supporting YOUR future

Arbour House School

Data Protection Policy

May 2018

Review Date: June 2019

Title of Document	**Information and Data Governance, Protection and Management Policy**
Policy Ref	Operations
First Issue Date	23 May 2018
Version Number and Re-Issue Date	1.0
Next review date	June 2019
Policy Owner/Author	Lisa Alcorn
Signed off by	Senior Management Team Board of Management
Distribution To	To All Services

Policy Content

1.0 Policy Statement

1.1 Potens recognises it must keep all records required for the protection and wellbeing of Service Users, and those employed by the organisation for the effective and efficient running of the care and support services to comply with the EU General Data Protection Regulation (GDPR).

1.2 This policy has further been developed in line with the data protection requirements found in associated Social Care Regulations in England, Wales and Northern Ireland to ensure Potens, as a Social Care Provider, have effective governance of record keeping with records that are comprehensively fit for purpose and securely maintained.

1.3 The policy applies to all manual and electronic records (including those retained on Caresys, People Planner and similar electronic platforms) kept by the service in relation to:

- Service Users,
- Members of the wider external multi-disciplinary team involved with their care and support and whose personal data might be found on their records,
- All staff
- Any third parties (agencies and professionals), with whom anyone's personal data information held by the organisation who might have to be disclosed or shared.

1.3 To comply with the General Data Protection Regulations (GDPR), the Company understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and electronically.

1.4 This means that all personal data obtained and held by the Company to carry out its activities must:

- Have been obtained fairly and lawfully
- Held for specified and lawful purposes as an organisation that is carrying out a public duty
- Processed in recognition of persons' data protection rights, which are described in the GDPR in terms of the right:
    - To be informed
    - To have access
    - For the information to be accurate and for any inaccuracies to be corrected
    - To have information deleted (e.g. if inaccurate or inappropriately included or the required retention period is deemed to have expired)
    - To restrict the processing of the data to keep it fit for its purpose only to have the information sent elsewhere as requested or consented to (e.g. in any transfer situation)
    - To object to the inclusion of any information (e.g. if considered to be irrelevant)
    - To regulate any automated decision-making and profiling of one's personal data
    - Be adequate, relevant and not excessive in relation to the purpose for which it is being used
    - Supporting business continuity and service delivery by remaining up to date, accurate and avoiding unnecessary duplication
    - Information is retained only as long as required or as directed by legislation and is destroyed appropriately

- Have appropriate safeguards against unauthorised use, alteration, disclosure, damage. loss or destruction with clear procedures for investigating any breaches of the data security
- Information is easily retrievable for those who require access during the course of their duties and for business arrangements, or for those that have a statutory right to request information
- Comply with the relevant GDPR procedures for international transferring of personal data to ensure effective and lawful partnership working with other agencies.

2.0 What is Information?

2.1 For purpose of this policy "Information" relates to all electronic, printed, handwritten information/documents that are created/shared/received/ retained and destroyed by us. This can include but not limited to the following:

2.2 *Service Documents:*

All electronic and printed information relating to clients within services, including handwritten notes, registers, finance information, Service User files, audits and electronic information maintained on Caresys or in any other electronic format.

2.3 *Financial Documents:*

Financial information that relates to Service Users and any information that is only to be seen/processed by those authorised to do so in the course of their duties. This includes electronic data on Caresys, Payroll, email or any other electronic system we use, printed and retained information and handwritten information.

2.4 *Administrative Documents:*

Any information that relates to clients and employees that is processed/retained within Central Offices. This includes but not limited to electronic data on Caresys, stored electronic data on servers/email, any printed information or handwritten notes.

3.0 Data Protection and The GDPR

3.1 Potens has taken the following steps to protect everyone's personal data, which it holds or to which it has access so that it complies with GDPR.

3.2 Potens have a designated Data Controller. This is currently: Lisa Alcorn, Director of Operations.
The responsibilities of the Data Controller include:

a. The processing and controlling of data – ensuring the collation, accessibility, storage and transferring of information is completed in line with the Data Protection principles outlined in this policy.
b. The comprehensive reviewing and auditing of its data protection systems and procedures
c. Overviewing the effectiveness and integrity of all the data that must be protected

This is achieved by way of monitoring the effectiveness and implementation of this policy and associated procedures through embedding this topic into Potens' Quality Assurance System and conducting and evaluating audits across all levels of the organisation.

