INFORMATION GOVERNANCE POLICY

Document Control
Reference: DSP DOC 01-1.2.1a
Issue No: 2.1
Issue Date: 08/02/2023
Page: 1 of 8

1. Introduction

This Policy establishes the key high-level principles of Information Governance at Saving Faces and sets out responsibilities and reporting lines for members of staff. It provides an over-arching framework for Information Governance across the charity.

Information Governance is an accountability and decision- making framework put in place to ensure that the creation, storage, use, disclosure, archiving and destruction of information is handled in accordance with legal requirements and to maximise operational efficiency. It includes the processes, roles, policies and standards that ensure the compliant and effective use of information in enabling an organisation to achieve its goals. Information is a key asset for Saving Faces and the regulatory, reputational and operational risks of poor information governance are ever increasing. As the creation of information proliferates, it is vital that Saving Faces has measures in place to manage and control these risks.

2. Purpose

This policy is a statement of Saving Faces approach and intentions to fulfilling its statutory and organisational responsibilities. It will enable management and staff to make correct decisions, work effectively and comply with relevant legislation and the organisations aims and objectives.

3. Scope

This policy applies to all staff, volunteers, Trustees, interns, contractors and third parties employed by or carrying out work on behalf of Saving Faces. It applies to all personal data processing we carry out for others (where we're the 'Processor' for the personal data being processed). It applies to all formats, e.g. printed and digital information, text and images, documents and records, data and audio recordings.

Information governance:

Information governance (IG) is a term used to describe how information is used. It covers system and process management, records management, data quality, data protection and the controls needed to ensure information sharing is secure, confidential and responsive to Saving Faces' needs and the people it serves.

Information Governance starts with looking at how information is collected, how it is recorded (on paper and computers), how it is then stored, how it is used (whether for audit, research or performance management) and then on what basis it is shared with others, both inside and outside Saving Faces.

4. Purpose

4.1 The purpose of the Information Governance Policy is to support the 10 Data Security Standards developed by the National Data Guardian, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise

INFORMATION GOVERNANCE POLICY

Document Control
Reference: DSP DOC 01-1.2.1a
Issue No: 2.1
Issue Date: 08/02/2023
Page: 2 of 8

data protection as a fundamental right and embrace the principles of data protection by design and by default.

4.2   This policy covers:

- Our data protection principles and commitment to common law and legislative compliance;

- procedures for data protection by design and by default.

5.   Principles

Saving Faces recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Saving Faces fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

Saving Faces believes that accurate, timely and relevant information is essential to deliver the highest quality service to its supporters and research partners. As such, it is the responsibility of all staff and managers to ensure and promote the quality of information, and to actively use information in decision-making processes.

There are four key interlinked strands to this information governance policy:

- Openness
- Legal compliance
- Information security
- Quality assurance

5.1   Openness

- Non-confidential information on Saving Faces and its services should be available to the public through a variety of media.

- Saving Faces will undertake or commission annual assessments and audits of its policies and arrangements for openness.

- Saving Faces will have clear procedures and arrangements for handling queries from supporters, research partners and the public.

5.2   Legal compliance

- Saving Faces regards all identifiable personal information relating to patients as confidential.

- Saving Faces will undertake or commission annual assessments and audits of its compliance with legal requirements.

INFORMATION GOVERNANCE POLICY

Document Control
Reference: DSP DOC 01-1.2.1a
Issue No: 2.1
Issue Date: 08/02/2023
Page: 3 of 8

- Saving Faces regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

- Saving Faces will establish and maintain policies to ensure compliance with data protection law, Human Rights Act and the common law duty of confidentiality.

- Saving Faces will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation.

5.3   Information security

- Saving Faces has policies for the effective and secure management of its information assets and resources.

- Saving Faces undertakes or commissions annual assessments and audits of its information and IT security arrangements.

- Saving Faces promotes effective confidentiality and security practice to its staff through policies, procedures and training.

- Saving Faces has incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

- In particular, business continuity and contingency plans, data backup procedures, installing anti-virus/malware software onto computers and laptops, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy.

