OR06

EDP Drug & Alcohol Services

Confidentiality Policy

1.0 Statement

1.1 EDP holds and processes personal information about its service users, employees, and other individuals for various purposes (e.g. the provision of services or for administrative purposes, such as HR and payroll).

1.2 At the heart of EDP's confidentiality policy is our commitment to treat people who use our services, staff and other stakeholders with the utmost respect and in a manner which will always aim to preserve their dignity. EDP recognises that unauthorised disclosure may put an individual at risk of harm. We are committed to meeting our legal obligations and associated requirements concerning data protection and confidentiality. These obligations arise from the Data Protection Act 1998 (DPA), the Common Law Duty of Confidentiality, and contractual requirements (such as the NHS Code of Practice: Confidentiality and Caldicott principles) and IG Toolkit.

1.3 EDP will ensure:

- service users and the public are effectively informed and know how to access their information and exercise their right of choice;
- the confidentiality of personal information;
- the security of information;
- that clinical and corporate information is managed in accordance with mandated and statutory requirements.

1.4 We will not routinely disclose information about people who use our services, who are detained in prison, or about staff and the internal business of the organisation to anyone. It is only in exceptional circumstances permitted by law (refer 7.12) that a worker should share information about a service user without informing them and gaining their consent.

1.5 In referring people who use our services to other agencies, EDP will only disclose information, having asked permission directly from the person involved and having their informed consent to do so.

1.6 EDP recognises that there are instances where a better service can be provided by sharing information about a service user with other relevant agencies. This could be to prevent duplication, ensure coordination of services or to protect a child or vulnerable adult. EDP workers should only share such information on a 'need to know' basis and should seek the consent of and inform the service user they are doing this.

1.7 We will make staff aware of the consequences of failing to maintaining appropriate confidentiality and security:

1.7.1 Any organisation that processes personal information faces severe consequences for failing to maintain appropriate confidentiality and security. This includes fines of up to £500,000 for breaching the Data Protection Act, and/or significant reputational damage.

- All people working with EDP, whether as paid employees, in a voluntary capacity, or as contractors are required to sign a Confidentiality Contract to the Service (reference Appendix 1).
- A comprehensive 3rd Party Confidentiality Agreement is required to be signed by parties who have access to assets and premises for a period of time, such as Partner and Specialist Agencies, hardware and software maintenance and support staff, cleaning and other outsourced support services.
- In addition, people working in EDP Criminal Justice services are required to sign the Official Secrets Act (1911-1989).
- Anyone working for EDP who breaches these Contracts will be liable to Disciplinary Procedures, which could be classed as gross misconduct and result in dismissal.

2.0 Scope

2.1 This policy is a core policy and thus applies to all staff. In the context of this policy the term 'staff' is defined as all salaried staff, volunteers, students on placements, trustees and any other individuals accountable to EDP.

3.0 Aims and Objectives

3.1 The Policy aims to:

- Provide guidance for all staff to follow so that they do not inadvertently breach any of the expectations required of them by law. The Data Protection act should not be a barrier to sharing information, but provides guidelines about when and how to share information.
- Inform staff that they are bound by a legal and common law duty of confidentiality to protect personal information they process during the course of their work. This duty is expressed in staff contracts and, for most health professionals, in their own professional codes of conduct.

- Provide guidance on keeping personal information secure and confidential.
- Make staff aware of the correct procedures for disclosing personal information.

4.0 Definitions

4.1 Personal information (or data) means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller (in this case EDP). It includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

4.2 Sensitive personal information (or data) means personal data consisting of information as to: the racial or ethnic origin of the data subject, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), physical or mental health or condition, sexual life, the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

4.3 Confidential information can be any information that relates to services users, staff, their family and friends, however stored.

4.4 Personal information and personal data are used interchangeably in this document.

5.0 Responsibilities

5.1 The Board is ultimately responsible for Information Governance within the organisation and is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

5.2 The Chief Executive Officer has overall responsibility for Information Governance and this Policy within EDP. Implementation of and compliance with this Policy is delegated to the SIRO, Caldicott Guardian and to the members of the Clinical Governance Committee.

5.3 The Director of Operations is the designated Senior Information Risk Owner (SIRO), who takes ownership of EDP's information risk policy,

acts as an advocate for information risk on the Board. The SIRO also reports annually to the Board on IG performance.

