CORPORATE SERVICES

POLICY AND PROCEDURES DOCUMENT

Information Technology

Owner:	**Director of Corporate Services**
Author:	**Kashmira Heer**
Version Number:	**3**
Version Date:	**26/06/2018**
Current Document Approved by:	**Board**
Equality Impact Assessment Number:	**EqIA-P001-07/2013**
Review Date:	**26/06/2020**

Information Technology

Policy Document

CONTENTS

Information Technology

Policy Document

1 Introduction

Sacro relies on its IT and communication systems and support networks to provide an efficient and effective service. These systems are essential to the organisation and must be protected from damage or unauthorised access. The purpose of this policy and its associated procedures is to set out clear rules on the use of IT hardware, software, email, internet, intranet and telephones to ensure that Sacro's IT systems and data are protected.

2 Policy Statement

Sacro's Board members and its Chief Executive recognise their responsibilities to ensure that all of Sacro's staff are provided with appropriate computer and telephone systems to allow them to effectively and efficiently deliver Sacro's services to its business partners, as well as to its service users, and relevant visitors and members of the public.

They also seek to ensure that its IT and communication systems are used properly and efficiently, and primarily to the benefit of the organisation.

As an organisation, Sacro will take all reasonably practicable steps that are within its power, to meet this responsibility.

All of those people who are given access to Sacro's computer facilities must also read, and comply with, the information contained in Sacro's Data Protection Policy and Procedures in respect both of protecting information and hardware, and of using the equipment and information appropriately.

3 Scope

This policy and its associated procedures apply to all persons who carry out work on behalf of Sacro, whether directly employed or otherwise, and who in doing so use Sacro's computer and telephone equipment.

4 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 its services and of its 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.

5 Core Principles

In seeking to fulfil its responsibilities, Sacro will:

- provide staff with access to telephone and computer systems that will allow them to deliver an efficient service;
- provide a support network that will ensure that staff are afforded the necessary back-up when problems are encountered in respect of Sacro IT and telephony equipment;
- give guidance to all of its staff in respect of reasonable use, and in respect of unauthorised use and the consequences of it;
- regularly review the effectiveness of this policy, the restrictions that are set out within it, and any procedures that have been developed to support it.

6 Offensive Email and Internet Content

Sacro views the sending and requesting of offensive emails, and the accessing of offensive internet content as misconduct, and a breach of this policy in respect of these matters may result in disciplinary action.

Offensive content includes obscene or indecent material, sexist, pornographic or racist remarks.

Sending or agreeing to receive emails with offensive content, or accessing offensive internet content, may also contravene UK law, and could be reported to the police.

7 Online Social Networking, Professional Networking and Blogging

Two separate policies relating to the use of social media websites have been published, and all staff are subject to the directions and guidance contained therein.

8 Data Storage Devices

Sacro computers have been reconfigured to block access to or by any external storage device. Any member of staff with Sacro data still saved on such devices must consult the procedures associated with this policy for guidance in respect of dealing with these situations.

If a member of staff loses a data storage device containing Sacro information, or becomes aware of a compromise of security, to comply with the demands of the Data Protection Act 1998, and to satisfy the requirements of the Information Commissioner, s/he must contact the IT Officer immediately. The member of staff losing the device must also notify his/her line manager of any such loss.

Upon receipt of any such report referred to in the previous paragraph, Sacro’s IT Officer will ascertain if there is a potential infringement of Sacro’s Data Protection Policy, and if there is, will ensure that the Director of Corporate Services is notified.

9 Monitoring

Sacro recognises that employees may wish to utilise company telephones and computer equipment for personal use during their own time, and the procedures associated with this policy set out guidance regarding acceptable personal use.

If required, the IT Officer has the ability to monitor email and internet use, as well as files stored on Sacro’s computers.

The use of company telephones will be monitored via itemised telephone bills.

10 Breach of the Policy

Any breach of this policy and the associated procedures may lead to proceedings being taken against a member of staff in accordance with Sacro’s Disciplinary Policy and Procedures, and could lead to disciplinary action.

11 Responsibilities

The Sacro Board of Directors and its Chief Executive take ultimate responsibility for Sacro’s Information Technology and Information systems.

The Director of Corporate Services will ensure that this policy is comprehensively reviewed at least every three years, and earlier if demanded by changing circumstances.

The IT Officer will ensure that the content of the document is adjusted as new technology or software becomes meaningful to the guidance contained herein.

Any further guidance that is required in respect of this policy should initially be sought from the IT Officer.

