties who process personal data on behalf of St Anne's are subject to a written contract which stipulates appropriate security and confidentiality

Senior Management Team

All members of the Senior Management Team are responsible for identifying and implementing confidentiality and data protection processes relevant to their areas of responsibility.

Caldicott Guardian

The Caldicott Guardian is the organisation's Senior Professional who is responsible for:

- Ensuring that the personal data of those who use its services is used legally, ethically and appropriately, and that confidentiality is maintained
- Representing and championing information governance requirements and issues at Senior Management Team and Board level and, where appropriate, throughout the organisation's overall governance framework, including the governance of information management and technology

- Overseeing the development and implementation of those St Anne's policies and procedures designed to ensure that all routine use of Personal Confidential Data (PCD) is identified, justified, documented and monitored
- Overseeing the development and implementation of criteria and processed for dealing with ad hoc requests for use of Personal Confidential Data (PCD) for non-direct care purposes
- Ensuring standard procedures and protocols are in place to govern access to Personal Confidential Data (PCD)
- Providing advice and guidance where required to the organisation's Information Research and Clinical Audit processes and personnel to ensure protocols for releasing information for research and audit are in line with applicable information governance standards and
- Understanding and applying the principles of confidentiality and data protection as set out in the Confidentiality: St Anne's Code of Practice and, where current practice falls short of the requirements, to agree challenging and achievable improvement plans.

At St Anne's the Caldicott Guardian is the Director of Operations.

Senior Information Risk Owner (SIRO) and Information Asset Owners (IAO)

The SIRO is a Director level individual responsible for ensuring that organisational information risk is properly identified and managed. Appropriate assurance mechanisms exist to support the role of SIRO, including the identification of IAOs and other supporting roles. At St Anne's the SIRO is the Finance Director.

At St Anne's Information Asset owners (IAO) are ROMs and Area Managers. One of the roles of the IAOs is to understand the nature and justification of information flows to and from information assets. IAOs, supported by nominated staff, are responsible for ensuring that information assets are managed in accordance with confidentiality and data protection requirements.

Director of Corporate Affairs / Head of Information Governance

The Director of Corporate Affairs/Head of Information Governance has overall responsibility for managing and effectively implementing all activities necessary to achieve compliance with the GDP/DPA throughout the organisation. He or she will (and may delegate to the Information Governance Officer):

- Inform and advise St Anne's staff about their obligations to comply with the GDPR/DPA and other data protection laws
- Advise and update the organisation in relation to relevant directives/guidance
- Via the Information Governance Framework – ensure that the Caldicott Guardian and Senior Information Risk Owner (SIRO) are informed of relevant issues and decisions are recorded
- Monitor compliance with the GDPR/DPA and other data protection laws, including by managing internal data protection activities, advising on data protection impact assessments, training staff and conducting internal audits

- Maintain an up to date notification under the GDPR/DPA with the Information Commissioner's Office and
- Be the first point of contact for supervisory authorities and for individuals whose data is processed

Information Governance Officer

- Responsible for co-ordinating the return of the annual Data Security & Protection Toolkit via the NHS Digital on-line self-assessment portal on behalf of the Director of Corporate Affairs/Head of Information Governance, SIRO and Caldicott Guardian;
- Provide effective training for all staff in the requirements of data protection legislation and Caldicott principles
- Carry out data protection and Caldicott compliance checks in services
- Develop and support the Data Subject Access Request process and
- Maintain an Information Asset Management Framework

Head of IT

- Provide an advisory service to the Information Governance team
- Monitor and report on the state of Information Management & Technology security within the organisation
- Develop and enforce detailed procedures to maintain information security
- Ensure compliance with relevant legislation
- Monitor for actual or potential information security breaches and
- Lead on issues with regard to cyber security issues

All Managers

All managers are responsible for ensuring that their staff receive relevant training, guidance and support to understand and adhere to this policy and all appropriate supporting guidance.

All Staff

All St Anne's staff must be aware or their individual responsibilities for complying with confidentiality and data protection requirements in accordance with this policy.

The Data Protection Principles

The DPA and GDPR require organisations to demonstrate, through policies, procedures and other specified documentation, how they comply with the six data protection principles:

Accuracy	All reasonable steps must be taken to ensure that personal data that is inaccurate is erased or rectified as soon as possible. Checks will be carried out on a regular basis to ensure that the data held is accurate. If the data is inaccurate or has changed, we will take steps to make sure that it is erased or rectified.
Storage limitation	We should not keep personal data for longer than we need it. There is no "one size fits all" and when personal data is no longer needed, it should be securely deleted/destroyed in accordance with agreed retention periods outlined in the Records Management, Data Retention and Archiving Policy. Some records relating to former Clients or employees may be kept for an extended period for legal reasons and to enable the provision of references.
Integrity and confidentiality	It is a requirement of GDPR that appropriate technical and organisational security measures are used, monitored, controlled and audited to protect against unauthorised processing, accidental loss, destruction or damage of personal data. We take security very seriously and have in place policies, procedures and technologies to maintain the security of personal data.
Lawfulness, fairness and transparency	We must be transparent with data subjects about how we will use their personal data. This is generally done through Privacy Notices.
Purpose limitation	Personal data must not be collected for one reason and then processed for another unless we have informed the individual. Privacy Notices will normally specify that some personal data may be used for a variety of purposes.
Data minimisation	Personal data collected must be necessary for the purposes for which it is being processed and not be collected "just in case" and forms that are used to collect data will be reviewed to determine whether any sections can be made optional.

