

1. Introduction

Saving Faces implements physical and local access controls across its premises, networks, IT systems and services to provide authorised, granular, auditable and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability.

It is vital that authorised users who have access to Saving Faces' premises, systems and information are aware of and understand how their actions may affect security.

Definitions

- 1.1 Physical access control refers to the selective restriction of access to a location.
- 1.2 Logical access control is defined as restricting virtual access to data and consists of identification, authentication and authorisation protocols.
- 1.3 Confidentiality: systems and information will only be access by authorised users.
- 1.4 Integrity: the accuracy and completeness of systems and information are safeguarded.
- 1.5 Availability: systems and information are physically secure and are accessible to authorised users when required.
- 1.6 Authorised users refer to the following groups who either as a part of a contract of employment or third party contract, have access to or use Saving Faces' systems and information:
 - Chief Executive
 - Trustees
 - Full and part time staff
 - Volunteers
 - Interns
 - Agreed third parties (auditors, HMRC,)

2. Purpose

The purpose of this policy is to ensure that both logical and physical access to information and systems is controlled and procedures are in place to ensure the protection of information systems and data.

3. Scope

The scope of this policy includes all access to Saving Faces' information, systems and physical access to areas and locations where information and data is located. This policy applies throughout the information lifecycle from acquisition/creation, utilisation, storage and disposal.

4. POLICY

Saving Faces will provide all authorised users with access to the information they require to carry out their responsibilities in as effective and efficient manner as possible.

4.1 **Systems and information access**

4.2 Saving Faces controls access to information based on business and security requirements. Information risk owners have a responsibility to keep information access requirements for specific roles up to date and regularly reviewed.

4.3 For systems containing restricted and personal information and data; the security requirements are determined by a risk assessment that identifies the information related to the system and the risks to that information.

4.4 The access rights take into account:

- The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements.
- Data protection and privacy legislation and any potential client contractual commitments regarding access to data or services.
- The 'need-to-know' principle (i.e. access is granted at the minimum level necessary for the role).
- 'Everything is forbidden unless expressly permitted';
- Any privileges that users need to perform their roles, subject to it being on a need-to-use and event-by-event basis
- The appropriate level of access to systems and information will be determined on the prospective users required business need, job function and role. User access requests are subject to formal authorisation and to periodic review. When authorisation is granted, unique log on credentials and passwords will be provided.
- To adhere to national legislation security standards, personnel checks such as a DBS may be undertaken.
- Generic logons are not generally permitted.

5. **Systems and information de-registration**

If a member of staff changes their role or their contract is terminated, their line manager should ensure that the user's access to the system/information has been reviewed or if necessary removed as soon as possible.

6. **Network access control**

6.1 Access to patient systems on the NHS HSCN (N3) network services and associated privileges will be the subject of the Registration Authority procedure as defined in the Access Control Procedure.

7. **Physical access and controls**

Maintaining the physical security of offices and rooms where information, data and processing facilities are accessed and located is vitally important. There must be methods of physically securing access to protect information and data:

Staff should wear their Saving Faces ID cards and visitors must be signed into the premises. People not displaying ID badges should be challenged. Any person not known to staff must be challenged in order to establish who they are and whether authorisation has been provided for them to be there. If there is any doubt about the identity of an individual, the appropriate manager should be contacted to confirm the individual's identity.

ACCESS CONTROL POLICY

Document Control
Reference: DSP DOC 01-1.2.1f
Issue No: 2.1
Issue Date: 08/02/2023
Page: 3 of 4

The use of keys to access buildings, rooms, secure cabinets and safes must be controlled and recorded. Keys must be stored in secure areas/locked cabinets when not in use and must be identifiable by recording serial/ID markings of all keys. The location of keys must be known at all times and a record kept against individual names when keys are used.

Access to and knowledge of door lock codes or access to keys for locks are restricted to authorised personnel only and must not be shared with any unauthorised person.

Electronic access cards must be issued to authorised staff on an individual basis.

Electronic access cards issued to personnel no longer working for Saving Faces must be deactivated and recovered immediately- a record of this action must be kept, using an official recording system.

All contracted cleaners must have and display appropriate identification and be made aware of the requirements within this procedure.

8. Breaches of Policy


Breaches of this policy and /or security incidents should be immediately reported to the Data Protection Officer as quickly as possible. If a member of staff is deemed to have contravened any of the information in the Security policies or procedures, potentially jeopardising the availability, confidentiality or integrity of the systems or information, their access rights should be reviewed immediately by the system owners. Failure to comply with this procedure could result in action in line with Saving Faces' Disciplinary Procedure.

9. Document Owner and Approval

The Data Protection Officer (DPO) is the owner of this document and is responsible for ensuring that The Access control 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 policy was approved by the Chief Executive Officer (CEO) and is issued on a version controlled basis under their signature.

Name	Iain Hutchison
Signature	

ACCESS CONTROL POLICY

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

Approval Date	03/04/2024
Review Date	03/04/2024

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	CEO	23/06/2021
2	SM Reviewed with the following additions: Introduction, Purpose, Scope, Systems Physical Access and Controls, Breaches of Policy.	SM	09/06/2022
2.1	Removed inapplicable/out-of-date network access requirements	FR	02/02/2023
2.1	Reviewed – no changes	Hannah John and Ping San	13.02.2024