5.4 The Director of Operations is the appointed Information Governance Lead (responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the Agency and raising awareness of Information Governance) and Caldicott Guardian. (The 'conscience' of the organisation, providing a focal point for service user confidentiality, information sharing issues and advising on the options for lawful and ethical processing of information as required).

5.5 The Quality and Performance Manager is accountable to the Director of Operations and supports both the SIRO and the Caldicott Guardian to ensure appropriate use of personal information. The Quality and Performance Manager is responsible for assisting the SIRO with reporting and analysing IG incidents, e.g. data protection/confidentiality breaches, reporting and investigation; and for assisting staff on queries relating to information sharing and confidentiality.

5.6 The Directorate are designated Information Asset Owners (IAOs) with responsibility for providing assurance to the SIRO that information, particularly personal information, is effectively managed within their Directorate/Department.

5.7 Senior Managers responsible for the individual or team use paper of electronic record systems must ensure IG policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date.

5.8 Team Leaders will monitor staff practice and discuss any issues relating to confidentiality with regard to service delivery at supervision and team/clinical meetings. They will discuss with Service Managers and appropriate leads decisions in situations where it is not clear as to whether or not information should be shared without the consent of the person to whom the information relates to; this will be documented for auditable purposes (e.g. in service user notes/supervision records).

5.9 All staff and anyone else working for EDP (e.g. agency staff, honorary contracts, management consultants etc.) who use and have access to EDP personal information must understand their responsibilities for data protection and confidentiality, which include adherence to policy and confidentiality clauses in the contract, the Data Protection Act, Common Law of Confidentiality, and professional obligations e.g. Confidentiality NHS Code of Practice and professional codes of practice.

6.0 Implementation

6.1 Information Sharing & Consent

Additional Practice Guidance for the sharing of information can be found in information sharing guidance for practitioners and managers published by HM the government. This guidance focusses on supporting front-line practitioners who have to make case-by-case decisions about sharing personal information, where decisions about information sharing may be less clear. The Seven golden rules are:

- The Data Protection Act is not a barrier to sharing information but provides a framework.
- Be open and honest.
- Seek advice.
- Share with consent where appropriate.
- Consider safety and well-being.
- Necessary, proportionate, relevant, accurate, timely and secure.
- Keep a record.

6.1.1 At initial meetings with people who use EDP's services, the worker will explain responsibilities regarding confidentiality to the individual. They will explain how information will be kept confidential and when and what they would need to share. If at any point it seems appropriate to repeat this to the individual to help them and reaffirm working practice then it should be repeated. Refer also to P22 Service User Rights and Responsibilities Policy.

6.1.2 All individuals must be informed that information is confidential to the Team, and not to the individual worker, and why that is so.

6.1.3 All confidentiality/consent agreements will be signed and dated by service users and staff and kept in the care record.

6.1.4 Additional information regarding a service user's right to confidentiality and access to their records should be readily available to service users if requested. (Refer to Appendix 3: Service User Information Leaflet: Care and Personal Information and Confidentiality).

6.1.5 If workers are in doubt over any instance, they should always consult with their line manager.

6.1.6 If the friend or relative of a person using the service is also using EDP services, information should not be given from one friend to another, again without specific permission.

6.1.7 Workers should not give information about a user of EDP's services or member of staff to anyone outside the organisation, either voluntarily or on request, unless the person concerned has specifically given their permission, preferably in writing (permission given at assessment can constitute permission in writing). Where possible, workers should verify the identity of the person making the request and should say they cannot confirm or deny that the person is accessing the service unless the service user has given consent to share the information with the individual, except where a recognised exception applies (Refer to 7.12)

6.1.8 In Media work, EDP will not use any information that could identify a service user unless they have their express permission and the service user has signed a disclaimer form. Where a service user does agree to be named in any of this work, the risks to them doing so should be clearly outlined and the worker needs to be satisfied that these have been understood. In training or educational this will also be done wherever practical.

6.1.9 Workers should be able to clearly and respectfully explain to people the reasons why they cannot share information. Where the person making the request is struggling to understand the policy or there is a Safeguarding issue, they should be referred to the worker's line manager.

6.1.10 Workers should not access any files or documents to which they do not have appropriate authority to access.

7.0 Working Guidelines

7.1 Multi-agency working

7.1.1 As EDP works in close collaboration with a number of other agencies, the boundaries of confidentiality with each worker must be clear and information sharing protocols must be adhered to.