St Anne's staff must at all times comply with these principles.

Technically the DPA only applies to living individuals. However, St Anne's upholds the duty of confidentiality owed to the deceased and their relatives and staff should, as far as possible, follow data protection guidelines and seek the consent of the recognised personal representative of the deceased to disclose information.

The Caldicott Principles

One of St Anne's Executive Directors acts as our Caldicott Guardian to oversee the processing of Personal Confidential Data (PCD). This helps to ensure that we are compliant with the Caldicott principles governing the use of PCD.

The Caldicott Guardian must be satisfied that all PCD processing follows the 7 Caldicott principles:

The 7 Caldicott Principles

Principle 1: Justify the purpose(s)

Every proposed use or transfer of PCD within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2: Do not use PCD unless it is absolutely necessary

PCD should not be used unless there is no alternative and it is essential for the specified purpose(s) of that flow.

Principle 3: Use the minimum PCD

Where the use of PCD is considered to be essential, each individual item of information should be justified accordingly.

Principle 4: Access to PCD should be on a strict need to know basis

Only those individuals who need access to PCD should have access to it.

Principle 5: Everyone should be aware of their responsibilities

Action should be taken to ensure that those handling PCD are aware of their responsibilities and obligations to respect client confidentiality.

Principle 6: Understand and comply with the law

Every use of PCD must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7: The duty to share information can be as important as the duty to protect Client confidentiality

Staff should have the confidence to share information in the best interests of their patients within the framework set out by these principles.

Confidentiality

The common law 'duty of confidence', or 'duty of confidentiality' is a legal obligation deriving from cases decided in the civil court system. It is well established within professional codes of conduct.

The duty arises when a person discloses information to another (e.g. client to staff or employee to employer) in circumstances where it is reasonable to expect that the information will be held in confidence. St Anne's owes a 'duty of confidence' to Clients and must support professional ethical standards of confidentiality.

A breach of confidentiality is rarely a malicious act and often information is given out inadvertently or due to staff not following procedures. St Anne's staff must be constantly aware of their obligations to prevent breaches of confidentiality.

Appendix A provides further information on the common law duty of confidentiality, but in summary it means that information provided for one purpose must not be used or disclosed for another purpose, unless one of more of the following applies:

- the individual's explicit consent has been obtained
- disclosure is necessary to safeguard the individual, or others
- where disclosure is in the overriding public interest or
- where there is a legal duty to do so (e.g. Court Order or other statutory basis, such The NHS Act 2006 and the Regulations that enable the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be transferred to an applicant)

In specific circumstances, information may need to be disclosed without the individual's consent. For further details see Confidentiality, Disclosure of Personal Confidential Data and Use of Anonymised Data section.

St Anne's staff who require guidance and or advice about sharing PCD should contact the Information Governance Officer and/or the Caldicott Guardian.

Lawful Processing of Personal Data

We must ensure that the collection and use of personal data is lawful, this means that any use of 'personal data' must fall within a "lawful purpose".

Lawful Basis	**Examples**
Contractual Obligation	The processing is necessary for a contract we have with an individual or third party or specific steps we are asked to take before entering into a contract, including terms and conditions of employment.
Legal Obligation	The processing is necessary for us to comply with the law (not including contractual obligations). There are many lawful obligations which we must fulfil e.g. tax, pension, compliance with Health & Safety at Work Act, CQC regulations, etc.
Vital Interests	The processing is necessary to protect someone's life.
Public Interest (Task)	The processing is necessary to perform a task in the public interest or for our official functions and the task or function has a clear basis in law. **We should normally consider whether consent or legitimate interests are more appropriate bases for processing.**

Legitimate Interest	The processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the data subject's personal data which overrides those legitimate interests.
Consent	The data subject has given consent for us to process their personal data for one or more specific purposes. Consent must be freely given, specific, informed, an unambiguous indication of the data subject's wishes, a form of firm confirmation or positive opt-in, such as ticking boxes on a web-page, and be easily able to be withdrawn. Consent cannot be obtained from silence, pre-ticked boxes or inactivity. Consent cannot be used where there is a power imbalance, such as in the employment relationship, or where there is a lack of capacity to consent.