Potens has a Senior Information Risk Owner who retains the corporate ownership of this policy. The Data Controller communicates Data Protection related issues to the Senior Information Risk Owner via the Potens Board structure.

Potens Senior Information Risk Owner is: Nicky Stadames, Chief Operating Officer.

3.3 Potens provides information to its Service Users and others involved in their care and support on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions Service Users and staff can take if they think that their data has been compromised in any way (e.g. through the complaints procedure or grievance procedure in the case of staff). Please refer to Appendix 1 and 2: Privacy Statements for Service Users and for Employees.

3.4 To comply with the GDPR the Company has logged all personal data types it holds, where it comes from, how it's stored, the legal basis for holding it and who it might be shared with. The log is stored centrally and will be reviewed when the collation of any new personal data types are introduced or the processing of Data is changed.

3.5 The Senior Information Risk Owner arrange for a risk assessments as part of the Company's reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the service.

4.0 Subject Access Request (SAR) by Employees to their own Personal Data

4.1 GDPR gives data subjects the right to have access to their personal data on request. Should employees wish to request access to their personal

data, the request must be addressed to their line manager in the first instance. The line manager must then inform the data controller in writing that a SAR has been made. The following principles will be observed:

- Time to respond: the Line Manager must respond to these requests within a month, with a possibility to extend this period for particularly complex requests.

- Fee: Potens will not charge for complying with a request unless the request is 'manifestly unfounded or excessive'. The Company may charge a reasonable administrative-cost fee if further copies are requested. This will be a maximum of £40 and will be based on the volume of copies requested.

- Content of response: the request should allow the individual to know what information is held about them and what processing is being carried out. In responding to a request, line managers/data controllers may need to provide further information such as the relevant data retention period and the right to have inaccurate data corrected

- Right to withhold: line managers/data controllers can withhold personal data if disclosing it would 'adversely affect the rights and freedoms of others'.

4.2 If a SAR is obtained, the employee is required to read this information carefully and inform their Manager in the first instance and at the earliest opportunity if they believe that any of their personal data is inaccurate or untrue, or if they are dissatisfied with the information in any way.

4.3 In the event of a disagreement between an employee and a Service Manager regarding personal data, the matter should be referred to Potens' Data Controller by either party. The Data Controller will seek to mediate a resolution and outline the outcome in writing. The Data Controller's Outcome is final and there are no further internal opportunities for appeal through the Access to Data procedure. The staff member does have a right to use the Company Grievance Procedure if they remain dissatisfied.

5.0 Access Request by Service Users' to Information held about them

5.1 Service Users should have access to their own records held about them in accordance with the GDPR and be given the opportunity to correct any error or omission. Service Users can be assured that the protection of

their privacy and confidentiality are given the highest consideration.

5.2 All Service Users should have access to their records and information about them as well as opportunities to help maintain their personal records.

5.3 Any Service User requiring access to their files should contact the Service Manager to make arrangements to view. Service Users with sensory or other disabilities must be given appropriate help and support from an independent source as required e.g. advocate.

5.4 The viewing of certain records may only be refused in the following circumstances as consistent with the GDPR:

- Where disclosing the personal data would reveal information which relates to and identifies another person unless that person has consented to the disclosure or it is reasonable to comply with the request without that consent.

- Where permitting access to the data would be likely to cause serious harm to the physical or mental health or condition of the data subject or any other person.

- Where the request for access is made by another on behalf of the data subject, access can be refused if the data subject had either provided the information in the expectation that it would not be disclosed to the applicant or had indicated it should not be so disclosed, or if the data was obtained as a result of any examination or investigation to which the data subject consented on the basis that information would not be so disclosed.

5.5 Before deciding whether the above restrictions apply, the Manager should consult the Health, Social or Education professional responsible for the care and support of the Service User in relation to the request being made. If there is more than one, the most suitable available professional. If there is none, then the Manager should consult a professional with the necessary qualifications and experience to advise on the matters to which the information requested relates.