7.1.2 Where three-way work is undertaken with a service user, worker and professional from another agency, the bounds of confidentiality between all three should be agreed and documented at the outset, with copies to all three parties. This may constitute Informed Consent, and thereby enable all parties to share relevant information routinely.

7.1.3 Where the service user is satisfied it is in their own interest for information to be divulged to EDP by other professionals, workers should ask to see a signed consent form from the

service user. If time is of the essence, verbal assurance that the service user has given their Informed Consent will suffice with professionals with whom we have a standing working relationship, particularly if we can gain written consent retrospectively. Any verbal assurance needs to be documented in case notes. EDP accepts faxed copies of consent forms.

7.1.4 At assessment and review, it is routine to ask the service user which other agencies and professionals they are already in contact with. They are then asked if we have permission to discuss relevant matters with them, to facilitate sharing of information, and this should be clearly documented in case notes.

7.1.5 When service users consent to service provision and sensitive information relating to their health and other matters is obtained:

- Staff will respect their privacy and act appropriately.
- While there may be an expectation among most service users that their information will be shared to provide that healthcare, EDP has a duty to ensure that service users understand how their information is to be used to support their healthcare and that they have no objections.
- Where this has been done effectively, consent can be implied, providing that the information is shared no more widely than absolutely necessary and that "need to know" principles are enforced.
- It is important to check that service users understand and are content for information to be disclosed to other organisations or agencies contributing to their healthcare.
- Service users may wish to restrict what their relatives/carers are told about their healthcare and should be encouraged to be very explicit if there is anyone that they do not want to be given information.
- In the event of the service user being unable to give permission a person must be identified to provide permission on behalf of the service user.
- In all cases, the wishes expressed by the service user must be appropriately documented in the case notes.

7.1.6 Confidentiality policies are not intended to prevent the exchange of information between different professional staff when it has the purpose of:

- Ensuring the protection of children under the Children Act 1989, 2004.
- Ensuring the protection of vulnerable adults.
- Ensuring the protection of service users believed to be at risk of self-harm.

- Ensuring the safety and security of service users, staff or the wider community.
- Ensuring acceptable standards of professional practice.
- Monitoring and research where full name and address are not recorded.
- Ensuring the protection of the public, where there is evidence of risk of serious harm.
- The prevention, detection or prosecution of serious crime.
- Meeting requirements of a court (NB. This can involve **all** clinical notes being subpoenaed).
- Giving information regarding a serious crime which has been committed, such as a murder, manslaughter, rape, treason or kidnapping (Police and Criminal Evidence Act 1984).
- Giving information about suspected terrorism (Prevention of Terrorism Act 2005).
- Meeting the requirements of the Mental Health Act 2007 where a service user objects to their 'nearest relative' being consulted re:-
  - An application for Treatment Order (Section 3) is being considered
  - An application for assessment and/or treatment in relation to the service user has been made
- Meeting the requirements of the Mental Health (Patients in the Community) Act 1995 where the service user is known to have propensity to violent and dangerous behaviour

Specific guidelines regarding confidentiality when working with under 16 year olds are set out in P11 Working with Young People Policy.

7.1.7 Where EDP routinely and justifiably shares personal data with other organisations, e.g. to support continuity of care, the ICO recommends that a data sharing agreement is drawn up between the affected organisations. Where service user information is shared the agreement will usually be authorised by the Caldicott Guardian.

7.1.8 All records or any material about individuals must be kept secure, with the person's informed consent (see P07 Record Keeping Policy, and OR10 Information Security Policy). Individuals must be informed that some Records will be kept on a Computer in accordance with the Data Protection Act.

7.1.9 Staff are encouraged to challenge strangers or those who may not be authorised to be in parts of the site.

7.2 Access to personal records - Subject Access Requests

Principle six of the DPA provides individuals with the right to access personal information held about them by EDP.

7.2.1 Service user access to their records:

Service User requests for access to their care record are managed by the Service Manager who should check regarding what information can and cannot be shared in accordance with the guidelines below and OR01 Data Protection Act 1998 (DPA) Policy or if in doubt, with the Caldicott Guardian. When a copy of records (original or copy) are requested the Caldicott Guardian must be notified on receipt of requests and approve release of records. Refer Subject Access Request Guidance Documents available on Sharepoint.