Information Technology

Procedures Document

CONTENTS

Information Technology

Procedures Document

1 Terms and Conditions of Use of Sacro's IT System

All staff when they initially log on to the Sacro IT system will be presented with the Security Warning page. By clicking on the 'OK' button to move past this page and onto the system proper, staff are acknowledging having read and understood the content of the warnings presented on the page.

2 General Information Technology (IT) Guidance

The following general guidance is relevant to all staff in respect of the use of Sacro's IT equipment and systems:

- keep your network drive folders clear of unnecessary and unneeded files;
- do not keep personal files stored on Sacro equipment;
- a member of staff must never reveal any information that could potentially be used to compromise the security of Sacro's IT systems, and any enquiries seeking information relating to Sacro's IT systems or procedures must be referred to the IT Officer

3 Data Storage Devices

Sacro has recently carried out a complete update and refresh of its IT system. As a result, Sacro computers have been reconfigured to block access to or by any external storage device. Any member of staff with Sacro data still saved on any such devices should return them to the IT Officer for secure disposal. Staff needing to transfer files should contact the IT Officer for advice.

As a consequence of this change:

- the carriage of Sacro data by a worker in any electronic format that has not been facilitated by the IT Officer is now, except in exceptional circumstances, as facilitated by the IT Officer, not permitted;
- the secure sharing of documents and other data over the Sacro network is now available from anywhere in the Sacro organisation; and,
- the transfer of data from Sacro equipment to portable devices is generally no longer permitted and all Sacro-owned computer equipment is configured to block any such data transfers.

With regard to the above, some typical scenarios where a worker may have previously used a memory card or stick include:

- when giving a presentation at an external event – in such cases, the worker should email her/his presentation to the host of the event in advance of its happening (contact IT Officer if any apparently insurmountable compatibility issues are encountered);
- when a worker is working on data (not sensitive data) outside Sacro premises and remote access to the Sacro system is not possible – in such cases, the worker should email her/his new data to her/his work address and copy the document to the Sacro server upon his/her return to work;
- when a worker needs to send a significant amount of data to an external body e.g. the submission of a large tender document - in such cases, if a document is too big to be emailed or another data solution is sought by the intended recipient, the worker should contact the IT Officer for a solution to the problem, which may in fact be through the use of a suitably-encrypted external data storage medium.

The above list is not intended to be prescriptive and where any worker is in doubt or has concerns about data storage or transfer, s/he is encouraged to seek guidance from the IT Officer at National Office.

The ultimate aim of the terms of this part of the IT procedures is to ensure that Sacro's policy in respect of the protection of data is not breached.

4 Personal and Laptop Computer Guidance and Procedures

The following guidance is relevant to all staff in respect of the use of personal computers:

- do not ever share your access passwords with anyone and do not write your passwords down; the IT Officer maintains a secure list of staff passwords if urgent access is required;
- if you need to leave your computer, you must lock your screen;
- if you leave your computer for an extend period, you should shut it down;
- do not attempt to alter any computer settings;
- do not attempt to open the computer case or tamper with the equipment or cables attached to it;
- email the helpdesk with any requests to install any program;
- do not plug any device (music player, mobile phone etc.) into your computer;
- do not place food or drink on or near computer equipment as it may affect the maintenance contract.

5 Additional Specific Guidance for Laptop Users

The following specific guidance is relevant to all staff in respect of the use of Sacro-owned laptop computers:

- you are responsible for the security of any Sacro laptop that you are being allowed to use, and you must ensure the safe-keeping of the laptop at all times;
- you must never leave a company laptop unattended in a public place or in a car and you should take all reasonable precautions to avoid its being stolen or damaged;
- the hard disks of Sacro laptops/netbooks are encrypted so that if they are stolen or lost, the files cannot be readily accessed;
- you must not allow any person who is not authorised by Sacro to use a company laptop assigned to you;
- any data prepared or stored on a laptop should be transferred to the Sacro network regularly to ensure it is backed up regularly;
- if connecting to the internet outwith a Sacro office, the Sacro IT Policy applies;
- insurance cover is in place for Sacro laptops.

6 Remote Access Policy and Guidance

It is the responsibility of Sacro workers, contractors, and agents with remote access privileges to Sacro's network, to ensure that their remote access connection is given the same consideration as when they are connecting to the network in the workplace.

All of those persons who are given remote access must also read and comply with the terms of Sacro's, "IT – Remote Access to Sacro's IT Systems" Policy for full direction in respect of both acceptable use of computer equipment, and protecting information when accessing the Sacro network.