5.3.1   Securing information

- Patient records must not be left in a position where unauthorised persons can obtain access to them in hard copy or other format.

- Patient records must not be left unattended unless in a secure and lockable area and stored in an environment that does not cause damage or decay to the documentation or media.

- Where feasible, all patient records should be protected by two layers of physical security, i.e. in a lockable cupboard within a locked room.

- Keys to lockable cupboards should themselves be stored securely.

- Cleaning staff should not be able to access patient records in any format.

For all types of hard copy health records, staff are required to:

INFORMATION GOVERNANCE POLICY

Document Control
Reference: DSP DOC 01-1.2.1a
Issue No: 2.1
Issue Date: 08/02/2023
Page: 4 of 8

- Lock doors and cabinets when not in use but always out of hours;

- Ensure that folders containing patient records are stored closed or turned face down when not in use so that contents are not seen accidentally; and

- Ensure that patient records are inaccessible to members of the public and not left for even short periods where the records may be looked at by unauthorised persons.

Staff should ensure that the clear screen policy is followed at all times:

- Computers are to be logged off or locked when unattended.

- Computers should have password-protected screensavers set to activate within ten minutes of no keyboard or mouse activity.

- Computer screen should be sited in such a way to avoid or minimise oversight of the screen by unauthorised persons.

When it is no longer required, Saving Faces media shall be disposed of securely either by physical destruction of the media or by secure erasure of stored data, such as:

- Where not required, media classified confidential should be permanently deleted or destroyed/shredded prior to disposal.

- Customer owned media that is not to be returned will be disposed of securely using Saving Faces procedures.

- Computer hard drives will be erased securely prior to reuse.

- Faulty hard drives that contain 'Confidential' information will be destroyed.

Individuals will ensure:

- All confidential information on paper relating to Saving Faces, its business, staff and patients is shredded, either by using the secure shredding bins provided or shredding via the shredders located within the offices.

- Personal data on encrypted (AES256) USB memory sticks and hard drives are retained until all quality control checks have been performed and then destroyed by: multi pass pattern wiped (minimum of 3 passes but where possible 7 passes) to at least HMG S5 on site and if end of life, degaussed and physically destroyed.

5.4 Information quality assurance

- Saving Faces has policies and procedures for information quality assurance and the effective management of records.

Saving Faces
The Facial Surgery Research Foundation

INFORMATION GOVERNANCE POLICY

Document Control
Reference: DSP DOC 01-1.2.1a
Issue No: 2.1
Issue Date: 08/02/2023
Page: 5 of 8

- Saving Faces undertakes or commissions annual assessments and audits of its information quality and records management arrangements.

- Managers are expected to take ownership of, and seek to improve, the quality of information within their services.

- Wherever possible, information quality should be assured at the point of collection.

- Saving Faces will promote information quality and effective records management through policies, procedures/user manuals and training.

5. Responsibilities

The Data Protection Officer (DPO) carries out tasks under Article 39 (1) of GDPR to:
- Inform and advise on compliance with GDPR
- Monitor compliance with GDPR
- Provide advice with regards to data protection impact assessments
- Cooperate with the ICO
- Act as contact point with the ICO on issues relating to processing

The Chief Executive Officer (CEO) is responsible for ensuring that the necessary resources and facilities are available to ensure that staff can adhere to this policy. The policies listed in this document apply to all staff.

For the purposes of this policy, the term 'staff' refers to all personnel working for or with Saving Faces or who have been authorised to access Saving Faces information assets. This includes all management, employees, contractors, temporary staff, trainers, consultants, agents and client personnel.

All Staff
All Saving Faces staff are responsible for:

- Maintaining the confidentiality of Saving Faces data and information;

- Adhering to company policies;

- Following any appropriate security procedures for Saving Faces systems they use;

- Only using authorised Saving Faces software and preventing unauthorised introduction of new software;

- Choosing effective passwords (3 random words) and keeping them confidential;

- Ensuring that any terminal they use is protected when unattended;

- The security of any computer equipment they take off-site;

- Using email, public networks and the Internet in a professional manner;

- Taking appropriate precautions against viruses; and

INFORMATION GOVERNANCE POLICY

Document Control
Reference: DSP DOC 01-1.2.1a
Issue No: 2.1
Issue Date: 08/02/2023
Page: 6 of 8

- Reporting security breaches or weaknesses to the appropriate person.

