DATA PROTECTION AND CONFIDENTIALITY POLICY (TIER 1)

1. Purpose and scope

The Data Protection Act 2018 and UK GDPR sets out the legal framework by which we can process personal information safely and securely and operates alongside the common law duty of confidentiality which governs information given in confidence to health professionals with the expectation that it will be kept confidential.

This policy:
Applies to all staff, volunteers, Trustees, interns, contractors and third parties who process data on behalf of Saving Faces to ensure that data is handled in accordance with the Data Protection Act 2018 and UK GDPR.

It applies to all processing of personal data using information systems provided to authorised users to perform their roles and responsibilities.

2. Responsibilities

All employees, contractors and associates share the responsibility for ensuring that information assets are handled in accordance with this policy.

3. Definitions

Confidentiality: The ethical principle or legal right that a physician or other health and social care professional will hold secret all information relating to a patient/service user, unless they have given informed consent permitting disclosure.

Data: Information as defined by data protection law that is:
- Processed electronically i.e. information systems, databases, microfiche, audio and video systems (CCTV) and telephone logging systems;
- Recorded with the intention that it shall be processed by equipment; or
- Recorded as part of a relevant filing system, i.e. structured, either by reference to individuals or by reference to criteria relating to individuals which is readily accessible.

Data controller: The individual, company or organisation who determines the purpose and the way personal data may be processed.

Data processor: Any person other than an employee of the data controller who processes data on behalf of the organisation.

Data subject: A living individual who is the subject of the processed personal data. They are someone who can be identified as a person, or with a combination of other information can be identified.

Disclosure: The divulging or provision of access to data.

Personal confidential data: Personal information about identified or identifiable individuals, which should be kept private or secret. Personal includes the General Data Protection Regulation (GDPR)'s definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in data protection law.

Personal information: Information that relates to a living individual who can be identified from that information or from that information and other information which is in the possession of, or likely to come into the possession of the data controller.

Processing: Any action taken with someone's personal data including::
- Obtaining
- Recording
- Retrieving
- Altering
- Disclosing
- Destroying
- Using
- Transmitting
- Erasing

Special category personal data (formally known as sensitive personal data): Personal data which requires additional protections because it relates to an individual's:
- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sex life
- Sexual orientation

Third party: Any person other than:
- The data subject;
- The data controller; and
- Any data processor or other person authorised to process for the data controller.

4. Data Protection – Key Principles

4.1 The principles of Data Protection 2018 and UKGDPR Data Protection law sets out the following 7 key principles to support good practice and fairness in processing personal information. These principles stipulate that:

- Personal data must be processed lawfully, fairly and transparently;
- Personal data can only be collected for specific, explicit and legitimate purposes;
- Personal data must be adequate, relevant and limited to what is necessary for processing;
- Personal data must be accurate and kept up to date with every effort to erase or rectify without delay;
- Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing;
- Personal data must be processed in a manner that ensures the appropriate security; and
- The controller must be able to demonstrate compliance with the Data Protection Act 2018 and UK GDPR.

4.2 Lawful basis for processing

Saving Faces is obliged to have a lawful basis to process personal data. There are six lawful bases for processing, a lawful basis must be determined before processing begins.

Saving Faces also processes special category information, which requires more information. In order to lawfully process special category data we need to identify a condition for processing, this is in addition to the lawful basis (Article 6 of the UK GDPR).

Lawful bases, conditions and special category data:
The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever Saving Faces processes personal data

Article 6(1)(a) Consent	the individual has given clear consent for you to process their personal data for a specific purpose
Article 6(1)(b) Contract	the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract
Article 6(1)(c) Legal obligation	the processing is necessary for you to comply with the law (not including contractual obligations)
Article 6(1)(d) Vital interests	the processing is necessary to protect someone's life

Article 6(1)(e) Public task	the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law
Article 6(1)(f) Legitimate interests	the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

5. Confidentiality

Duty of confidentiality
All staff and contractors must recognise that confidentiality is an obligation. Any breach of confidence, inappropriate use of records or abuse of computer systems may lead to disciplinary procedures and may result in legal proceedings.