5.6 Service Users who have a complaint about the way Potens keeps information about them, or who are refused access to files that they believe they should have access to, should follow the internal complaints procedure and be referred to the Information Commissioners Office, should they remain dissatisfied. The ICO can be contacted on 0303 123 1113 or via their website https://ico.org.uk/concerns/

5.7 Potens aims to fulfil its obligations under the General Data Protection Regulations to the fullest extent.

6.0 Requests for Service User Information by Third Parties

6.1 The Service will not provide information to relatives, spouses, friends or advocates without the consent of the individual Service User concerned. If the person is unable to give their consent a decision will be taken in line with "best interests" procedures set by the Mental Capacity Act 2005.

6.2 All enquiries for information, even if they are from close relatives, should be referred back to the Service User or the Service User's permission sought before disclosure. If the relative or person who seeks to have access to this information objects to the decision they will be asked to make a formal written complaint, which will be addressed through the service's complaints procedure.

6.3 Occasionally, other third parties (insurance companies, solicitors, employers, etc) requests information about the Service User. Before providing these reports we shall require written consent from the Service User concerned, or their representative if the service user lacks capacity, and will never divulge information without consent unless obliged to by law. Where the Company believes there is the potential for the Service User being at potential risk due to divulging their personal data, the Manager will seek advice from other professionals involved with the service user to establish if a Best Interest decision to withhold the information should be applied. The action could include referring the case to the local Safeguarding Team.

7.0 Caldicott Principles/ Sharing and Transfer of documents externally

7.1 The Caldicott principles provide guidance to the NHS and Local Authorities on the use and protection of personal confidential data and how it should be shared. Potens understands that health and social care professionals should have the confidence to share information in the best interests of the people supported by the agencies within the framework set out by these principles.

7.2 The Caldicott Principles are as follows.

- Principle 1 — justify the purpose(s) for using confidential information.
- Principle 2 — only use confidential information when absolutely necessary.
- Principle 3 — use the minimum information that is required.
- Principle 4 — access to confidential information should be on a strict need to-know basis.
- Principle 5 — everyone must understand their responsibilities.
- Principle 6 — understand and comply with the law.

- Principle 7 — the duty to share personal information can be as important as the duty to have regard for the person's confidentiality.

7.3 With reference to both the GDPR and the Caldicott guidelines, Potens recognises person-identifiable confidential information as including:

- A Service User's name, address, full postcode and date of birth
- A Service User's NHS number and any notes, records or information about their care or treatment
- Any pictures, photographs, videos, audio recordings or other images of Service Users
- Anything that may be used to identify a Service User directly or indirectly, such as rare diseases, drug treatments or statistical analyses using small sample sizes that may allow individuals to be identified.

7.4 Importantly, the organisation recognises that person identifiable information does not only relate to medical information and can take many forms. It can be stored on computers, transmitted across networks, printed or stored on paper, spoken or recorded.

7.5 The organisation understands that overall there should be a balance between the protection of personal information and the use and sharing of this information between agencies to improve care and support.

7.6 NHS organisations and local authorities will have an allocated Caldicott Guardian who is responsible for agreeing and reviewing protocols for governing the transfer and disclosure of personal confidential data about patients and Service Users. The Guardian plays a key role in ensuring that the organisation satisfy the highest practical standards for handling personal identifiable information.

Potens Caldicott Guardian is: Lisa Alcorn, Director of Operations

7.7 Any personal information 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 concerned. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.

7.8 The Company and its staff have a legal and ethical duty to safeguard the integrity, confidentiality, and availability of sensitive person identifiable information. Every use of person identifiable information must be lawful.

7.9 Individual Service Users have a right to believe and expect that private and personal information given in confidence will be kept securely and used only for the purposes for which it was originally given and agreed to.

7.10 Staff and managers must ensure that, to comply with the Caldicott guidelines:

- Every proposed use or transfer of person identifiable information within or from this organisation should be clearly defined and justified.

- Personal identifiable information should not be used unless it is absolutely necessary and there is no alternative.

- Where use of person identifiable information is considered to be essential, the minimum necessary personal identifiable information should be used and each individual item of personal information should be justified with the aim of reducing identity.