The DPA stipulates that a copy of the service user's care record must be released to them within 40 calendar days, subject to receipt of a written request and payment of the appropriate fee. EDP must provide information in an intelligible format (clearly written in an unambiguous way).

However, EDP is not required to supply copies of care records if the:

- Individual requesting the information has not provided enough support information in order for the information to be located, and/or they have not supplied the appropriate fee.
- Retrieval of the care records requires disproportionate effort.
- Identity of a 3rd party would be revealed if disclosed.

A service user requesting access to their records/files may be refused access to parts of the information if an appropriate health professional deems exposure to that information could cause physical or mental harm to the service user. Health professionals should be prepared to justify their reasons in a court of law if necessary.

In all cases reasons for non-disclosure should be documented.

If a service user or their representative is unhappy with the outcome of their access request, e.g. information is withheld from them or they feel their information has been recorded incorrectly, the service user or their representative can:

- Meet the lead worker to resolve the complaint.
- Utilise EDP's Complaints procedure.
- Take their complaint direct to the Information Commissioner.

7.2.2 Staff access to their personnel record:
Employee personal information is also governed by the Data Protection Act and their rights of access to information, privacy, dignity and confidentiality remain the same as for service users. All information held in a member of staff's personnel file is confidential and must be kept securely. However, EDP supports a 'no surprises' culture and managers should offer their staff reasonable access to their own personnel files.

Members of staff may formally request access to information held about them by sending a letter or email to the Human Resources Manager, who will:

- Liaise with the relevant line manager and Head of HR to identify what information should be supplied.
- Ensure that the information is reviewed prior to disclosure.
- Request and process the fee from the applicant (should this be considered necessary e.g. retrieval of archived data).

Managers must bear in mind that staff are entitled to access all information EDP holds about them and this information should be disclosed unless there are lawful grounds for withholding it.

Information given in confidence about a member of staff may not offer grounds for withholding that information, although it may be possible to redact information to respect the privacy of third parties.

7.3 Keeping Personal Information Secure and Confidential

7.3.1 Keeping personal information secure and confidential is essential and staff are required to familiarise themselves with and follow the EDP Confidentiality Guidelines detailed in Appendix 4: Quick Reference Guide: Confidentiality and Information Sharing. The Guidelines provide all staff (including contractors on how to ensure the:

- security of electronically held records, including use of passwords and mobile devices;
- physical security of paper records.

7.3.2 Security of electronically held records

- Personal passwords issued to employees should be regarded as confidential and passwords must not be communicated to anyone else. Sharing of passwords constitutes a breach of EDP policy.
- Staff must not put any identifiable, confidential or sensitive information onto removable media or on laptops without encryption of such devices.

- Staff must not use their personal devices, e.g. iPads, Smartphones to capture and store personal information, e.g. photographs, digital recordings.

7.3.3 Physical security of paper records

Paper records and other confidential documents should be:

- Physically protected from unauthorised access, damage and interference.
- Kept in secure areas with appropriate entry control and security barriers.
- Staff should are encouraged to challenge strangers or those who may not be authorised to be in parts of the site.
  - Offices containing personal identifiable information and care records should be locked when unoccupied and contain lockable cabinets.
  - Support facilities and equipment, e.g. photocopiers should be sited appropriately within a secure area to avoid demands for access which could compromise the confidentiality and security of information. The secure print option should be used where available when printing confidential information.
  - External doors and windows should be locked when unattended and external protection, e.g. alarm systems used where fitted.
  - Monitoring access to key facilities and information to ensure relevant and appropriate access to confidential information should also be considered.

7.3.4 Working from home

The rules of confidentiality are the same whether working from an office, in the community or at home. While at home, staff have a personal responsibility to ensure any personal information taken off site is kept secure and confidential. No other member of family and/or visitors must be able to see EDP-related personal information.

Staff must not save any work-related information to their home PC/laptop' particularly identifiable, confidential or sensitive information.

7.4 Use of Service user Data for Non-Healthcare Purposes

7.4.1 Use of service user personal data for non-healthcare purposes typically falls into the categories of Clinical audit, Research or Service evaluation. This use of service user information must also comply with the DPA and Caldicott principles.