Lawful Processing of 'Special Categories of Personal Data'

There are additional conditions which need to be met in order to process 'Special Categories of Personal Data'. These are set out in Article 9 of GDPR and are as follows (paraphrased):

- Explicit consent
- Employment and social security obligations
- Vital interests
- Necessary for establishment or defence of legal claims
- Substantial public interest and
- Various scientific and medical issues

Withdrawal of Consent

"Consent" can be withdrawn by the individual at any time.

Personal Data Breaches

A breach is defined as:

Article 4(12) "Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

There are three types of personal data breach, which are as follows:

- a **Confidentiality breach** - unauthorised or accidental disclosure of, or access to personal data, e.g. hacking, accessing internal systems which you are not authorised to access, putting the wrong letter in the envelope,

sending an email to the wrong person, or disclosing information over the phone to the wrong person

- an **Availability breach** - unauthorised or accidental loss of access to, or destruction of, personal data, e.g. the loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting personal data in error, loss of access to personal data stored on systems, inability to restore access to personal data from back up, or loss of an encryption key and

- an **Integrity breach** - unauthorised or accidental alteration of personal data

Notifications to the Information Commissioner

In line with the Information Commissioner's national notification guidance, any serious data protection breaches which are likely to result in a risk to the rights and freedoms of individuals (data subjects) within 72 hours of detection. Failure to report a breach when required to do so may result in penalties and fines.

St Anne's also has an obligation to keep adequate documentation of its processing activities. The documentation must be made available to the Information Commissioner on request. Individual data subjects can obtain full details of St Anne's data protection registration/notification with the Information Commissioner, from the Information Governance Officer, or from the Information Commissioner's website.

Notification of Breaches to Data Subjects affected

Article 34 of GDPR requires any personal data breach, that is likely to result in a high risk to the rights and freedoms of individuals, to be communicated with those affected. The communication must contain the following four elements:

- a description of the nature of the breach
- the name and contact details of a contact point from whom more information can be obtained
- a description of the likely consequences of the personal data breach
- a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

Whilst we are still required to notify the Information Commissioner, we are not obliged to notify the data subjects affected where:

- There are technological and organisational protection measures in place (e.g. encryption)
- We have taken action to eliminate the high risk and
- It would involve disproportionate effort – in this case data subjects can be informed some other way, e.g. by a notice in newspapers

Reporting a Personal Data Breach or Concern Internally

The Datix Incident Reporting system should be used in all St Anne's areas to report and investigate data breaches and data concerns, following the process set out in the St Anne's Incident Management Policy and Procedures.

Potential Penalties for a Breach

Under the DPA, individuals may be entitled to compensation if they have been caused distress that has resulted in damages due to having their right to privacy breached. St Anne's Staff can be sued in their personal capacity and may be subject to a fine and/or civil or criminal action for a breach of confidentiality.

In the event of very serious breaches of confidentiality, regulatory action can be taken by the Information Commissioners Office, which can include a fine.

Transfers of data must comply with our '***Secure Transfer of Information and Safe Haven Policy***'.

PCD **must not** be routinely stored or transferred using mobile storage devices*, due to the risk of the data being lost, stolen or damaged. Where this is required, documented authorisation **must** be obtained in advance from the Caldicott Guardian. The information and/or device must be encrypted. See the **Information Security Policy** for more details.

Protection of St Anne's Information Assets

Information assets* owned by St Anne's include any electronic and paper-based information that we process. This also includes systems, services and resources deployed in processing that information.

**For the purpose of this and all other St Anne's Information Governance policies, the term 'information asset' refers to IT infrastructure and operating systems, business applications, off-the-shelf software products, services of specialist staff, user-developed applications (e.g. databases), hard-copy records and electronic data.*

St Anne's '**Information Security Policy**' provides detailed information on the management of information assets and the associated roles and responsibilities of identified staff within the organisation.

The Information Governance Officer should be informed of all new information assets, for inclusion on the St Anne's Information Asset Register.

The Information Governance Officer will ensure that any proposal to undertake new or extended processing of personal data, is first subject to a formal Data Protection Impact Assessment as required by the DPA.

All transfers of PCD must be undertaken in a secure manner and in accordance with the St Anne's' '***Secure Transfer of Information and Safe Haven Policy'***.

Details of any PCD, e.g. health information or staff employment records, should not be discussed with anyone that does not have a legitimate 'need to know'. This applies both within the organisation and externally.

Individuals' Data Protection Rights (general)

Under Part 2 of the Data Protection Act, an individual (known as the data subject) has the following rights:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object and
- rights in relation to automated decision making and profiling

Where an individual asserts their data protection rights as outlined above, advice should be sought from the Information Governance Officer to ensure compliance with the provisions of the DPA.

The Data Protection Act 1998 does not cover the records of deceased persons but the Access to Health Records Act 1990 (the Act) gives certain people a right to see the health records (dating back no further than 1 November 1991) of somebody who has died. To exercise this right, you must be either:

a) A personal representative, meaning the executor or administrator of the estate or

b) Any person who may have a claim arising out of the individual's death

There are some restrictions on what can be disclosed, for example it is not possible to access the records of someone who made it clear that they didn't want other people to see their records after their death.

