CORPORATE SERVICES

POLICY DOCUMENT

Data Protection Policy (INTERIM)

Owner:	**Director of Corporate Services**
Author:	**R Gillies / A Philip**
Version Number:	**3**
Version Date:	**31/10/2017**
Current Published Version Approved by:	**-**
Equality Impact Assessment Number:	**EqIA-**
Review Date:	**3 Years from Date of Publication**

Data Protection Policy (INTERIM)

Contents

Data Protection Policy

Introduction

The purpose of this policy is to set out the Sacro policy on data protection and compliance with the Data Protection Act 1998.

Sacro collects, uses and shares personal information about staff, volunteers, contractors, people from other organisations and service users (data subjects), in order to exercise its responsibilities and duties of care as an employer and service provider and to fulfil its legal and contractual obligations.

Sacro must comply with the Data Protection Act 1998 (DPA), Privacy and Electronic Communications (EC Directive) Regulations 2003 and Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 and any new requirements implemented under and/or arising from the General Data Protection Regulation 2016 (GDPR) and related privacy legislation.

This legislation requires Sacro to respect the privacy, rights and freedoms of individuals while fulfilling its obligations as a data controller. Sacro's approach to this is consistent with its values and principles. Sacro regards complying with its legal responsibilities to protect personal data as very important to its continued success, and to maintain trust and confidence in the organisation.

Policy Statement

Sacro is committed to protecting the privacy, rights and freedoms of individuals and meeting its obligations with respect to the processing of personal data in accordance with the:

- Data Protection Act 1998, and the spirit of the Act
- Associated legislation, including the General Data Protection Regulation
- Case law
- Sacro notification with the UK Information Commissioner
- Privacy Notice published on the Sacro website

Scope of the Policy

This policy applies to all Sacro staff, whether permanent or temporary, volunteers, Board members, contractors and others directly involved in delivering Sacro business activities or acting on Sacro's behalf. The policy uses the term "Staff" to encompass all of these groups.

Equality Impact Assessment

In accordance with the Equality Act 2010, Sacro aims to design and implement policies and procedures that meet the diverse needs of our services and workforce, and seeks to ensure that no person is placed at a disadvantage to any other person.

In accordance with Sacro's Equality Impact Assessment (EqIA) policy and procedures, this document has been assessed for its impact upon equality, and reflects the findings of anything identified by the EqIA procedure.

Data Protection Principles

The Data Protection Act (DPA) sets out eight principles governing the use of personal information with which all staff must comply, unless an exemption applies, to ensure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Not transferred to other countries without adequate protection

Responsibilities

Sacro is the Data Controller under the DPA. The Director of Corporate Services, supported by the Corporate Management Group, has lead responsibility for ensuring Sacro complies with the DPA and associated legislation. The Chief Executive is held accountable for this by the Sacro Board.

All Sacro staff are responsible for complying with the DPA in relation to their roles in Sacro.

Compliance

All staff, volunteers, contractors or other persons provided access to Sacro data are required to comply with the:

- Data Protection Act 1998
- Sacro Data Protection Procedures
- Sacro Information Security Policy
- Sacro IT Policy and Procedures
- Associated Sacro policies, procedures and guidance on the provisions and practical implementation of the DPA.

These requirements apply to all personal data related to a living individual who can be identified from that data, created and received, regardless of where it is held and irrespective of the ownership of the equipment used, if the processing is for Sacro purposes.

Any breach of the Sacro Data Protection Policy and Procedures may result in Sacro or the individual concerned being legally liable for the consequences. Sacro reserves the right to take disciplinary action against any individual member of staff, or to cancel the engagement with any third party where there has been any abuse or breach of this policy.

Monitoring and Review of Policy

The Data Protection Policy will be reviewed annually by the Director of Corporate Services, and in line with any legislative changes. Amendments to the Policy will be approved by the Board, on recommendation from the Audit Committee.

The Corporate Management Team is responsible for ensuring staff understand and comply with the data protection measures that are in place to support the implementation of the Data Protection Policy.

DATA PROTECTION PROCEDURE

Introduction

Sacro needs to collect, use and share personal information about staff, volunteers, contractors, people from other organisations and service users (data subjects), in order to exercise its responsibilities and duties of care as an employer and service provider and to fulfil its legal and contractual obligations.