All Saving Faces staff **shall not:**

- Disclose or discuss corporate data or information to any non-organisation employee without explicit authorisation from a director of Saving Faces;

- Attach portable memory sticks, hard drives or CD writers to Saving Faces IT equipment without authorisation from the Office Manager.

- Disclose or discuss Saving Faces confidential data with any other person without explicit authorisation from the *CEO*;

- Disclose their password or confidential details of any other access mechanisms to any person;

- Discuss information classified as confidential in a public place or on mobile phones; or

- Remove confidential information on magnetic media or paper without authorisation from the *CEO*.

6. Information exchanged with other organisations

Saving Faces may periodically receive information from NHS or customers or suppliers that has specific information security requirements. In some instances, this will require contractual agreements binding Saving Faces and the client or supplier to take appropriate care of exchanged information and/or software (whether electronic or manual).

To determine the need for a contractual, binding (legally and morally) agreement between parties an appropriate risk assessment must be undertaken. In conjunction with the assessment results and the information classification guidelines, it will be apparent whether or not a formal agreement should be drawn up.

Dependent upon the sensitivity of the information involved and the method of exchange the following security conditions will apply and should be incorporated into the contractual agreement (unless specifically excluded due to the low security classification of the information and/or the results of the risk assessment determine that exchange of the information in question is a low risk to the business):

- Clearly defined management responsibilities and procedures for controlling and notifying sender, transmission, dispatch and receipt. This applies to electronic and manual information.

- Definition of the minimum technical standards to be adhered to for packaging and transmission.

INFORMATION GOVERNANCE POLICY

Document Control
Reference: DSP DOC 01-1.2.1a
Issue No: 2.1
Issue Date: 08/02/2023
Page: 7 of 8

- A clear statement regarding the responsibilities and liabilities of each party in the event of loss of information.

- A statement of the agreed labelling system for sensitive or critical information. This will ensure that the information is readily identifiable and hence appropriately protected.

- Ownership and ownership rights of the information/software must be clearly stated. Responsibility for compliance (both regulatory and statutory), e.g. data protection law must be followed.

- Definition of the technical standards for recording and reading information must be clearly stated.

- Special controls adopted (e.g. safes or cryptographic keys) must be clearly stated within the agreement.

7. Data protection by design and default

New initiatives that involve high-risk processing of personal data will be subject to a DPIA to ensure the privacy and security of personal confidential data is maintained. Saving Faces will:

- implement appropriate organisational and technical measures to uphold the principles outlined above. Saving Faces will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

- uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

- record all existing data processing on our Record of Processing Activities. Each process has been risk assessed and is reviewed annually.

- ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

- use the least amount of identifiable data necessary to complete the work it is required for in all processing of personal data.

- will only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

- will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support, where possible.

Saving Faces
The Facial Surgery Research Foundation

INFORMATION GOVERNANCE POLICY

Document Control
Reference: DSP DOC 01-1.2.1a
Issue No: 2.1
Issue Date: 08/02/2023
Page: 8 of 8

8.   Document Owner and Approval

The Information Governance Lead is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the DSP Toolkit.

A current version of this document is available to all members of staff on the Saving Faces website.

This procedure was approved by the CEO and is issued on a version controlled basis under his/her signature.

Name	Iain Hutchison
Signature	
Approval Date	03/04/2024
Review Date	03/04/2025

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	CEO	25/06/2021
2	SM Review, Addition of Introduction, Purpose and amendments to Responsibilities, Scope and Information Governance	SM	22/06/2022
2.1	Amendment to 5.3 Information security clarifying the requirement to install anti-virus/malware software onto computers and laptops.	FR	07/02/2023
2.1	Review – no changes	FR	21/02/2024