- 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 is transferred or accessible as is necessary for a given function to be carried out.

- Access to personal identifiable information should be on a strict "need to know" basis. Only those individuals who need access to person identifiable information should have access to it and they should only have access to the personal information items that they need to see. This may mean introducing access controls or splitting data flows where one information flow is used for several purposes.

8.0 Confidentiality of Service User Data/ Information

8.1 Potens recognises that it has a duty of confidentiality to the people it supports. The Company regards this as being of the utmost importance and a key part in building a trusting, caring environment where Service Users are safe in the knowledge that their confidences will be kept and where information about them will be protected safely. The Service will:

- Ensure that all files or written information of a confidential nature are stored in a secure manner in a locked filing cabinet and are only accessed by staff who have a need and a right to access them

- Wherever practical or reasonable fill in all care records and Service Users' notes in the presence of and with the co-operation of the Service User concerned

- Ensure that all care records and Service Users' notes, including care plans, are signed and dated.

8.2 The Service will always seek the written permission of its Users prior to sharing personal information about them with anyone else. Rare situations may arise which give rise to exceptions to this duty where confidential information may relate to harm to other Service Users or harm to the person sharing the confidence. In such circumstances the Service reserves

the right for staff to break their duty of confidentiality and to take the information to a senior member of staff. In such rare circumstances:

- The relevant Service User will be informed of the service's position and full details will be discussed with the Service User
- Appropriate notes will be made in the Service User plan and these notes will be open to inspection by the Service User
- The information will only be given to those who absolutely need to know and wider issues of confidentiality of that information will still apply
- The Service User will be free to make a complaint through the service's complaints procedure if he or she considers that the information held about them has not been treated in the confidential manner they should expect.

8.3 People supported by the Company will be told exactly what their personal information will be used for and how it will be stored and shared. This means fully describing how the data will be used and taking into consideration any language requirements or barriers to understanding, such as requirements under the Mental Capacity Act 2005.

8.4 The member of staff performing the initial assessment of a prospective and new Service User is expected to ensure that the new Service User understands the Privacy Notice (Appendix A) have it explained to them and their representatives so that they can appreciate the implications of it as fully as possible and sign it.

8.5 Accessible information designed for people with particular communication needs detailing how the organisation safeguards personal information is provided to those who need it.

9.0 Record keeping and the Development and Storage of Paper Information Records

9.1 All records required for Staff and the protection and support of Service Users and for the effective and efficient running of the service are maintained and should be accessible only to those who require access in the course of their duties. They should be up to date and stored in an orderly and secure manner.

9.2 Service Users and Staff have access to their records and information about them held by the service, the right to correct any error or omission in it, as well as opportunities to help maintain their personal records.

9.3 Overarching Procedural Principles:

- Ensure that all files or written information of a confidential nature are stored in a secure manner in a locked filing cabinet and are only accessed by staff who have a need and a right to access them.

- Be aware that the relatives of a Service User do not have any automatic right of access to that Service User's files and need to have the Service User's permission to see any information on that person. If the Service User lacks the mental capacity to give their permission a "best interests" procedure would then need to be followed in line with the Mental Capacity Act 2005.

- Check regularly on the accuracy of data being entered into computers.

- Always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

- Use computer screen blanking to ensure that personal data is not left on screen when not in use.

9.4 Personal data relating to Service Users or staff should not be printed/ transferred/ transported, unless it forms part of their Hard Copy file and is authorised by the service manager.

9.5 Where personal data is recorded electronically other than Caresys etc, staff should ensure it is not stored on any shared drives or Folders that allow people without authority access to it. Documents of a personal or sensitive nature should be password protected.

9.6 Informal Paper Information Records

- Information in paper format can include basic post notes with confidential information noted on them up to concise client files within services and financial/administrative information held within Central Offices.

- Information that may be noted in an ad hoc format on a post note, note pad, loose piece of paper etc must be safely destroyed by shredding once the information has been transferred to electronic/file system, passed to a relevant person or no longer required.

9.7 Paper Filing Systems in Service

- Each Service Manager is responsible for ensuring a secure and confidential system for storage of staff and client files and confidential information. If files are stored in a Manager's office on shelving, the Manager has the responsibility that no person, whether it is a visitor, client or employee (who would not in the

remit of their duties have reason to view information), is left unsupervised in the office.