Temporary and voluntary staff are also subject to such obligations and must sign a confidentiality agreement as appropriate when working for or on behalf of Saving Faces.

The Caldicott Principles for protecting and using personal information
The Caldicott Committee Report on the Review of Patient-Identifiable Information in 1997 found that compliance with confidentiality and security arrangements was patchy across the NHS and identified good-practice principles for the health service when handling patient information. This was revised by in 2020. The principles are as follows:

1. Justify the purpose for using or sharing person confidential data.
2. Do not use personal confidential data unless it is absolutely necessary.
3. Use the minimum necessary personal confidential data.
4. Access to personal confidential data should be on a strict need-to-know basis.
5. Everyone with access to personal confidential data should be aware of their responsibilities.
6. Comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.
8. Inform patients and service users about how their confidential information is used

The role of the Caldicott Guardian
The Caldicott Committee Report also led to the appointment of Caldicott Guardians.

Their role is to agree and monitor protocols for sharing information across organisational boundaries, ensure that patient's/service user's rights to confidentiality are respected and to safeguard the security of personal information.

Saving Faces is not required to have a Caldicott Guardian. Advice on data protection and confidentiality will be obtained from the Data Protection Officer.

Disclosure of confidential information
The NHS has strict guidance on the disclosure of personal confidential data. Saving Faces complies with these as part of its contractual obligations.

Non-care purposes
Individuals must give explicit consent for data sharing for the following non-care purposes:

- Checking quality of care
- Protecting the health of the general public
- Managing care services
- Supporting research

5.1 Data Processing
Data processing covers the collecting, recording, using, storing, disclosure and disposal of data. The lawful and safe processing of data is important to successful business operations and to maintain confidence between Saving Faces and its patients, staff, and others with whom we work.

The UK GDPR requires that processing of any personal information held by Saving Faces must comply with principles and has a lawful basis. Routine data processing for the purposes of patient care will normally be conducted for a purpose that satisfies one of the processing conditions in the UK GDPR.

5.2 Information security
In order to ensure the confidentiality of personal information, systems and procedures are required to control access to such information. Such controls are essential to ensure that only authorised persons have:

- Physical access to computer hardware and equipment;
- Access to computer system utilities capable of overriding system and access controls, e.g. administrator rights; and
- Access to either electronic or paper records containing confidential information about individuals.

Saving Faces responsibilities for confidentiality and appropriate processing of personal data remain in place even if the processing is being undertaken by a third-party contractor.

The Access Control Policy, Access Control Procedure and Information Security Policy provide detailed guidance including minimum standards.

5.3 Communicating personal information

In order to comply with the UK GDPR principles it is important that any transfer or communication of personal data is carried out securely and safely and the risk of accidental disclosure or loss in transit is minimised. Any data containing identifiable information transferred by Saving Faces outside of the charity for processing must be securely encrypted during transit. Detailed guidance can be found in theInformation Security Policy.

5.4 Access to personal information

Individuals or persons acting on their behalf with consent have a right of access to data held about them. This includes access to audit trails that indicate who has accessed their personal or confidential data. The subject access procedure is set out in the Subject Access Requests (SARs) Procedure document.

5.5 Individual Rights

There are eight rights which all employees and non-employees are required to be familiar with the rights of individuals and follow the Subject Access Procedure policy.

The eight rights are:

Information right	**Meaning**
The right to be informed	Individuals have the right to be informed about how their data is used, which is included in the Saving Faces' privacy notice
The right of access (Subject Access Request)	Individuals have the right ask for and receive a copy of their personal data
The right to rectification	Individuals have the right to have inaccurate personal data rectified or completed if incomplete
The right to erasure (Right to be forgotten)	Individuals have the right to ask for information to be erased; this is not an absolute right
The right to restrict processing	Individuals have the right to request the restriction or suppression of their personal data; this is not an absolute right
The right to data portability	Allows individuals to obtain and reuse their personal data for their own purposes
The right to object	Individuals have the right to object to the processing of their personal data in certain circumstances
Rights in relation to automated decision making and profiling	Where there is no human involvement in decision-making or

	profiling, this is restricted and can be challenged

5.6 Data Protection by Design and Default
As part of the UK GDPR's accountability principle Saving Faces is required to safeguard individual rights by putting in place the appropriate technical and organisational measures. The UK GDPR requires Saving Faces to integrate data protection into every aspect of processing activity. This includes implementation of the data protection principles and safeguarding individual rights, such as data minimisation, pseudonymisation and purpose limitation as set in this policy.