7.4.2 *Clinical audit* (usually conducted by those involved in service user care, and overseen and approved by the Clinical

Governance Committee). Where an audit is to be undertaken by the team that provided care, or those working to support them, service user identifiable information may be used assuming implied consent, provided that service users have been informed that their data may be used for this purpose and have not objected

7.4.3 *Research* (usually undertaken in partnership and conducted with explicit service user consent). The use of service user identifiable information for research requires explicit informed consent. When seeking consent for disclosure, you must ensure that the service users are given enough information to allow them to make a considered and informed decision. Specifically, they should be informed of the reasons for the disclosure, the way that it will be made and the possible consequences. The exact amount of disclosure and the identity of those who will receive it should also be explained.

If a service user cannot be contacted to give consent, it should not be assumed that their care details can be used for research purposes.

7.4.4 *Service evaluation and other non-healthcare activities*. For service evaluation and other non-healthcare activities, minimal service user identifiable information may be used providing the principles below are strictly followed

The purpose of the processing must be identified in a fair processing notice.

- The purpose of the processing must be approved in advance by the respective IAO.
- Anonymised or pseudonymised data should be used wherever possible. Where pseudonymised data is used, the key must be known only to minimal numbers of staff. Use of any identifiable data must be justified.
- Where personal data is justified, e.g. to follow a specific service user through a pathway, only process the minimum personal data required to fulfil the purpose, e.g. NHS number or hospital number. The data collected must not be used for a different purpose without further authorisation.
- Outputs (e.g. reports, from service improvement/evaluation activities, should be anonymised unless use of personal data can be justified.
- Access to personal data for service improvement/evaluation activities is restricted only to EDP staff who need to process it.
- Personal data must be stored and transferred securely, and when no longer required must be disposed of securely. Data

repositories (e.g. spreadsheets/databases containing personal data) must be registered in the Directorate's Information Asset Register.
- All staff who have access to personal data must be up-to-date with their IG training.

7.4.5 *Use of Service user Data for Training*

Most service users understand and accept that the education and training of students and trainees relies on their having access to information about service users. In most cases, anonymised information will be sufficient and should be used whenever practicable.

If students are part of the team providing or supporting a service user's care, they can have access to the service user's personal information like other team members, unless the service user objects.

Therefore, service users must be asked to provide their consent, to allow a student/trainee clinician to sit in on a consultation and it is the lead clinician's responsibility to ensure that the service user is under no pressure to consent.

7.4.6 *Use of Service user Data for Systems Testing*

The ICO advises that the use of actual personal data for system testing should be avoided. Where there is no practical alternative to using live data for this purpose, systems administrators should develop alternative methods of system testing. Should the ICO receive a complaint about the use of personal data for system testing, staff must be able to justify why no alternative to the use of live data was found.

7.5 Safe Transfer of Personal Information

7.5.1 Confidential information should only be taken out of the office with the express permission of line managers. This information should be kept in a locked case and workers should ensure that any work they need to do outside of the office cannot be seen by anyone else and is locked away when not being worked on. Under no circumstances should confidential information be removed from Prison establishments without the permission of the Governing Governor.

7.5.2 Workers should not access any files or documents to which they do not have appropriate authority to access.

7.5.3 Staff should adhere to the procedures below when personal information is being transferred from one person or organisation to another.

Fax Transfers

Fax transfers are considered a high risk method of communicating personal information and use is minimised where practical by EDP. Safe haven procedures should always be followed.

The term 'Safe Haven' is a term recognised throughout many organisations, including the NHS, to describe the administrative arrangements to safeguard the confidential transfer of service user identifiable information and other sensitive information between organisations or sites. When information is disclosed through a designated safe-haven point to an equivalent point in another organisation, staff can be confident that agreed protocols will govern the use of the information from that point on.

'Safe Haven' facsimile machines should be sited in areas where the general public and, if possible, staff from other organisations, do not have physical access. Many facsimile machine models can be set to store information stopping the fax printing out until a designated member of staff activates the machine by entering a secure PIN. If your fax machine is not in a secure environment or you receive faxes outside office hours, consider other arrangements such as 'fax to e-mail' solution

If you have reason to send and/or receive a fax which contains service user identifiable information and/or other sensitive information, please ensure that a 'Safe Haven' facsimile machine is used at both ends, whenever possible.