7 INTERNET Guidance and Procedures

The following guidance is relevant to all staff in respect of the use of the internet:

- do not attempt to access any kind of system - internal or external - that you are not authorised to access;
- do not access websites for non-business-related purposes within your working hours;

- do not access websites that have potentially offensive, illegal, or otherwise dubious content; if you are unsure about a particular site, or if you have unintentionally accessed such a site, contact the IT Officer as soon as possible, by email if necessary;
- do not access any non-work-related on-line chat services;
- you share the internet connection with other users and you should refrain from high bandwidth tasks (such as watching videos, downloading large files);
- do not use an Internet Browser that has not been installed by the IT Officer; if you have problems accessing a site, or in general with the internet, please contact the IT Officer;
- do not attempt to circumvent the web filtering system;
- do not attempt to access any kind of file-sharing system or related websites;
- do not access or use any kind of external file-hosting system;

8 INTRANET Guidance and Procedures

In addition to the guidance in respect of internet use, the following guidance is relevant to all staff in respect of the use of Sacro's intranet:

- it is the responsibility of all users to check the Sacro intranet on a regular basis for information that may be relevant to their work;
- all users must keep both their username and their password secure, and must not let anyone else use them;
- all users must ensure that the content of the intranet is kept confidential and secure, and must not externally distribute information from the intranet in any format (e.g. in an email) without prior permission from a member of staff in the Publications Department;
- users should notify the IT Officer in respect of any issues or problems that are encountered when using the intranet;
- all users must log off from the intranet when they have finished using it;
- the IT Officer must be notified of any breach or suspected breach of this policy.

9 Email Guidance and Procedures

The following guidance is relevant to all staff in respect of the use of email communications:

- only use email for business-related purposes;
- for-by the above, in an employee's own time, Sacro will allow occasional and minimal personal use;
- do not circulate non-business-related emails received, including circulars that warn of security issues, most of which are spoofs;
- do not store non-business-related emails received, especially messages that include attachments;
- think carefully about what you say in an email, remembering that emails can be forwarded on to others, and should never be considered to be private;
- proceed with caution if you receive an unexpected email with an attachment – contact the IT Officer for guidance;
- when you are away from the office, remember to correctly set your "out-of-office" replies;
- if you receive a warning of a blocked email that you are either expecting, or that is from a known source, contact the IT Officer;
- in general, you should not send confidential information by email;
- if you consider it urgent enough to send confidential information via email, please contact the IT Officer for guidance;
- to avoid sending information to the wrong person, always remember to double-check that you have the correct recipient(s) for emails before you click on send;
- regularly tidy up your inbox and either archive important emails or delete unneeded emails.

10 Telephone Use

The following guidance is relevant to all staff in respect of the use of telephone equipment paid for by Sacro:

10.1 All Sacro Telephone Systems

Staff are permitted to use Sacro telephones for personal calls on an occasional basis, and are similarly allowed to receive occasional personal calls. As a guide, “occasional use” in this context means making or receiving no more than one brief personal call per day, although where significant personal issues arise and a member of staff has no other appropriate means of communication available to him/her, extended use will generally be accommodated. Excessive use of a Sacro telephone for personal calls may result in this privilege being withdrawn.

Telephone bills will be monitored to ensure that private calls are occasional, and that business calls to mobile, fixed tariff and premium rate numbers (see below) are kept to a minimum.

Staff should avoid calling premium rate numbers where possible, by checking an organisation’s website for alternatives, or by going to **www.saynoto0870.com**.

10.2 Additional Guidance in Respect of Sacro Mobile Telephones

For certain roles within the organisation it is necessary to provide an employee with a mobile telephone. As with all Sacro telephones, a mobile phone is to be used for business purposes foremost.

A mobile phone will always remain the property of Sacro, and as such all communication via the phone is regarded as business communication. Any personal communication to the phone (verbal or text message) is to Sacro equipment, and could be received by persons other than yourself, and as a consequence, confidentiality and/or privacy should not be expected;

As with all items of Sacro property or equipment in your possession, you are deemed to be responsible for the safekeeping of a mobile phone allocated to you, and it should be kept secure at all times. Do not leave a mobile phone in view in an unattended vehicle.

Do not attempt to hack or “jailbreak” a Sacro mobile telephone allocated to you. This includes installing a different operating system to the pre-installed operating system. Additionally, you must not let anyone else perform or attempt to perform such an installation. Do not update your phone’s operating system, even from official sources.