Sacro must comply with the Data Protection Act 1988 (DPA), Privacy and Electronic Communications (EC Directive) Regulations 2003, Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, and any new requirements implemented under and/or arising from the General Data Protection Regulation 2016 (GDPR) and related privacy legislation. The implementation of GDPR in the UK is being led by the Information Commissioner's Office and Sacro will monitor developments and take any necessary action when necessary.

This legislation requires Sacro to respect the privacy, rights and freedoms of individuals while fulfilling its obligations as a data controller. Sacro's approach to this is consistent with its values and principles. Sacro regards complying with its legal responsibilities to protect personal data as very important to its continued success, and to maintain trust and confidence in the organisation.

Scope

The Data Protection Procedure applies to all personal data created or received in the course of Sacro business in all formats: paper, electronic or communicated verbally face to face or by means of a telephone or other such device(s). It relates to all data subjects (an individual who is the subject of personal data).

It applies to anyone who obtains, records, can access, store or use personal data in the course of their work for Sacro. Users of personal data include all of Sacro workers (employees, sessional workers, agency workers, contractors and volunteers) and board members. It applies to all locations from where Sacro personal data is accessed, including remote access.

'Personal data' means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller. 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.

'Sensitive personal data' means personal data consisting of information as to the data subjects:

- Racial or ethnic origin,
- Political opinions,
- Religious beliefs or other beliefs of a similar nature,
- Membership of a trade union (within the meaning of the m1trade union and labour relations (consolidation) act 1992),

- Physical or mental health or condition,
- Sexual life,
- Commission or alleged commission of any offence, or
- Involvement in proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

The general rule is to handle and use information about other people as carefully as you would want other people to handle and use information about you.

Purpose

The purpose of this document is to ensure that all staff are aware of their legal and moral responsibilities to protect the data that we gather in order to conduct our business and to provide services to the people that have asked for our help. This document sets out core responsibilities, procedures and guidance in support of Sacro's Data Protection Policy to ensure that Sacro can demonstrate its respect for the privacy, rights and freedoms of individuals while fulfilling its obligations as a data controller in accordance with its registration with the Information Commissioners Office, and its responsibilities in relation to good governance, risk and compliance management.

This should enable Sacro to comply with the related legislative requirements. Key to this is compliance with the **Data Protection Principles**, which in summary state that personal data shall:

1. Be processed fairly and lawfully and, in particular, shall not be processed unless for personal and sensitive personal information certain conditions are met (page 9)
2. Be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes (page 11).
3. Be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Be accurate and, where necessary, kept up to date.
5. Not be kept for longer than is necessary for that purpose or those purposes.
6. Be processed in accordance with the rights of data subjects under this Act.
7. Have appropriate technical and organisational measures taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Accidental or deliberate misuse, loss or disclosure to third parties of personal data presents significant legal, financial and reputational risks, including fines of up to £500,000 under the DPA and under the GDPR up to 2% of turnover or up to the equivalent of 10 million euro in sterling, dependent upon the type of breach.

In order to manage these risks and contribute towards Sacro demonstrating its legislative compliance, this procedure sets out responsibilities for all categories of people that can

access or use personal data in their work with Sacro. It also sets out the governance and accountability framework for data protection compliance across Sacro. This includes reference to policies and procedures necessary to protect Sacro information by maintaining:

- **Confidentiality:** protecting information from unauthorised access and disclosure.
- **Integrity:** safeguarding the accuracy and completeness of information and preventing its unauthorised amendment or deletion.
- **Availability:** ensuring that information and associated services are available to authorised users whenever and wherever required.

Responsibilities

Overall responsibility for proper administration and compliance with data protection legislation lies with the Chief Executive and is exercised through the Corporate Management Group.

The Director of Corporate Services has been appointed as the Director responsible for Data Protection and all related matters. This includes the roles of senior Information Risk Owner and Information Asset Owner.