Saving Faces ensures that data protection is considered at the start of any new project, service or process.

5.7 Data Protection Impact Assessment (DPIA)
A DPIA identifies and assesses potential risks to Saving Faces of processing activities. It is an integral part of data protection by design and by default, and should be completed for all projects, proposals or business changes that involve personal information.

6 Objections to handling confidential data

Any queries or objections on the handling of personal information will be referred immediately to the Data Protection Officer. Where Saving Faces is acting as a data processor under contract, the query will be referred to the data controller.

7 Information flow mapping

Flows of personal information into and out of Saving Faces is mapped on the Records of Processing activities spreadsheet.

8 Data sharing – third parties

Where Saving Faces, as Data Controller, instructs a third-party organisation to process data on its behalf there is a requirement to ensure the processor provides "sufficient guarantees" that they have the appropriate technical and organisational measures in place to ensure the processing complies with the UK GDPR and protects the rights of individuals.

These guarantees may be within the contract between the two organisations or within other terms of processing.

Disposal of personal information

It is a principle of the UK GDPR that data should 'not be kept for longer than necessary'. To assist staff in meeting this requirement, the Records Retention Procedure provides detailed guidance to staff about the minimum retention periods applicable to Saving Faces' records and record disposal procedures.

Any documents containing personal data should be disposed of securely and not discarded in general waste or recycling bins.

The disposal of items of electronic equipment which may hold personal data (PCs, laptops, and any other devices with information storage capabilities) should be carried out through a specialist asset disposal service to ensure all data is effectively removed before disposal.

9 Breach of data protection and confidentiality

Any breach or suspected breach of data protection and confidentiality can have severe implications for Saving Faces, our patients and staff.
The Data Protection Officer is the single point of contact for all breaches and advice and guidance must be sought as soon as possible by contacting *info@savingfaces.co.uk*

Staff who wish to report incidents relating to data protection and confidentiality should follow the incident reporting procedures contained in the Information Security Guidance for Staff.

Breaches of confidentiality or unauthorised disclosure of any information subject to the DPA and UK GDPR constitutes a serious disciplinary offence or gross misconduct under the Saving Faces' Disciplinary Policy. Staff found in breach of this policy may be subject to disciplinary action up to and including summary dismissal.

10 Roles, Responsibilities and Implementation

Chief Executive Officer

As the accountable officer the Chief Executive Officer is responsible for overall leadership and management of Saving Faces and has the ultimate responsibility for ensuring compliance with the Data Protection Act 2018 and UK GDPR. The Chief Executive Officer delegates aspects of their responsibility to relevant members of staff.

Data Protection Officer (DPO)

The DPO is responsible for ensuring Saving Faces complies with data protection legislation and for its compliance with its own policies in relation to the protection of personal data. The day-to-day responsibility for data protection and confidentiality falls within the remit of the DPO.

Information Governance (IG) Manager

The IG Manager is responsible for protecting the confidentiality of patient and service user information while enabling appropriate information sharing. They are responsible for information risk and ensure that effective systems and processes are in place to address Saving Faces' information governance agenda.

Individual responsibility
Everyone working for Saving Faces has a legal duty to keep information about patients and other individuals such as staff, or volunteers confidential. They are required to adhere to all of Saving Faces' policies, confidentiality agreements, their contract of employment and code of conduct.

11 Document Owner and Approval

The Data Protection Officer 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. This will be reviewed annually.

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

This policy 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 version	CEO	25/06/2021
2	SM Review and Amendments to: Purpose and Scope, Data Protection – Key Principles, Roles, Responsibilities and Implementation	SM	14/06/2022
2.1	Corrected reference document of the data breach procedure.	SM	05/04/2023
3	Update of Caldicott Principles – added 8th new principle. Updated DPO contact email	Hannah John and Ping San	06/02/2024