CORPORATE SERVICES

POLICY DOCUMENT

Data Sharing Procedure (INTERIM)

Owner:	**Director of Corporate Services**
Author:	**R Gillies / G Stott**
Version Number:	**2**
Version Date:	**31/10/2017**
Current Published Version Approved by:	**-**
Equality Impact Assessment Number:	**EqIA-**
Review Date:	**3 Years from Date of Publication**

Data Sharing Procedure (INTERIM)

Contents

Data Sharing Procedure

Introduction

Sacro collects a range of personal data for Sacro's purposes in delivering services and to meet legal requirements in relation to employment and taxation. There are times where it is necessary for Sacro to share some of the personal data it collects.

This procedure sets out the key points that Sacro needs to ensure are in place in relation to sharing/disclosing the data it collects. This is necessary in order to fulfil its contractual and legal obligations, including compliance with the Data Protection Act 1998 (DPA).

Readers of this procedure must also read Sacro's Data Protection Policy and related policy, procedures and guidance and in particular the Confidentiality policy.

Scope of the Procedure

This procedure applies to anyone who obtains, records, can access, stores, share/discloses or uses 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. This procedure applies to all personal data recorded by Sacro, not just that of service users.

Purpose

The purpose of this document is to ensure that all staff are aware of their legal and organisational responsibilities in relation to sharing personal data processed by Sacro.

Types of Data Sharing

Data sharing falls into two main categories. Firstly, routine (systematic) data sharing where the same sets of data are shared within Sacro and between organisations for an established purpose. Secondly, one off (*ad-hoc*) decisions to share data for any range of purposes. Both types of sharing are a form of "data processing" under the DPA.

The details of systematic sharing between organisations can be developed through the use of a Memorandum of Understanding (MOU), sometimes referred to as an Information Sharing Agreement (ISA) or Data Sharing Agreements or Protocols. In essence, these agreements amount to a set of common rules binding on all the organisations involved in the agreement. These agreements are kept under review by the Director of Corporate Services.

Systematic sharing also takes place within Sacro within individual services where Sacro staff share information within a service where it is necessary in order to provide the service for an individual. This is done on a "need to know basis". There must be a legitimate business objective for sharing data. A record should be made in the relevant case file, where such data is shared.

Where new systematic sharing is being developed, for example in relation to Sacro working with other service providers, any MOU or ISA will be signed off by the Director of Corporate Services. A checklist for developing systematic data sharing with third parties is available at Appendix A.

Ad hoc sharing often requires the exercise of professional judgement, particularly in emergency situations. In the event of any doubt advice can be obtained from the relevant Service Manager or the Director of Corporate Services. A record should be made in the relevant case file, of the circumstances, what was shared, why and how.

To be clear, access within Sacro to personal or sensitive personal data processed by Sacro is only permitted where there is a legitimate "need to know". It is wrong to assume just because personal data is held by Sacro that anyone at Sacro can access it.

It is a criminal offence under Section 55 of the DPA to knowingly or recklessly obtain or disclose personal data or the information contained in personal data, or to provide this to another person, without the consent of the data controller (Sacro).

Conditions for Processing Personal Data

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.

For Sacro as a data controller to fairly and lawfully process personal data, at least one of the following conditions must be met:

- 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.

Conditions for Processing Sensitive Personal Data

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 trades 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.

For Sacro as a data controller to fairly and lawfully process sensitive personal data, at least one of the following conditions must also be met in addition to one of the conditions at 6.1 above, to 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.

Consent

The consent referred to in the previous sections is an important aspect of processing personal and personal sensitive data. The Data Protection Directive, on which the UK Data Protection Act 1998 is based, defines consent as:

"Any freely given specific and informed indication of his (hers) wishes by which the data subject signifies his (hers) agreement to personal data relating to him (her) being processed."

This requires an active communication where the individual (data subject) knowingly indicates consent. Where consent is relied upon, the individuals giving their consent must do so based upon Sacro providing them with a clear understanding of what personal or sensitive personal data is involved and what the implications might be for them.

Consent or explicit consent is most likely to be required in cases where:

- Confidential or particularly sensitive data is going to be shared without a clear legal basis for doing so;
- The individual would be likely to object should the data be shared without their consent; or
- The sharing/disclosure is likely to have a significant impact on an individual or group of individuals.

Sacro will ensure individuals are provided with appropriate information, verbally and in writing, to allow them to provide specific and informed consent, wherever this is appropriate in relation to Sacro processing personal and personal sensitive data.

Where consent is withdrawn by an individual, the Director of Corporate Services must be informed so that the necessary steps can be taken.