In addition, each National Office Manager, Service Manager, and Service Team Leader, has delegated day-to-day responsibilities for compliance with the Data Protection Act 1998 within their areas of authority. The following key responsibilities apply:

Board members

- oversight of compliance with policy, governance, risk and compliance
- compliance with the law and holding the Chief Executive to account

Chief Executive

- Leadership in relation to policy, governance, risk and compliance
- Compliance with the law, accountability to the board of trustees

Corporate Management Group

- Leadership in relation to creating and reviewing policy, governance, risk and compliance and creating a privacy and security culture within Sacro
- Providing a Security Group function
- Maintain registration with ICO Data Controller Register
- Oversight of the effectiveness of the day to day management of related practice and procedure in their areas of responsibility
- Providing appropriate guidance and training
- Compliance with the law, accountability to the Chief Executive

Senior Managers

- Leadership in relation to implementing policy and a privacy and security culture
- Day to day management of related practice and procedure
- Applying the approach described in this document relevant to their role
- Authorising access to personal data for the services they manage on a “need to know” basis
- Managing subject access rights for the services they manage

- Providing information on services where there is personal and personal sensitive data to the director of corporate services for notification to the information commissioner's office data protection register
- Accountability to their directors and the corporate management group

All users of Sacro information

- Complying with their responsibilities under the legislation
- Reading and complying with associated policy, procedure and guidance
- Adopting a privacy and security culture
- Undertaking related training and awareness activities
- Using personal data only for the purposes for which it was originally obtained
- Using data fairly, taking good care of it, taking all necessary steps to prevent data breaches
- Ensuring that it is: adequate, relevant, not excessive, accurate, up to date, and not held for any longer than necessary
- Reporting all suspected privacy and information security breaches so that appropriate action can be taken to minimise harm
- Notifying the human resources department of any changes of information in connection with their employment
- Applying the approach described in this document relevant to their role remembering it is a criminal offence to access personal data that you are not authorised to access, or disclosing it to people who you are not supposed to disclose it to, whether knowingly, or recklessly
- Remembering it is a criminal offence to sell personal data that you are not entitled to sell.

Approach

Sacro will adopt "privacy by design" principles when developing and managing new information systems used for processing personal data. This means Sacro will:

- Adopt data minimisation - collect, disclose and retain the minimum personal data, for the minimum time necessary for the purpose or purposes it was collected;
- Anonymise personal data wherever necessary and appropriate – such as for research or statistical purposes.

Sacro will apply the principles of the DPA to the management of all personal data by doing the following, while monitoring developments of the GDPR in the UK.

Data Principle 1: Fair and Lawful Purposes

Each year Sacro receives referrals about people who require support, guidance or monitoring to reduce reoffending to benefit communities and society. Sacro processes personal data in connection with these and related purposes. Sacro's Director of Corporate Services has notified the Information Commissioner's Office that Sacro is a data controller. Further information is available on the ICO Data Protection Register.

The conditions for processing are set out in Schedules 2 and 3 of the Act. At least one of the following conditions must be met to process **personal data**;

- The individual about whom the personal data is about has consented.
- The processing is necessary:
  - In relation to a contract which the individual has entered into;
  - Because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to Sacro (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". (This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident).
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- The processing is in accordance with the "legitimate interests" condition for Sacro as a data controller.

In relation to **sensitive personal data**, at least one of the following conditions must also be met before the processing can comply with the first data protection principle:

- The individual whom the sensitive personal data is about has given explicit consent to the processing.
- The processing is necessary so that Sacro can comply with employment law.
- The processing is necessary to protect the vital interests of:
  - the individual (in a case where the individual's consent cannot be given or reasonably obtained), or
  - another person (in a case where the individual's consent has been unreasonably withheld).
- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. (Additional limitations apply to this condition).
- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
- The processing is necessary for administering justice, or for exercising statutory or governmental functions.
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

When collecting, creating and using personal data, users of Sacro information must:

- Make sure the individuals concerned, understand who is collecting this (Sacro or Sacro in partnership with another organisation)
- Collect and use personal data only in accordance with the conditions of the Act;
- Collect only the minimum necessary for the purpose it is need for;
- Be fair and open, tell people why their information is collected and what is done with it;
- When starting a new service, consider if a Privacy Impact Assessment is necessary;

- Treat people fairly by using their personal data in a way in which they would expect and for the purposes which they allowed Sacro to collect it;
- Contact the person concerned for their authorisation to use their personal information for a different purpose e.g. in annual reports, for media purposes.
- Do not use their personal information in ways that unjustifiably has a negative effect;
- Base recorded comments (negative or positive) on facts that can be defended as accurate when challenged;
- Remember people have the right of access to information recorded about them;
- Record personal information only in authorised systems – do not start an unauthorised record keeping system;
- Provide privacy information to people when their personal data is collected through the publication of a Privacy Notice on the website and other ways that suit individual circumstances.

