ACCESS CONTROL PROCEDURE

1. Scope

This procedure should be read, understood and agreed by all individuals who have access to Saving Faces' information, systems and physical access to areas and locations where information and data is located.

2. Responsibilities

2.1 The Office Manager is responsible for this procedure.

3. Procedure

3.1 User access management

3.1.1 The Office Manager is responsible for allocating and authorising user access rights in conformity with the Access Control policy.

3.1.2 There is a formal electronic user registration and de-registration maintained by the Office Manager on REDCAP.

3.1.3 Saving Faces provides users with appropriate training and awareness prior to enabling access to the system.

3.1.4 The available access privileges for each of Saving Faces' operating systems, applications and other systems are identified and documented.

3.1.5 Privileges are allocated on a need-to-use and event-by-event basis; the request for allocation of a privilege is initiated in an email from the user concerned to the Office Manager copied to the CEO who sets out the reasons why the privilege is required, for what it is required and the period for which it is required.

3.1.6 The Office Manager retains a log of all privileges authorised and allocated and checks on a regular basis that they have been deactivated, if necessary as specified in the original request.

3.1.7 The Office Manager is responsible for ensuring that the Registration Authority procedure is followed for employees requiring access to patient information provided by use of a smartcard. (See section 3.7 for detailed smartcard access management)

3.1.8 The Office Manager checks that unauthorised privileges have not been obtained.

3.2 Password management

3.2.1 The allocation of passwords is formally controlled.

3.2.2 Users are initially issued with a unique temporary password which they are forced to change at first logon.

3.2.3 Where appropriate controls are available, reuse of passwords is prohibited for three subsequent attempts as a minimum, and strong passwords are required using three random words (https://www.ncsc.gov.uk/cyberaware/home).

3.2.4 The default passwords on all new equipment are changed to conform with Saving Faces' password requirements before the equipment is brought into service.

3.3 Review of access rights

3.3.1 Changing of roles internally may require changes to access control privileges. To maintain effective control over access to data information services,the Office Manager should conduct a formal process quarterly to review user's access rights. The Office Manager will retain records of this review.

3.4 User responsibilities

3.4.1 Where appropriate, paper and computer media are stored in suitable locked cabinets when not in use.

3.4.2 Restricted or confidential business information is locked away when not required.

3.4.3 Laptops and computers are not left logged on when unattended. Passwords or other controls are used to log in securely.

3.4.4 All information, especially confidential or restricted information, when printed, is cleared from printers and fax machine immediately.

3.4.5 Laptops and computers are protected by, passwords, screen savers or equivalent controls when not in use. Laptops and computers have screen saver enabled after 10 minutes of inactivity.

3.4.6 Users are trained not to access patient information in public areas, or in areas which might result in a breach of confidential information.

3.4.7 Any workstations used in public areas must have password-locked screen savers enabled to activate after 10 minutes of inactivity.

3.5 Registration authority/Smartcard procedure

It is important that NHS patient information is kept secure and confidential in line with the *NHS Care Record Guarantee*. To achieve this objective all staff requiring access to these applications must be registered with a Smartcard and have appropriate access profiles. The process enabling smartcards to be issued is handled by the registration authority (RA) within the NHS. Saving Faces will use the RA within the Clinical Commissioning Group (CCG) to provide this service.

3.5.1. The Office Manager is responsible for ensuring this procedure is followed and acts as liaison between Saving Faces and their appointed Registration Authority within the CCG. They will inform the RA of any starters, leavers and staff changes.

3.5.2. The Office Manager will ensure that all Saving Faces employees who require access to patient information via the HSCN (N3) services provide all necessary information required by the Registration Authority.

3.5.3. The Office Manager will ensure that the appropriate level of smartcard access is assigned to Saving Faces staff commensurate with their job responsibilities. They will make sure the employee understands their responsibilities regarding the use of smartcards as agreed to in the employee User Agreement. Applicants who receive a Smartcard will be required to sign to indicate their agreement and acceptance to terms and conditions regarding the use of the card. In particular they agree not to permit anyone else to use their card. If there are any breaches of this agreement the Office Manager should confiscate the card and report the breach as a security incident.

3.5.4. The management and use of smartcards within Saving Faces will be subject to audit to ensure that national and local and national policies are followed.

Specifically, the audit will confirm that a) Smartcards are handled correctly by users, b) smartcard equipment is appropriately secured and c) appropriate levels of access have been assigned to users.

3.5.5. Remote access is provided by a secure virtual private network (VPN) connection.

Compliance

Failure to comply with this procedure could result in action in line with Saving Faces' Disciplinary Procedure.

Document Owner and Approval

The Data Protection Officer (DPO) 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 Chief Executive Officer (CEO) and is issued on a version controlled basis under their signature.

Name	Iain Hutchison
Signature	
Approval Date	23/06/2022
Review Date	23/06/2023

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	CEO	23/06/2021
2	SM review: Amendments to Scope, Review of access rights.Addition of Compliance	SM	09/06/2022