- The Managers office door when not in use must be locked with only authorised employees having access to a key to the office.

- Individual staff that are authorised to have access to confidential and personal information will ensure that the paper information they use in the course of their duties will not be left visible and unsupervised. After use it shall be returned to the secure drawer/cabinet.

- Any staff personal/sensitive paper information that may be retained within a service must be filed securely.

9.8 Paper Filing Systems in Central Offices

- Filing cabinets used to hold confidential staff information must be lockable devices with only authorised personnel having access to a key.

- All staff must ensure any confidential information that may be noted on loose paper/post notes etc must be either destroyed once no longer required or retained securely.

9.9 Clean Desk

- All staff must ensure that any confidential/ sensitive paper work they are using is not visible to visitors or those who would not be privy to the information.

- All staff must ensure that during breaks away from their desk e.g. lunch/meetings that any confidential/sensitive information is not left on the desk and that it is locked in a way.

- At the end of the working day all staff should make time to clear their desks of paper work and lock confidential/sensitive/ information in drawers/filing cabinets.

9.10 Duplication of Paper Work

- We acknowledge that documents are duplicated in the course of our operations e.g. invoices are copied and sent to finance. In the event of duplications the last department e.g. Finance will be deemed the owner of the document with the service retaining the invoice for a period of time only as necessary.

- To assist environmental policies and to ensure filing space is effectively utilised duplication will be limited to on a need basis; all

employees/staff should ensure no unnecessary duplication of documents.

10.0 Electronic Information Systems

10.1 Please refer to Potens' IT Policy and Social Media Policy and associated protocols.

10.2 Potens as a company operates and maintains electronic data via a secured monitored server that is backed up . We use software that is updated and protected by the monitored server.

10.3 Encryption Software - Potens uses encryption software called DESlock. This takes the form of full Hard Drive & Email encryption. Email encryption allows you to send encrypted emails when the information that you are sending is deemed sensitive. E.g.: Sending Service User information. Further guidance on its use can be found within the Encryption Protocol.

10.4 Retention periods apply to all electronic data and there is an associated user guide for the archiving of emails.

10.5 Staff must adhere to the laptop security measures outlined in the IT Policy. A laptop risk assessment must be conducted when laptops are issued to employees/staff for use in the course of their duties both on and off site.

10.6 IT Passwords must be updated every 3 months. If staff fail to comply they will be automatically locked out of their account. An IT password security protocol is operational.

10.7 Electronic Software Systems

- Usernames and passwords have been provided to staff at all levels throughout the organisation. An employee's job role will determine what access they have to the company network and Management Information (Caresys) system. Certain access will be restricted for some staff due to the confidential nature of the information e.g. payroll. Passwords throughout the company must be kept confidential.

- Levels of authority apply to systems such as Caresys. Area Managers will approve level of authorisation within service. Regional Director will approve level of authorisation at Area Manager or similar etc.

Line Managers will approve level of authorisation within Central Offices.

11.0 Retention Archiving and Destruction of Documents

11.1 Potens recognises the critical importance of keeping records confidential and respects the right of Service Users and staff to have accurate information stored about them for as long as necessary and required by law.

11.2 All employees have responsibility for ensuring records are retained in line with this policy and that good practice is maintained throughout Potens.

11.3 All managers are responsible for ensuring that they are aware of their personal responsibilities for records management, and for ensuring that their staff are aware of their individual responsibilities. This includes covering records management in induction programmes, personal development plans and identifying and meeting any noted training needs.

11.4 The retention, storage and destruction relates to all records in any format. This includes but is not limited to;

- Paper/manual records;
- Electronic records
- Scanned records
- Photographs and other images including digital;
- CD-Rom, memory cards etc

11.5 Weeding/Review - Examination of records to determine whether they should be archived or destroyed.

This should take place not less than once a year; ideally more often.
When weeding/reviewing documents you should refer to the appendix tables for guidance as to how long to store, archive and/or destroy the record concerned. If you are unsure please discuss with your line manager.