Data Principle 2: Informed and Explicit Consent and Confidentiality

Sacro does not exclusively rely on consent to process personal and sensitive personal information, it will seek the consent of individuals to collect and use their personal data whenever it is appropriate or the law requires it. The Act makes a distinction between consent for personal data and explicit consent for sensitive personal data and provides "conditions" that must be met for processing such information.

The Act does not provide a definition of consent, however Article 2(h) of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data and GDPR 2016 requires that consent must be:

- Freely given;
- Specific;
- Informed;
- Unambiguous and consist of any indication by which the data subject signifies agreement.

The GDPR requires some form of affirmative action, which must be verifiable in the form of a record of how and when consent was given. Provision must also be made for the withdrawal of consent at any time. Consent should cover all processing activities carried out for the same purpose or purposes.

The individual's consent should be absolutely clear. It should cover the specific processing details; the type of information (or even the specific information); the purposes of the processing; and any special aspects that may affect the individual, such as any disclosures that may be made.

Consent must also be appropriate to the age and capacity of the individual and to the particular circumstances of the case and should be kept under review as Sacro's relationship with an individual develops, or as the individual's circumstances change.

There are circumstances when it is not appropriate to seek an individual's consent to process their data. Sensitive personal information can be processed without consent if, amongst other reasons more fully referred to in the act, there is:

- a life and death situation and either consent cannot be obtained or it is reasonable to proceed without it;
- data related to ethnic or racial origin, disability or religion and which is being processed to monitor equal opportunities;
- a legal obligation to process the information in connection with employment.

Employees should check with the Director of Corporate Services if they are uncertain as to whether or not their work comes into a special category. In most cases there are limitations to the extent to which the conditions may be fulfilled. For further information, see Schedule 3 of the Data Protection Act 1998, as implemented by the Data Protection (Processing of Sensitive Personal Data) Order 2000 (UK Statutory Instrument No. 417/2000)

Data Principe 2: Inform data subjects what Sacro is doing with their personal data

Sacro has published a Privacy Notice on the website that sets out a general description of how it will process personal data. This will be kept under review.
At the point of collection of personal information users of Sacro information must explain in a clear and accessible way the following:

i. Information collected in a face-to-face meeting or on a form (paper or internet)

- That the personal information is being collected by Sacro (or Sacro in partnership with another organisation);
- What their rights are in relation to their personal information and what the obligations are as a data controller;
- What personal data collection is voluntary and what is necessary and why (adequate, sufficient, relevant not excessive);
- Why personal data collection is mandatory and why Sacro are entitled or obliged to process their data, for example in relation to employment;
- How Sacro record it, store it, and secure it and protect their privacy;
- How the information will be used;
- What personal data Sacro collect;
- The purpose it is collected for;
- The length of time for which the information will be kept;
- How Sacro will securely delete or dispose of personal data;
- Whether or not the information could potentially be disclosed to a third party and to whom it may be disclosed;
- Who can be contacted for more information;
- Where consent is obtained verbally, this must be recorded and kept on the individual's file;
- Why Sacro needs the data subject to sign a consent form;
- What personal information Sacro may publish and why (e.g. some employees' names on the website;
- How data subjects can update their personal data;

In addition, a membership form will make clear:

- How the person can indicate that they do not wish to receive direct marketing material i.e. there is an “opt out” box;
- Whether or not the information could potentially be disclosed to a third party, and that there is an “opt out” for this section.

ii. Information collected by telephone

The person’s identity must be confirmed through the asking of questions that only the data subject would be able to answer. At all times be aware of the increasing amount of fraud and identity theft.

All of the information that is referred to in the previous section must be explained to the individual concerned, and employees must ensure that the data subject has fully understood these details and implications.

All the information collected will be stored in the appropriate system (computer or manual). If the information is collected verbally and the person has indicated their desire to ‘opt out’ of any part (e.g. their information being passed on to a third party) this will be recorded.

iii. Information provided by a data subject that has not been specifically requested

All persons processing personal information on behalf of Sacro must consider the fairness and legal basis of any such processing.