Requests for access to a deceased person's health records should be made in writing on **Form DAT[X]** - see **Appendix C** and this should be sent to the Information Governance Officer at Head Office. The request will be registered and sent to the appropriate data controller for action.

Confidentiality, Disclosure of Personal Confidential Data and Use of Anonymised Data

If a Client or their carer makes a request for information held about them, or a member of St Anne's staff or an outside contact makes a 'subject access' request, subject to appropriate exemptions, St Anne's will comply promptly with the request and in any event within one month of the receipt of the request and following confirmation of the identity of the person making the request.

Where the request for access is made by another on behalf of the individual, access can be refused if the individual had either provided the information in the expectation it would not be disclosed to the applicant or had indicated it should not be so disclosed.

A written request for access to information can be made on **Form DAT1** - see **Appendix B** and this should be sent to the Information Governance Officer at Head Office. The request will be registered and sent to the appropriate data controller for action.

In specific circumstances, information may need to be disclosed without the consent of the individual and may be done so under the limited exemptions provided in the DPA. Staff are advised to seek guidance from the Information Governance Officer and/or the Caldicott Guardian if they are unsure if there is a legal basis to share PCD without consent.

Where it is considered necessary to disclose PCD St Anne's will ensure that individuals disclosing that information justify their reasons for doing so in line with the DPA and the guidelines issued by the Information Commissioner.

Circumstances where disclosure without consent may be considered include:

- **When it is necessary to fulfil a legal obligation, including in compliance with a court order**

  Advice should be sought from the Caldicott Guardian if you have any concerns.

  If information is requested in compliance with a court order, the Information Governance Officer must be notified. You must always request a copy of the court order; establish what has been ordered, in relation to whom, the scope and the deadline to respond.

- **Where there is a serious public health risk**. The Public Health (Control of Disease) Act 1984 and the Public Health (Infectious Diseases) Regulations 1988 require the notification of certain diseases to the local authority.
- **In the interest of the protection of a vulnerable adult or child from abuse or neglect**
- **Where there is a risk of serious harm to an individual or others**
- **For the prevention, detection and prosecution of a serious crime**[1]

The Data Protection Act (2018) includes exemptions which allow personal data to be disclosed to law enforcement agencies without the consent of the individual who is the subject of the data, and regardless of the purpose for which the data were originally

[1] There is no definition of "serious crime". Section 115 of the Police and Criminal Evidence Act 1984 identifies "Serious Arrestable Offences" as: treason, murder, manslaughter, rape, kidnapping, certain sexual offences, causing an explosion, certain firearms offences, taking of hostages, hijacking, causing death by reckless driving, offences under the prevention of terrorism legislation and making a threat which if carried out would lead to a serious threat of security of the state or public order, serious interference with the administration of justice or with the investigation of an offence, death, serious injury or financial gain or serious financial loss to any person. The Information Commissioner's guidance on the Crime and Disorder Act 1998 gives advice on the data protection implications for data sharing; in some circumstances, it may be necessary to seek legal advice.

gathered. In particular, personal data may be released if the information is required for safeguarding national security (DPA section 26) or if:

Failure to provide the data would prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty (Schedule 1 Part 2 Clause 1 of the DPA).

Personal data may also be disclosed without contravening the DPA where the disclosure is required by law. For example, the Social Security Fraud Act 2001 requires organisations to provide any information to authorised officers of the Department for Work and Pensions or local authorities which they require for the investigation of fraud against the state benefit system. Refusal to provide the information can lead to prosecution of the institution.

Police forces have standard forms (known as "121" forms, relating to the relevant part of the DPA2018 which provides for the exemption, Schedule 1 Part 2 Clause 1) for requesting personal data, in accordance with guidance issued by the Association of Chief Police Officers (ACPO). The form should certify that the information is required for an investigation concerning national security, the prevention or detection of crime, or the apprehension or prosecution of offenders, and that the investigation would be prejudiced by a failure to disclose the information. This provides St Anne's with a legal basis for supplying the data under the DPA exemptions. Staff should compel police authorities who make requests for personal data, apart from in emergency situations, to complete a "121" form

In all cases, consent should be sought in the first instance unless the police indicate that to seek consent could cause harm or prejudice the investigation at hand.

The Information Governance Officer must be notified and will advise accordingly as to the disclosure of relevant information.

If the disclosure of PCD to the Police for the purpose of the prevention or detection of crime is likely to have a detrimental effect on the individual Client and it is considered that confidentiality outweighs the disclosure of information to the Police, then the Police should be advised to request a court order to ensure a lawful basis for the disclosure.

Advice must be sought from the Information Governance Officer.