Data Sharing Decisions

In making decisions in relation to sharing or not sharing personal data, Sacro and its staff will consider the potential benefits and risks, to individuals, society and in relation to Sacro as an organisation. Key questions that can help in making such decisions include:

- What is the objective of the sharing?
- Can the objective be achieved with anonymous data – e.g. when planning services?
- Is there a clear and lawful purpose for sharing?
- Is the proposed data sharing fair?
- Does the sharing fit with the terms of our privacy notice, consent arrangements and notification with the Information Commissioner's Office?
- Is there a concern that an individual is at risk of serious harm?
- Does an exemption (see paragraph 10.1) under the DPA need to be applied?
- What risk does the data sharing create – is there risk of harm to an individual, will it undermine trust?
- Is there adequate transparency about the proposed sharing – does the data subject need to be advised in advance of the proposed sharing?
- What is the minimum information that is needed to be shared to meet the objective?
- Is fact distinguished from opinion in the data to be shared?
- Is the data personal or personal sensitive in nature?
- Who requires access to the shared personal data?

- Is the information to be shared on a "need to know" basis only?
- Are restrictions to be included on any onward sharing of data with third parties?
- When should it be shared – ongoing or one off?
- How should it be shared – have the rules around the security of the means (electronic, paper, verbal) been considered?
- Have Sacro adequately identified who the data is to be shared with?
- Is the data sharing achieving the objective?
- Does the sharing need to take place without the knowledge of the data subject?
- Has there been a consideration of where the decision is to be recorded, what is shared, how, when, who with, the justification and if it was done with or without consent?

Decisions in relation to sharing or not sharing personal data should be recorded including, where appropriate, responses relating to the questions above.

Fairness and Transparency in Data Sharing

The DPA requires that personal data be processed fairly. Sacro will take reasonable steps to make individuals generally aware of which organisations their data may be shared with and for what purposes.

Sacro understands that the need to communicate Privacy Notice/Consent information is particularly important where sharing:

- sensitive data; or
- is likely to be unexpected or objected to; or
- is widespread, involving organisations individuals might not expect; or
- being carried out for a range of different purposes; or
- sharing or not sharing might have a significant effect on the individual.

Sacro will publish and maintain a Privacy Notice on the Sacro public facing website. A similar notice will be used in the Sacro Privacy Notice/Consent Form. The key components of the notice will include details of:

- Who Sacro is as the data controller;
- Why Sacro may share their personal data; and
- Who Sacro may share their personal data with.

Sacro recognises that some individuals may require assistance in understanding the content of any Sacro Privacy Notice/Consent notice. Sacro encourages members of staff and volunteers to read over and discuss what giving consent to processing including sharing/disclosing personal and personal sensitive information means to them. In addition, Sacro will provide individuals, particularly service users, with a Privacy Notice/Consent form.

Sharing Without the Individuals Knowledge or Consent

There are limited circumstances when the DPA provides for personal data, even sensitive data, to be shared without the individual concerned knowing about it. This includes the:

a) Protecting the vital interests of the data subject;

b) Preventing serious harm to a third party that would occur if the data were not disclosed;
c) Safeguarding national security;
d) Prevention or detection of crime;
e) Apprehension or prosecution of offenders;
f) Assessment or collection of tax or duty;
g) Discharge of regulatory functions, including the health, safety and welfare of persons at work.

In relation to d) and g) above, disclosure is allowed in those cases only to the extent to which failure to disclose would be likely to prejudice the attainment of those aims. This means that if the information was not disclosed this would noticeably damage the prevention and detection of crime or health, safety and welfare of persons at work.

Decisions in relation to sharing individual's personal data without their knowledge should be recorded, including the reasons for the decision. In the event of any doubt advice should be sought from the relevant Service Manger or Director of Corporate Services.

External requests from third parties should normally be made in writing. The following should be covered:

- the authority under which the request is made;
- reasonable proof of identity and organisation;
- details of personal data requested, the purpose it is requested for and confirmation that the request is necessary and proportionate;
- where relevant any exemption under the DPA or other legislation that applies;
- request is to support the apprehension or prosecution of offenders;
- where applicable, confirmation that any data disclosed will be processed in accordance with the DPA.

There may be occasions where an emergency situation such as imminent danger of death or injury requires consideration of a quick response. The following actions should be taken:

- Seek advice from a Service Manager;
- If in doubt about the legitimate nature (e.g. attempt at gaining unauthorised access to data sometimes called "blagging" data, or through identity fraud) do not to disclose data;
- If request received by telephone obtain a switchboard number to call the person back, check for the organisations number, (be aware of telephone spoofing – call back on a different landline or mobile number);
- Make a record of the circumstances, what was shared and why;
- Ask the caller to make a formal written request for retention in Sacro records;

Responsibilities

The Director of Corporate Services is responsible for ensuring effective data sharing. Training in this area upon commencing work with Sacro and on an ongoing basis will be provided. The Director of Corporate Services will notify the ICO of any significant changes regarding who Sacro shares data with, in the annual registration.

Service Managers are responsible for the day to day operation of effective data sharing and providing advice to staff, volunteers and others operating within their services. This will include monitoring of data sharing on an ongoing basis to support service delivery.

All Sacro staff are responsible for ensuring personal and personal sensitive information that they share is carried out in accordance with the provisions of the DPA.