Further guidance for all Sacro users of personal data is provided in the Sacro Confidentiality Policy and from Service Managers. Guidance is also provided in the Sacro Privacy Notice published on the website and in consent forms referred to in Sacro’s Case File Management and Recording Practice in Criminal Justice Services Policy and Case File Management and Recording Practice in Criminal Justice Services Practical Guidance.

Data Principle 3 - Adequacy, relevancy and not excessive

Sacro will only hold personal data about an individual that is sufficient for the purpose for which it was collected and no more than is needed for that purpose.

Sacro records have been designed to document the minimum personal information necessary and all users of Sacro’s data should consider this aspect and refer any concerns about the adequacy, relevancy or excessive nature of personal information processed to their line manager for consideration by the Director of Corporate Services.

Sacro and users of Sacro information will:

- Seek to apply data minimisation in relation to personal data processed;
- Keep under review the personal and personal sensitive data processed;
- Only collect the minimum information needed in relation to an individual;
- Where opinion is recorded, clearly record the date, authors name and position;

- Where an opinion recorded is likely to be controversial or very sensitive, or if it will have a significant impact when used or disclosed – the author will provide detail on the circumstances or evidence it is based on;
- Where an opinion recorded summarises more detailed records held elsewhere, this should be made clear;
- Establish and maintain a records management policy and records retention schedule and users will conform to this;
- Keep records only as long as required in accordance with the records management policy and records retention schedule;
- Delete or dispose of records in a manner appropriate for their format; or
- Arrange for their longer term storage or archiving as appropriate.

Data Principle 4: Accuracy and where necessary up to date

Sacro will take reasonable steps to ensure that personal and sensitive personal data it processes is accurate, that the source of such data is clear and consider any challenges to the accuracy of such data and whether it is necessary to update the record.

Sacro and users of Sacro information will take the following steps:

- Keep records as accurate as possible by checking and confirming with the source at the time;
- Record accurately information provided by the individuals concerned, or by another individual or organisation;
- Where appropriate pass on corrections to the relevant area within the organisation or to the relevant external organisation;
- Support individuals rights, where a record is found to be incorrect, delete it or correct it and consider keeping a record relating to the correction;
- Provide contact information in a Privacy Notice and at the point of contact, about how to raise a concern regarding accuracy of any records or provide information to Sacro to keep a record up to date;
- Where there is a challenge about the accuracy of a record, record that its accuracy has been challenged;
- Where there is any dispute regarding accuracy that cannot be resolved, refer the matter to line management and where necessary escalate this to the Director of Corporate Services;
- Where the individual concerned is not satisfied advise them of their right to apply to the court for an order for Sacro to rectify, block, erase or destroy the inaccurate information;

Data Principle 5: Retain personal data only as long as necessary for the purpose it was obtained

Keeping personal data no longer than necessary can help reduce the risk that it will become inaccurate, out of date or irrelevant. It can also reduce the risk of a data security breach. In the majority of cases it is a matter for Sacro to determine the retention period for the personal data it holds, although some periods are specified by legislation for example matters relating to tax. Further detail is provided in the Sacro Records Management Policy and Records Retention Schedule.

It is necessary to review the length of time personal data is kept, consider the time in relation to the purpose(s) it was obtained for, securely delete information that is no longer needed for the purpose(s) and update, archive or securely delete information if it goes out of date. Retaining data longer than necessary can cause difficulties in securely managing, storing and responding to data subject access requests.

Sacro and its users of Sacro information will:

- Establish and maintain a records management policy and records retention schedule users will conform to this;
- Keep records only as long as required in accordance with the records management policy and records retention schedule;
- Delete or dispose of records in a manner appropriate for their format; or
- Arrange for their longer term storage or archiving as appropriate;
- Review and audit what personal data is held by them or processed through data processors, and destroy all personal data that is no longer necessary;
- File or delete incoming and outgoing emails once the action they relate to is complete;
- Ensure they do not keep emails containing personal sensitive data in their mailbox indefinitely;
- Review the contents of their mail box folders at regular intervals and file anything that requires to be retained in the appropriate corporate information system;
- Implement a records management audit.