- **Where the person lacks the capacity to give consent**

  No one can give consent on behalf of an adult who lacks capacity, unless they have the authority vested in them by a registered Lasting Power of Attorney. However, PCD about such a Client may still be shared if it is considered to be in their "best interests". "Best interests" requirements are set out in section 4 of the Mental Capacity Act 2005.

  The Mental Capacity Act (2005) allows St Anne's to share confidential information in respect to decisions about Clients with Independent Mental Capacity Act Advocates (IMCAs).

  For any issues relating to the Mental Capacity Act, please contact your Area Manager.

Other guidance available includes: 'Making Decisions – A Guide for people who work in Health and Social Care' (2007 2nd Ed.). You can also contact the Adult

Safeguarding Lead in the local authority in which St Anne's operates who will advise accordingly.

For further guidance on security of information please see the St Anne's '**Information Security Policy'**.

For further guidance on the requirements to safely store and send PCD please refer to the St Anne's '**Secure Transfer of Information and Safe Haven Policy'**.

Use of Anonymised Data

Information is considered to be anonymised when there is little or no risk of an individual being identified. Effectively anonymised information falls outside the scope of the DPA. Further guidance about anonymisation techniques can be found in the ICO '*Anonymisation Code of Practice*'.

Data Protection by Design and Default

We use data protection by design and default to ensure that our procedures and systems are designed to take account of data protection and security issues from when they first get implemented.

Systems and processes ensure that St Anne's staff only have access to those parts of PCD they require to carry out their role and information is processed on a 'need to know basis', with all transfers being part of an approved flow which has been risk assessed and documented according to DPA requirements.

St Anne's aims to ensure that only the minimum necessary personal data is processed, that pseudonymisation is used where possible, that processing is transparent and (where possible) allows individuals to monitor what is being done with their data.

Part of our data protection by design and by default is undertaking a Data Privacy Impact Assessment (DPIA) where necessary. Any new high-risk data processing activities will be assessed using a DPIA before the processing commences.

Information Sharing

Within St Anne's

St Anne's staff should only be able to access PCD required to carry out their roles. Information which contains PCD should only be shared with those who have a legitimate right of access and access is limited/non-excessive and on a 'need to know basis' (Caldicott principle 4).

The DPA requirements (re sharing information fairly, lawfully, proportionately, accurately and securely) and Caldicott principles must be adhered to at all times

following locally agreed processes and/or advice sought from an appropriate Line Manager, the Information Governance Officer or Caldicott Guardian.

Outside St Anne's

Information sharing should be supported by an appropriate information sharing agreement which provides for information sharing for a specific purpose, stipulates the legal basis for sharing any data and the parameters for the safe and secure sharing of such information in accordance with legislation, national guidance and best practice.

If there is a 'one-off' reason to share PCD, this must be approved by the Caldicott Guardian in advance.

Any reason for sharing information outside 'usual' working practices (e.g. an approved sharing process) must be referred to an appropriate Line Manager and the Director of Corporate Affairs/Head of Information Governance for approval.

Information sharing must not compromise confidentiality or security.

Privacy Notices

Any collection of PCD must satisfy the requirements of the fair processing condition set out in the first Data Protection Principle. An appropriate Privacy Notice (sometimes called a Fair Processing Notice) must be included wherever personal data is collected.

The purpose of a Privacy Notice is to explain to individuals:

- the identity of the organisation collecting their data, and contact details for their Data Protection Officer (where applicable)
- the purpose for which the personal information will be used, and the lawful basis for doing so
- how long the personal data will be retained
- any other information required to ensure the processing of his/her information is fair - for example:

- a description of any other organisations the information may be shared with or disclosed to
- whether the information will be transferred outside the UK
- the rights available to data subjects in respect of the processing, including that an individual can obtain a copy of his or her information

To ensure transparency, a Privacy Notice should be displayed in a prominent position. Details of how St Anne's uses the confidential information it holds is displayed on its website.

Data Accuracy

Staff who have responsibility for handling any PCD must ensure that it is accurate and as up to date as possible.

All staff members are responsible for checking that any personal information they provide to St Anne's in connection with their employment is accurate and up to date e.g. change of address or name. St Anne's cannot be held responsible for any errors unless St Anne's is informed of them.

Any request or query regarding access to images from the CCTV system operating in St Anne's premises should be referred to the Director of Corporate Affairs/Head of Information Governance.

Right to Opt Out of Processing of Personal Confidential Data

The detailed principles governing how organisations should handle objections is explained in rule 4 of the Health and Social Care Information Centres 'A Guide to Confidentiality in Health and Social Care'.