The following sets out good practice when sending faxes:

- Telephone the recipient of the fax to let them know you are about to send it.
- Check the fax number. If the information is confidential, ask them to wait by the fax.
- Consider asking the recipient to confirm receipt of the fax; or call them to ensure the fax has arrived.
- Use pre-programmed fax numbers where possible to reduce the chance of the fax being sent to the wrong machine.
- Ensure that you use an appropriate fax cover sheet. Make sure your cover sheet states who the information is for, and mark it 'Private and Confidential'.
- Ensure you do not refer to the names of the person(s) concerned in the subject heading or on the cover sheet of the fax.
- Keep a record that you have sent the fax.

If the information is not for you, either pass it to the proper recipient or inform the sender - please do not ignore it;

Telephone Enquiries

Service users have a right to privacy so we must respect their wishes about what information is shared over the phone, unless we have a justified reason to speak to someone on their behalf, e.g. it is in their best interests. Where it is justified, information may be given if certain precautions are taken. These include:

- Ensuring that procedures are carried out to confirm/verify the identity of the caller, e.g. verifying the information we have about the service user (i.e. DoB, address, etc.) and that it is appropriate that they receive the information being asked for.
- Taking a phone number that can be checked against records and phoning back from a location where the conversation cannot be overheard.
- Messages should not be left on answer phones and staff should ensure that 1471 cannot be used to recall the number. It would be a breach of confidentiality to leave a message, unless there is explicit consent to do so.

Sending confidential information by post

Confidential correspondence should be clearly addressed to a known individual and secured in a sealed envelope marked "Private and Confidential". This information can be sent via routine mail services.

Confidential documents, e.g. service user records, a confidential report or other personal papers, should be:

- Securely sealed in an inner envelope clearly addressed to a known contact and marked "Private and Confidential - To be opened by the addressee only".
- Securely sealed in a 2nd outer envelope clearly addressed to a known contact.
- Marked "Private and Confidential" and "If undelivered please return to – name, organisation, address" must be clearly marked on the reverse side.
- Dispatched via Special Delivery.
- Tracked and a confirmation of receipt obtained and kept.

Emailing confidential information securely

All staff are reminded of the risks associated with sending, forwarding and receiving emails which contain sensitive and/or confidential information, which may be service use, carer, staff, contractor or business related.

Using edp.org.uk to edp.org.uk is the recommended way to send confidential information securely by email. EDP mail to other mail addresses is NOT a secure route and sensitive data is at risk if sent this way without additional protection e.g. password protected files, than none at all. Alternate methods of data transfer should also be considered, for instance where regular information transfers occur between services, individual staff may be assigned multiple email addresses. Examples of secure and insecure data transfers are:

Secure	Insecure
edp.org.uk to edp.org.uk	edp.org.uk to riserecovery.org.uk
riserecovery.org.uk to riserecovery.org.uk	edp.org.uk to poole.gov.uk
gsi.gov.uk to gsi.gov.uk	gsi.gov.uk to edp.org.uk
gsi.gov.uk to nhs.net.	

Staff should include the minimum level of personal information that is required and ensure that the intended recipient has a legitimate need for the information. Consideration should be given to sending anonymised information.

There are some exceptions where it may be acceptable to send sensitive data in a way other than specified above. For example, if there is a greater risk of harm to an individual if we do not communicate information (e.g. child protection). Or it may be possible to send data by reducing the information that would identify the individual to a minimum, so that the authorised recipient would know who the service user was, but an unauthorised user would not. In these cases it is better to offer some protection, e.g. password protected files, than none at all.

7.6 Disclosures

Guidelines for various forms of disclosure are provided below. If in doubt about any disclosure, please seek guidance from the Caldicott Guardian or Manager of Quality and Performance.

7.6.1 *Police requests*

- All requests from the police for information about service users and/or their relatives should be forwarded to the Service Manager. When a copy of records (original or copy) are requested the Caldicott Guardian must be notified on receipt of requests and approve release of records.
- Requests from the police for information about members of staff should be forwarded to the Head of HR or the Directorate.
- Common requests relate to the prevention, detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others. Examples include murder, rape, child protection concerns, serious assault.

- In deciding whether we disclose confidential personal information a key consideration is whether the public good outweighs our obligation of confidentiality to the individual concerned. Whoever authorises the disclosure must make a clear and accurate record of the circumstances, the advice sought and the decision making process followed so that there is clear evidence of the reasoning used and the prevailing circumstances.
- Disclosures should also be proportionate and be limited to the relevant details. It may be necessary to justify such disclosures to the courts or to regulatory bodies.