Data Principle 6: Maintain individual's data subjects rights

Sacro will maintain data subjects' rights to:

- Access a copy of their personal data (subject access), responding in a timely, fair and approachable manner;
- Object to processing that is likely to cause or is causing unwarranted and substantial damage or distress;
- Have inaccurate personal data rectified, blocked, erased or destroyed – in certain circumstances;
- Claim compensation for damages caused by a breach of the DPA or GDPR as appropriate;
- Prevent processing for direct marketing, object to decisions being taken by automated means;

Upon receipt of a written request and, where appropriate, payment of the set fee, Sacro will tell the data subject whether Sacro is processing any of their personal data, give a description of the personal data, the reasons it is being processed, and whether it will be disclosed to others, they will also be given a copy of the data where it is available. A response will be provided within 40 calendar days.

i. Requests for access to a service user's personal data by a person other than that service user

All requests for information by third parties in respect of a service user must be made either in person at the local service's offices, or in writing.

ii. Requests for Access within Sacro

Personal data relating to a service user will always be regarded as having been provided to Sacro, and not to a particular member of staff, and communication of personal service user data between colleagues within Sacro will only be conducted on a 'need-to-know' basis.

iii. Requests for Access by other People

Personal data relating to a service user will only ever be shared with people out with Sacro if they are, or they may be, directly involved in providing a service to the service user, for example, to members of other social care agencies, and only if the requested information relates directly to this purpose. In these and all other cases, requests to provide information relating to a service user will normally only be met if the service user has been consulted, and has given his/her agreement to the disclosure of such information, other than in accordance with exemptions in law.

Data Principle 7: Protect personal data

Sacro will protect personal data by applying appropriate organisational and technical measures. It will:

- Maintain an Information Security Policy supported by an IT Policy and Procedures with guidance on the protection of manual and digital records, and require all users of Sacro personal data to read and comply with these policy and procedures;
- Provide appropriate levels of security and encryption to prevent unauthorised access and modification to personal data stored on authorised devices;
- Where data forms part of a Relevant Filing System, adequate security will be afforded to prevent, as far as is reasonably practical, unauthorised access;
- Where data sharing is routinely necessary do so with an appropriate legal basis with all parties with whom data the data is shared do so under a written agreement or Memorandum of Understanding.
- Control access to personal data on a "need to know" basis, collect only the minimum necessary and keep it no longer than necessary in line with the records retention schedule;
- Require all users of Sacro personal data to complete initial information governance training and ongoing refresher training;
- Provide ongoing advice, guidance and instructions to all users of Sacro personal data on measures to maintain the privacy of personal data;
- Erase or destroy all personal data once the need to hold it has passed in accordance with the Records Management Policy and Records Retention Schedule. The method adopted will be appropriate to the medium (paper or digital).
- Review and maintain agreements to disclose or share personal data processed to ensure proper governance, accountability and control;
- Manage all subject access requests and third party requests for personal data to prevent privacy breaches;

- Obtain written requests for a disclosure and maintain an audit trail of any disclosure made;
- Securely delete or dispose of personal data to prevent privacy breaches;
- Review and maintain written contracts with processors that are contracted to process personal data to ensure the security measures they take meet what Sacro expects;
- Review and monitor Sacro's status in relation to Cyber Essentials;
- Provide users of Sacro's personal data with secure means to communicate personal data remotely through the use of a secure virtual private network, encryption and cloud solutions;
- Make advice and guidance available from Service Managers or the Director of Corporate Services in relation to any intended disclosure;
- Where a large transfer of personal or personal sensitive data is considered necessary – this cannot be done without the prior authorisation of the Director of Corporate Services

Data Principle 8: Sending personal data out of the country

There may be occasions when it is necessary for Sacro to transfer data outside of the European Economic Area. Transport means physically transporting the data overseas in addition to electronic means of transportation such as email, cloud storage etc. In all cases the Director of Corporate Services must be consulted in order that the following can be considered:

- The position regarding the consent of the data subject(s);
- The position of any contract in place which provides equivalent protection of individuals' rights;
- The approval of the destination country by the information commissioner; or
- The application of an exemption from the limitations in the act.

Monitoring and Compliance

Sacro requires that its staff and its data processors comply fully with its data protection policy, procedure and the terms of the Data Protection Act. Sacro reserves the right to take disciplinary action against any member of staff, or to cancel any contract of engagement with any data processor where there has been any abuse or breach of this policy.

The Director of Corporate Services will monitor this area of risk and update the corporate risk register and escalate risk as appropriate in accordance with the Sacro approach to corporate risk management.

Compliance with this procedure and related risk exposure may be subject to audit.