In summary;

- In all cases, objections should be considered consistently, and individuals should receive an explanation of the likely consequences of their decisions
- Where an objection to the sharing of confidential information is implemented, anonymised information can be shared and
- In rare cases where the likely consequences of an objection pose such a significant risk that the objection is lawfully overruled, individuals should receive an explanation

Disclosure Outside the European Union
(change brought in by Data Protection Act 2018)

St Anne's may, from time to time, need to transfer personal data to countries or territories outside the UK or EU, or to international organisations in accordance with purposes made known to individual data subjects. For example, the names and contact details of members of staff at St Anne's on a website may constitute a transfer of personal data worldwide. If an individual wishes to raise an objection to this disclosure, written notice should be given to the Information Governance Officer.

Other personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures taken, be disclosed or transferred outside the UK or EU to a country or territory, or an international organisation, which does not ensure an adequate level of protection for the rights and freedoms of data subjects.

Under the DPA, the Secretary of State has the power to determine whether a third country (i.e. not an EU member state or other country on the EU's 'approved list')

ensures an adequate level of protection for personal data by reason of its domestic law or the international commitments it has entered into.

Before making any transfer of PCD to a third country or international organisation, staff should confer with the Head of Corporate Governance, or the Information Governance Officer for advice.

Retention of Data

All data retention will comply with the 5th principle of the DPA – i.e. personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

St Anne's will hold different types of information for differing lengths of time, depending on legal and operational requirements, following which it will either be archived or destroyed.

St Anne's 'Records Management, Data Retention and Archiving Policy' and supporting procedures provide further details on retention and disposal of information and reflect relevant Department of Health guidance.

Printouts and paper records must be treated carefully and disposed of securely.

This is also the case with both IT equipment and data. Please refer to 7.04 Information Security Policy for further information.

Interaction with Other Policies and Procedures

This policy should be read in conjunction with relevant sections of the following St Anne's policies and supporting procedures and relevant guidance:

- Information Governance Management Framework
- Information Security Policy
- Records Management Data Retention and Archiving Policy
- Internet and Electronic Mail Use Policy
- Secure Transfer of Information and Safe Haven (Personal Confidential Data) Policy and Procedure
- Data Privacy Impact Assessment Policy

Staff Training

It is mandatory for all new St Anne's staff to undertake the online Information Governance training relevant to their post as part of their induction process.

It is mandatory for all St Anne's staff to complete the online Information Governance refresher training every 1 year.

Staff must inform their Line Manager if they do not understand any aspects of this policy and/or require further associated training.
Any specific training needs identified to ensure compliance with this policy should be referred to the Information Governance Officer.

Monitoring & Review

The Information Governance Officer is responsible for monitoring overall compliance with this policy and shall have authority to update it where amendments are needed to reflect changes to ICO guidance and specifications, statutory or industry guidance and/or legislation and also to reflect changes to internal operational processes and personnel. Any such changes will be notified to the Senior Management Team. The Caldicott Guardian is responsible for monitoring compliance with the confidentiality and data protection requirements of this policy.

This policy is one of the Information Governance policies underpinning the St Anne's Information Governance Management Framework. The Quality Assurance and Risk Management (QUARM) Committee will therefore seek assurances on the overall implementation of this policy when monitoring compliance with the Information Governance Management Framework.

St Anne's are also required to complete the NHS Data Protection and Security Toolkit, which is a mandatory set of requirements care home providers are required to complete in order to monitor our GDPR compliance. The Toolkit is designed to encompass the National Data Guardian review's ten data security standards. It is a way for the organisation to audit and monitor our GDPR and data protection compliance.

As part of a rolling programme to assess the impact of the St Anne's policies, frameworks and procedures on its equality performance, a triennial review of this policy will be undertaken to provide an assurance that its implementation is not having a negative impact on the St Anne's equality performance, and to also identify any positive effects.

The Equality Impact Analysis will also be reviewed in light of any necessary changes to the policy, where this might be performed sooner than the required review

The Equality Impact Analysis will also be reviewed in light of any necessary changes to the policy, where this might be performed sooner than the required review date.

References

- Data Protection Act 2018
- EU General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000 and Environmental Information Regulations 2004
- Human Rights Act 1998
- Common Law Duty of Confidentiality

- Criminal Justice and Immigration Act 2008
- Access to Health Records Act 1990
- Mental Capacity Act 2005
- The Public Health (Control of Disease) Act 1984
- Records Management: St Anne's Code of Practice, parts 1 & 2: January 2009
  Section 46, Freedom of Information Act 2000, Code of Practice for the Management of Records (Department of Constitutional Affairs)
- Information Commissioner's Guidance on the Application of the Data Protection Act 1998 (2002)
- Caldicott Guardian Manual (2010)
- Caldicott Committee Report of the Review of Patient-Identifiable Information (1997)
- Caldicott2 Review 'To Share or Not to Share' (2013)
- Information Commissioner's Use and Disclosure of Health Data Guidance (2002)
- Public Health (Infectious Diseases) Regulations 1988
- Information Commissioners Anonymisation Code of Practice (2012)
- The Health and Social Care Information Centre's 'A Guide to Confidentiality in Health and Social Care'. (2013)
- Information Commissioners Office (ICO) Statutory Data Sharing Code of Practice.
- Equality Act 2010
- Information Security Standard: ISO/IEC 27000 family of standards
- Information Security NHS Code of Practice
- Cyber Essentials/Cyber Essentials Plus
- Confidentiality NHS Code of Practice
- Records Management NHS Code of Practice
- Public Records Act 1958
- Mental Capacity Act 2005
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988

Appendix A

Common Law Duty of Confidentiality

The Common Law Duty of Confidentiality is not written out in an Act of Parliament. It is based on previous court cases decided by judges, so is also referred to as 'judge-made' or case law. The law is applied by reference to those previous cases, so common law is also said to be based on precedent.