7.6.2 *Solicitors' requests*

Solicitors usually act on behalf of service users when they approach us for information. Requests for service user information in relation to a claim against EDP should be forwarded to the Director of Operations. The Director of Operations, as Caldicott Guardian, should also be notified of other requests and approve release of records.

7.6.3 *Service users*

Typically, these requests have the express consent of the service user affected.

7.6.4 *Court orders*

This is a written directive from a judge stating exactly what information is needed, for what purpose and by when.

Service Managers should forward Court orders promptly to the Director of Operations who will approve release of information.

A court order does not require the consent of the individual affected, however, they should be informed, preferably prior to disclosure. Disclosures must be strictly in accordance with the terms of the court order and to the bodies specified. A clear and accurate record of the circumstances should be kept.

7.6.5 *Requests about children, young people or vulnerable adults*

Any requests for information about children or vulnerable adults should be forwarded to the Safeguarding Officer.

7.6.6 *Disclosures to support external investigations*

NHS Fraud, the Coroner's Office and professional regulatory bodies, such as the Nursing Council, may compel staff to provide personal and confidential information to support an investigation.

However, staff may seek advice from HR to ensure that any information disclosed is appropriate and not excessive.

No staff should provide witness statements without first consulting HR.

7.6.7 *Disclosing information against the Service User's wishes*
The responsibility of whether or not information should be withheld or disclosed without the service user's consent, lies with the senior manager involved at the time and cannot be delegated.

Circumstances where the service user's right to confidentiality may be overridden are rare; examples of these situations are:

- Where the service user's life may be in danger or cases when the service user may not be capable of making an appropriate decision.
- Where there is serious danger to other people, or where the rights of others may supersede those of the service user.
- Where there is a serious threat to the worker.
- Where there is a serious threat to the community.

7.6.8 *Disclosures to Government Department*
All requests to EDP in relation to staff or service users e.g. from Department of Work and Pensions, Her Majesties Revenues & Customs shall be promptly forwarded to the Director of Operations (service users) and HR (staff) and require accompanying service user consent.

7.6.9 *Disclosures from Close Circuit Televisions (CCTV)*
EDP has responsibility for CCTV data which is used for security purposes at a number of its sites. EDP is registered with the Information Commissioners Office (ICO) for it's use and an annual review of the CCTC usage in line with ICO recommendations will be undertaken.

7.6.10 *Disclosure of service users after death*
The Data Protection Act applies only to living individuals. However, our duty of confidentiality continues after death. An ethical obligation to the relatives of the deceased exists and records of the deceased are public records, governed by the provisions of the Public Records Act 1958. This permits the use and disclosure of the information within them in only limited circumstances.

The Access to Health Records Act 1990 permits access to the records of deceased by anyone with a claim arising from the death of the service user. This right of access is negated,

however, if the individual concerned requested that a note denying access be included within the record prior to death (this might be part of a formal advance directive).

The Service Manager shall promptly advise the Director of Operations of any requests. Refer to Data protection Act Policy for further advice.

7.7 Disposal of Confidential Information

The effective management and disposal of waste materials that contain confidential person identifiable information, or confidential corporate information, is the responsibility of all staff.

For the secure and confidential disposal all staff are asked to ensure that confidential waste:

- Is either placed in the confidential waste sacks/console units provided, which must be located in a position out of direct view of the door/window. Or
- shredded, using the cross- shredding machines provided.

Examples of confidential waste include both paper and digital media that contain:

- Service user data (e.g. name, address, date of birth, phone number, care/service number, clinical information, etc.)
- Individual staff data (e.g. sickness records).
- Any documents with 'restricted access'.
- Drafts of contentious documents.
- Diaries which contain personal details.
- Job application forms.

7.8 Privacy Impact Assessments (PIA)

7.8.1 Any new (or significantly changed) system or process where personal data is processed must be subjected to a PIA at an early stage in the project. The aim is to identify any unacceptable risks to an individual's privacy. The PIA (identifying what data is processed, who has access to the data, where data is stored) is usually approved by the Caldicott Guardian. Refer to Privacy Impact Assessment Template.

7.8.2 External suppliers involved in processing and/or storing the data (e.g. EDP IT provider, new data storage providers) will be expected to demonstrate adherence to national standards of information security, e.g. 'satisfactory' IG Toolkit submission, ISO 27000 certification.