A performance management framework with key indicators contributing towards the outcome of Sacro demonstrating its compliance with privacy related matters will be maintained by the Director of Corporate Services and monitored by the Corporate Management Group.

Links to Other Sacro Policies

The following documents must be read and complied with by all Sacro users of personal information:

- Privacy Notice
- Case File Management and Recording Practice in Criminal Justice Services Policy
- Case File Management and Recording Practice in Criminal Justice Services Practical Guidance
- Data Subject Access Procedure
- Open Access Policy and Procedures
- Records Management Policy
- Records Retention Schedule.
- The Use of Social Media Websites for Business Purposes
- End of Employment Procedures
- Fraud Prevention Policy
- IT Policy and Procedures
- Information Security Policy
- Whistleblowing Policy
- The Protection of Vulnerable Groups Scheme Policy

Legal, Regulatory and Guidance

In order to comply with UK and Scottish law, appropriate data protection and information security controls are necessary. While legislation places an obligation on organisations there are related codes of practice and guidance material to support organisations in complying with the law, managing risk and protecting the privacy rights and freedoms of individuals.

The following lists includes legislation, codes of practice and guidance (not exhaustive) that places an obligation on all organisations in relation to data protection, information security and record keeping or provides guidance:

- Computer Misuse Act 1990
- Data Protection Act 1998
- Human Rights Act 1998
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- Regulation of Investigatory Powers Act 2000
- Regulation of Investigatory Powers (Scotland) Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Freedom of Information (Scotland) Act 2002
- Privacy and Electronic Communications Regulations 2003
- Environmental Information (Scotland) Regulations 2004

UK Information Commissioner's Office (ICO) Statutory Codes of Practice, including:

- Anonymisation
- CCTV

- Data Sharing
- Employment Practices
- Privacy Notices
- Personal Information Online
- Subject Access

UK Information Commissioner's Office (ICO) guidance, including:

- Bring Your Own Device
- Cloud computing
- Data controllers and data processors: what the difference is and what the governance implications are
- Data security breach management
- International data transfers
- IT asset disposal
- Privacy Impact Assessment
- Privacy and Electronic Communications - general

Appendix 1: Key Terms and Definitions

The DPA provides a number of terms and definitions. Where they have not been defined elsewhere in this document, they are listed below for quick reference:

'Data' - information that is:

- being processed by means of equipment operating automatically in response to instructions given (for example payroll systems);
- recorded with the intention that it should be processed by means of such equipment (for example computer disks, CD Rom or data entry sheets);
- recorded as part of a manual filing system where information relating to an individual is readily accessible;
- one of a number of records to which public access is allowed.

'Data Controller' must be a "person" recognised in law, that is to say individuals, organisations and other corporate and unincorporated bodies of persons. In Sacro's case it is Sacro the corporate body. Sacro determines the purpose for processing personal data and is responsible for compliance with the Act.

In relation to data controllers, the term jointly is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons share a pool of personal data that they process independently of each other. From time to time Sacro may be a joint data controller in relation to services run in a partnership and in accordance with a written agreement.

'Data Protection Act' - refers to the Data Protection Act 1998, and the EC Data Protection Directive (2006/24/EC)

'Data Processor' - means any person or company, other than an employee of Sacro who processes data on behalf of the data controller (for example an agency that performs an outsourced payroll function).

'Data subject' means an individual who is the subject of personal data (i.e. the individual whom personal data is about or any person who Sacro obtains and records information about).

'Inaccurate data' - for the purposes of this Act data are inaccurate if they are incorrect or misleading as to any matter of fact.

'Personal data' - means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller. 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.

'Processing', in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data,
- retrieval, consultation or use of the information or data,
- disclosure of the information or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data.

'Relevant Filing System' - means any data that is recorded as part of a filing system or with the intention that it should form part of a filing system.

'Recipient' - in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

'Sensitive personal data' - means personal data consisting of information as to the data subjects:

- Racial or ethnic origin,
- Political opinions,
- Religious beliefs or other beliefs of a similar nature,
- Membership of a trade union (within the meaning of the m1trade union and labour relations (consolidation) act 1992),
- Physical or mental health or condition,
- Sexual life,
- Commission or alleged commission of any offence, or
- Involvement in proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Third party, in relation to personal data, means any person other than the

(a) data subject,

(b) data controller, or

(c) any data processor or other person authorised to process data for the data controller or processor.