The general position is that, if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.

In practice, this means that all PCD, in whatever format held, must not be disclosed (outside of approved and known practices) without the consent of the service user or member of staff, regardless of their age or state of their mental health.

Three circumstances making disclosure of confidential information lawful are:

- where the individual to whom the information relates has consented
- where disclosure is in the overriding public interest
- where there is a legal duty to do so, for example a court order

Where this is not possible, an organisation may be able to rely on disclosure being in the overriding public interest. However, whether a disclosure is in the public interest is not a decision to be taken lightly. Solid justification is required before individual rights are set aside and specialist or legal advice should be sought before the information is disclosed. Any decision to disclose should be fully documented.

Disclosures required by court order should be referred to the St Anne's Information Governance Officer as promptly as possible, so that any necessary representations may be made to the court, for example to limit the information requested. If a disclosure is made which is not permitted under common law the patient can bring a legal action, not only against the organisation but also against the individual responsible for the breach.

There are no clear legal obligations of confidentiality that apply to the deceased. The DH and the GMC agree there is an ethical obligation to relatives of the deceased that confidentiality obligations continue to apply, although disclosures without consent may be necessary to assist a coroner or other similar officer in connection with an inquest or fatal accident inquiry, as part of national confidential enquiries or on death certificates.

Appendix B

DATA SUBJECT ACCESS REQUEST FORM (DAT1)

Data Subject Access Request Policy

Individuals have a right to request access to information held about them in accordance with Article 15 of the General Data Protection Regulation (GDPR). The *right of access* is one of the corner stones of GDPR and the Data Protection Act (2018). In accordance with the GDPR, the reasoning for allowing individuals to access their personal data is that the requester is aware of and can verify the lawfulness of the processing (Recital 63). The right of access means individuals can ask St Anne's to supply them with copies of both paper and computer records, and other related information.

St Anne's aim to process all data lawfully, fairly and in a transparent manner. Generally, St Anne's have to comply with a Data Subject Access Request (DSAR) without undue delay, and in any event, within one calendar month of receiving the request. If however we need to ask the data subject for more information in order to help locate the data, or if we require identification, then the period would only start once the further information has been received. In certain circumstances the request period may be extended by a further two months, and we will inform the requester in writing if this is the case. We would have one calendar to inform the data subject of the two-month extension.

Additionally, if we consider the request to be manifestly unfounded or excessive, we can:

- Charge a reasonable fee, considering the administrative costs of providing the information or
- Refuse to respond

St Anne's would again respond with this information within one calendar month.

Under the Data Protection Act 2018, a request can also be refused if negotiations are currently on-going with St Anne's when the request is made. An example of such negotiations are an on-going legal dispute or grievance.

"*Exemption if personal data consists of records of the intentions of the controller in relation to any negotiations with the data subject where this would be likely to prejudice those negotiations*." Schedule 2, Part 4 (23).

The right of access can be exercised verbally or in writing, either by phone, post or email, or by completing our Data Subject Access Request form. We also require proof of identity, so that we can be certain that we are supplying the correct individual their personal data.

There is nothing to stop someone making a DSAR on behalf of another individual, such as a solicitor. In these cases, St Anne's need to be satisfied that whoever is making the request has permission to act on the data subject's behalf. An example of the type of evidence we require would be written authority to make the request or power of attorney.

If consent cannot be given by the data subject, we will factor in whether the best interests of the individual are being met. Additional steps will need to be taken by the requester to ensure that St Anne's are satisfied that the bests interest of the data subject is at the forefront of the request.

If the requester is asking for personal information of an individual who is now deceased, there is a different data subject access request form which needs to be completed. They can contact St Anne's for the form to be provided by post or email. Additional paperwork will need to be provided along with the form to prove the individual is now the executor of the estate. The evidence can be provided in the form of a copy of the will.

All data subject access requests are signed off by a member of St Anne's Senior Management Team. The staff member who has the final decision on the DSAR will be either the Senior Information Risk Owner (SIRO) or the Caldicott Guardian.

If the person making the request is dissatisfied with St Anne's handling of it, they have the right to ask for an internal review. Internal review requests should be submitted within two months of the date of receipt of the response of the original letter and should be addressed to:

Governance Team
St Anne's Community Services
6 St Marks Avenue
Leeds
LS2 9BN

Alternatively, they can email it to: dataprotection@st-annes.org.uk.