Monitoring and Review of Policy

The Records Management Policy will be reviewed annually by the Director of Corporate Services.

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

Appendix A: Systematic Data Sharing Checklist

The following checklist should be used when developing new systematic personal or personal sensitive data sharing agreements or Memorandum of Understanding (MOU). It provides questions to prompt thinking about good governance, risk management and compliance in the area of sharing personal and personal sensitive information between Sacro and a third party.

Ref	Area	Considerations	Comment
1	Justification for sharing	▪ What is the objective of sharing – what are we trying to achieve? ▪ Could anonymised sharing achieve the objective(s) of sharing? ▪ Have the potential benefits of sharing or not sharing for individuals been considered? ▪ Have the potential risks of sharing or not sharing for individuals been considered? ▪ Is the sharing proportionate to the issue being addressed?	
2	Define the purpose	▪ What is the purpose of the data sharing? ▪ Does it fit with the purpose for which it was originally collected? ▪ Is it a new purpose? ▪ Does it fit with our Privacy Notice? ▪ Does it fit with any Privacy Notice we gave to the data subject when we collected the original data? ▪ Do we need to inform the data subject of our intention to share? ▪ Do we need to get consent from the data subject?	
3	Power to share	▪ What is the nature of the information to be shared? ▪ What is our organisations powers to share? ▪ What is the nature of the information that is to be shared – was it given to Saco in confidence? ▪ Is there any legal requirement to share – such as a court order?	

Ref	Area	Considerations	Comment
4	Identify the people involved	▪ Who will be providing the data to be shared? ▪ Who will be obtaining the data to be shared? ▪ Who will be recording the data to be shared? ▪ Who will be accessing the data shared?	
5	Clarify the data protection roles	▪ Is the third party with whom the data is to be shared a ▪ Joint Data Controller? or a ▪ Data Controller in common? or a ▪ Data Processor? ▪ Do they understand the data protection implications of their role?	
6	Consider scope of data	▪ Is it adequate for the purpose? ▪ Is it relevant for the purpose? ▪ Is it not excessive for the purpose?	
7	Is it personal or personal sensitive	▪ Has the data been confirmed as personal only? ▪ Has the data been confirmed as sensitive personal data? ▪ What types of sensitive personal data are involved?	
8	Processing conditions	▪ Can sharing (processing) be supported on one of the personal conditions (Schedule 2 of DPA)? ▪ Which conditions apply? ▪ Can sharing (processing) be supported on one of the sensitive personal conditions (Schedule 3 of DPA)? ▪ Which conditions apply?	
9	Multiple processing conditions apply	▪ Which one (conditions for processing personal or sensitive personal data) will be relied upon?	
10	Consent of the data subject	▪ Is this required for the data sharing to be lawful? ▪ Has it been obtained? ▪ If not how will it be obtained?	

Ref	Area	Considerations	Comment
11	Inform the data subjects	▪ With reference to the information given to the data subject at the time the data was collected, could they reasonably expect their personal data to be used for the purpose we propose to share it for? ▪ Could they reasonably expect it to be shared with the third party involved? ▪ Could the sharing cause substantial and unwarranted harm or distress to the data subject? ▪ How will we respond to any objections if we receive them? ▪ Will the data subject need to be informed of the data sharing by the third party?	
12	Security	▪ Have the technical security measures been checked and considered adequate to protect from loss, unauthorised access, disclosure etc.? ▪ Has the impact on a data security breach for individuals (data subjects) and the organisation been considered?	
13	Data subject access rights	▪ Have data subjects been provided with enough information to be able to exercise their rights under the DPA, including rights to access information held on them? ▪ Have data subjects been provided with enough information to identify the Data Controller(s) so they can exercise their subject access and other rights under the DPA?	
14	Data Sharing Agreements	▪ Is a formal documented agreement covering the rules of the sharing a sensible requirement? ▪ What type of agreement is appropriate: ▪ Data Sharing Agreement/Protocol ▪ Information Sharing Agreement ▪ Memorandum of Understanding ▪ Joint Data Controllers Agreement	

Ref	Area	Considerations	Comment
		▪ Data Processor Agreement ▪ Does the agreement cover: ▪ What type of information needs to be shared? ▪ What organisations will be involved? ▪ What we need to tell data subjects about the data sharing? ▪ How will the data sharing be communicated? ▪ Are the measures to ensure adequate security is in place to protect the data being shared clear? ▪ Are the subject access arrangements covered? ▪ Are common retention periods covered? ▪ Are secure deletion arrangements covered?	
15	Governance framework	▪ Does the original Data Controller and the third party have in place an appropriate policy, procedure and working practices to meet their DPA obligations?	
16	Retention Policy	▪ Have common retention periods for the data to be shared been agreed?	
17	Secure disposal	▪ Are there processes in place to ensure the secure destruction or disposal of the data regardless of type (electronic, paper etc.)? ▪ Does the third party with whom the data is to be shared have a policy or procedure on secure disposal?	