7.9 Consequences of policy breaches

7.9.1 Disciplinary Proceedings

In an instance where an individual worker has been found to have inappropriately breached Confidentiality, this should be reported as an incident and the Team Leader/Manager must address this and the action taken should take into account the effects of a Breach of Confidentiality on the Service, the organisation and the individual concerned.

Breaches of confidentiality without justifiable reason or failing to safeguard confidential information may constitute gross misconduct and may result in dismissal for a first offence.

Examples include staff who access their own personal data (manual and electronic held records) or that of their families, friends, or colleagues, even if they have been given that individual's permission to do so.

Any reported confidentiality breach will be raised with the Head of HR and relevant Director to take forward in line with EDP's Disciplinary Policy.

7.9.2 Legal Proceedings

The Information Commissioners Office has a number of tools available for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit. The ICO also has the power to serve a monetary penalty notice of up to £500,000 on a data controller.

7.10 Training and policy awareness

7.10.1 Training

- IG training is mandated at corporate induction and thereafter annually with a minimum target of 95% completion across EDP. Provision is available online or face to face and includes data protection and confidentiality issues.
- Training needs will be reviewed annually through the workforce development planning process which will consider the needs of all staff and of specific roles such as the Caldicott Guardian, SIRO, and Service Managers. Details of training to support delivery of this document are covered in EDP's Training Needs Analysis.
- Where additional training needs identified for individuals or groups (e.g. through monitoring and audit activities) these will be addressed appropriately.
- A copy of this policy and relating policies and procedures will be posted on EPD's Intranet (SharePoint) and where a service

has no access to SharePoint a controlled hard copy may be retained.

- All staff are made aware of their responsibilities for Information Governance at induction and annually as part of their mandatory training and development.
- The Manager of Quality and Performance ensures regular promotion of data protection and confidentiality matters through EDP e-news, briefings, posters, leaflets and committees.

8.0 Monitoring and Review

8.1 Monitoring compliance with Confidentiality obligations is essential for EDP to protect the rights of service users, staff in compliance with the law and contractual obligations. It is also plays an important role in service improvement. It will be monitored through audit, supervision, staff and service user surveys, incident reports, complaints, feedback and spot checks - the outcome of which will be reported through EDP's defined committee structure and management processes.

Appendices

Appendix 1 – External Contractor Confidentiality Agreement (Standard)
Appendix 2 – Confidentiality Agreement for Third Party Suppliers (Comprehensive)
Appendix 3 - Service User Information Leaflet: Care and Personal Information and Confidentiality
Appendix 4: Quick Reference Guide

OR06 – Confidentiality Policy Version 5		
Summary:	To understand our responsibilities and obligations to service users, staff and any other individuals who disclose personal information to the organisation under the Data Protection Act 1998 (DPA), the Common Law Duty of Confidentiality, best practice NHS Code of Practice: Confidentiality and Caldicott principles and the IG Toolkit	
Related Legislation:	Data Protection Act 1998 (DPA) Common Law Duty of Confidentiality NHS Code of Practice: Confidentiality Caldicott principles IG Toolkit Children Act 1989, 2004 Police and Criminal Evidence Act 1984 Prevention of Terrorism Act 1998 Mental Health Act 1983 Mental Health (Service users in the Community) Act 1995	
Related Policies:	HS01 Health and Safety at Work Policy HR07 Whistleblowing (Confidential Reporting) Policy OR01 Data Protection Act 1998 (DPA) Policy OR08 Information Governance Policy OR10 information Security Policy P07 Record Keeping Policy P11 Working with Young People Policy P15 Safeguarding Children Policy P16 Safeguarding Vulnerable Adults Policy and Procedure P22 Service User Rights and Responsibilities Policy	
Next Review Date:	October 2017	
Approved by (Head of Department):	Directorate	**Date:** 16 March 2015
Ratified by:	Clinical Governance Sub-Committee	**Date of meeting:** 11 May 2015
Date issued:	August 2015	
Author:	Sue Dormer	
Reviewers/contributors: Quality & Performance Manager	Sue Dormer	**Date:** January 2015

Version Control

Change Record

Date	Author	Version	Page	Reason for Change
July 2010	Head of Finance	1	All	Updated due to company reorganization and leglislation change
March 2015	Manager Quality & Performance	2	All	Updated due to changes in external requirements and compliance with IG Toolkit

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives, but should always be accessed from the intranet.