In addition, the Information Commissioner can give advice about the request, and if they think St Anne's hasn't dealt with it properly, they will tell us, and help the requester get the information. The ICO are also available if the requester wanted to make a complaint externally. The Information Commissioner's details are:

Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF

www.ico.org.uk.

1 Details of person requesting the information

Full Name.....

Address.....

.....

Tel No..... Email.....

Are you a member of staff? Yes / No (delete as appropriate)

2 Are you the Data Subject?

Please note that where the term "Data Subject" is used it refers to the person about whom the information is being requested.

2.1 If you are the Data Subject please supply evidence of your identity and a stamped addressed envelope for returning the document (s) requested.

(please go to question 5).

2.2 Are you acting on behalf of the Data Subject with their written authority? If so, that authority must be enclosed.

2.3 If consent cannot be given by the data subject, it will be necessary to take additional steps to ensure the best interests of the individual are being met.
(please complete questions 3 and 4)

3 Details of the Data Subject (if different to 1)

Full name.....

Address.....

Tel No.....

Date of Birth…….

4 Please describe your relationship with the Data Subject that leads you to make this request for information on their behalf.

.....

.....

.....

5 Please describe the information you seek together with any other relevant information. This will help to identify the information you require and if we are able to provide it in accordance with our legal obligations.

.....

.....

.....

.....

Declaration. To be completed by all applicants. Please note that any attempt to mislead may result in prosecution.

I....., certify that the information given on this application form to St Anne's Community Services is true. I understand that it is necessary for St Anne's to confirm my/Data Subject's identity and it may be necessary to obtain more detailed information in order to consider the request and locate the correct information.

Signature.....

Date.....

Note: The period of one month in which St Anne's must respond to the request will not commence until it is satisfied upon these matters.

Please return the completed form to Corporate Affairs, St Anne's Community Services, 6 St Mark's Avenue, Leeds, LS2 9BN. Documents which must accompany this application:

a) evidence of your identity;

b) evidence of the data subject's identify (if different from above);

c) stamped addressed envelope for return of proof of identity/authority documents.

Appendix C

ACCESS TO HEALTH RECORDS ACT 1990 APPLICATION FORM (DAT[X])

Access to Health Records Act 1990 Application Form

Please fill in this application form using BLOCK CAPITALS and black ink.

Section 1: Right of Access – (evidence required)

I am the executor/administrator for the estate of the person who has died ☐

I have a claim arising from the person's death and want to access information relevant to my claim ☐

Section 2: Details of the individual this access request is about

Please fill in this section as fully and accurately as you can with the personal details of the individual this access request is about.

Last name:		**First name:**	
Address (including postcode):			
Date of Birth:		**Sex:**	

If relevant, please provide further details below:

Previous name(s):	
Previous address:	

Section 3: Information You Require

If there is specific information you wish to access, please provide further details below:

Please put an X in the appropriate box to show how you would like to access this information:

1. View records only ☐
2. Receive a copy of the records ☐

Please note the records you request may hold many paper copies of laboratory results which contain figures and letters which may be understood only by a clinical person. Providing a copy of these reports may increase the cost you have to pay. If you wish us to provide copies of results please put an X in the box below.

I wish to receive copies of laboratory results, if any are held ☐

□

Section 4: Declaration

You must sign this section and get it countersigned (please see section 5). The counter signatory should be present when you sign.

I declare that the information I have given in this form is correct and that I am the executor/ administrator of the estate or have a claim against the estate.

I enclose evidence of my right to receive this information and the fee of £10.

Last name:		**First name(s):**	
Signature:			**Date:**
Address (including postcode):			
Phone number:			
Email:			
Relationship to the individual this access request is about:			

Section 5: Countersignature

We require a countersignature because we have confidential information and we must get proof of your identity and your right to receive any relevant information.

Any of the following can sign (this should not be a member of the applicant's family).

- Member of Parliament
- Member of the Scottish Parliament
- Justice of the Peace
- Minister of Religion
- Professional and qualified person (for example, a doctor, lawyer, engineer or teacher)
- Bank Employee
- Civil Servant

- Police Officer

As the person countersigning, you only need to confirm the identity of the person applying and be a witness when they sign the declaration in section 4. You do not need to see the rest of the form.

I (write your full name) _____ confirm that I have known (name of the person applying) _____ for _____ years, and I was present when they signed the declaration.

Signature:		**Date:**	
Full Name:		**Profession:**	
Address:			
Postcode:		**Phone number:**	

Section 6: Further Information

If the criteria in section 1 of the application does not apply to you and you would still like to access records of a deceased person, please provide details of why you require access in the box below:

Please note that access is not an automatic right and applications will be considered on a case by case basis. In extreme circumstances we may release the last episode of care to applicants who do not meet the criteria.