11.6 Retention and Archiving of Information - The continued storage of records for as long as they are required.

11.7 Items to be archived should be place in an appropriate strong archiving box. The contents noted on a sheet inside the box. The box should then be named with the service and allocated an archive reference number. This number should correspond to a service excel sheet accessible in All Services-open access folder. This record should be data locked and backed up on a regular basis so that archiving "audit trail" cannot be lost. The excel sheet shows the Service name as part of the box number, brief description of the box contents, destruction or review date, the name of the staff who archiving, date of archive and any additional notes.

11.8 Services that archive via Head Office should continue to do so. The North East Services should arrange collection and retrieval via the North East Office in Darlington.

- Any archived paper confidential information must be retained securely in archived boxes in locked storage either on/off site in

accordance with Potens' Retention Archiving and Destruction Schedule (Appendix D).

- Electronic information must be archived as advised by policy (Refer to IT Policy).

11.9 Destruction of Information - the process of eliminating records beyond any possible reconstruction.

If records can be destroyed in accordance with the guidance in Potens' Retention Archiving and Destruction Schedule - Appendix D, these should be shredded. If there is a large amount, arrangements to secure the services of a contracted confidential shredding company should be made, with the appropriate certificate of confidential shredding being retained.

- Paper information should only be retained in accordance with the Retention Period Schedule.

- All confidential and personal paper information must be destroyed securely by the following methods
  - Shredded using cross cut shredder
  - By approved external company

- Electronic data must be permanently deleted/destroyed as per policy.

- Potens has a legal responsibility to ensure that computers are disposed of properly. This is regulated by environmental and data protection legislation. Please make IT Support aware of any computers that need disposing of. Do not attempt to dispose of computers yourself as they hold company sensitive data. The IT Dept will arrange for their collection and disposal.

12.0 Governance and Responsibilities

The table below identifies authority for Information Governance, Protection and Management

Senior Information Risk Owner	Nicki Stadames
Data Controller & Caldicott Guardian	Lisa Alcorn

13.0 Data Breach Procedure

13.1 Potens has developed appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences (eg fine).

13.2 Any suspected data breaches, including breaches of confidentiality, should be reported immediately on being discovered using the Incident Reporting procedure including On Call, where appropriate. Incidents involving potential data breach should be fully investigated by a suitably competent and experienced person and findings escalated to the appropriate Regional Director who will share the findings with the Company's Data Controller and Caldicott Guardian.

14.0 Quality Assurance

14.1 Information Management will be included in service and quality audits.

14.2 Escalation and normal reporting procedures will be followed where acts or assessments identify any possible or actual concerns or breaches.

14.3 Information Management assessments (audits) will be conducted in each service and in central offices, no less than bi-annually.

14.4 Data sharing arrangements should be regularly audited, with support and guidance obtained from the relevant local authority Caldicott Guardian wherever necessary.

15.0 Training

15.1 All new staff to Potens are required to complete a Potens Induction that includes a section covering Confidentiality & Security of Information.

15.2 Managers have a responsibility to ensure all staff that access and are required to handle information, are familiar with and have an understanding of policies that form the Information Governance and Management Framework. Policies must be accessible at all times.

15.3 Managers should ensure that everyone is aware of their responsibilities and that a culture of care and due diligence for data security is in place.

15.4 All staff receive up-to-date training on data protection principles, access to records procedures, confidentiality and good practice in entering information on Service Users' records.

15.5 All staff who use the computer system are trained to develop the required skills to protect individual's private data, to ensure data security, and to understand the consequences to them as individuals and the organisation of any potential lapses and breaches of the service's policies and procedures.

15.6 The nominated data controller and staff responsible for data protection and information governance receive appropriate specialised training to equip them for their respective roles and responsibilities under the GDPR and Data Protection Act 1998.

16. Associated Policies, Procedures and Protocols

- IT Policy
- Laptop Risk Assessment
- Security and Unauthorised Access (Buildings)
- Encryption Protocol

17.Appendices (See Policy Folder)

A. Privacy Notice for Service Users

B. Privacy Notice for Service Users – Accessible Format

C. Privacy Notice For Employees

D. Potens Retention Archiving and Destruction Schedule

E. Archiving Record for each service

F. Access to Deceased Service User Records