ACCEPTABLE USE POLICY

Document Control
Reference: ACCEPTABLE USE POLICY
Issue Date: 23/06/2022
Issue No: 2

1. Scope

This policy applies to every individual who uses Saving Faces's information assets and it sets out what Saving Faces considers to be the acceptable use of those assets.

1.1 Internet acceptable use

1.1.1 Saving Faces' user IDs, websites and email accounts may only be used for Saving Faces' sanctioned communications.

1.1.2 Use of Internet/email/instant messaging may be **subject to monitoring for reasons of security** and/or network management and users may have their usage of these resources subjected to limitations by Saving Faces.

1.1.3 The distribution of any information through the Internet (including by email, instant messaging systems and any other computer-based systems) may be scrutinised by Saving Faces and Saving Faces reserves the right to determine the suitability of the information.

1.1.4 The use of Saving Faces' computer resources is subject to UK law and any abuse will be dealt with appropriately.

1.1.5 Users may not visit Internet sites that contain obscene, hateful or other objectionable material, and shall not make or post indecent remarks, proposals or materials on the Internet.

1.1.6 Users shall not solicit emails that are unrelated to business activity or which are for personal gain, shall not send or receive any material that is obscene or defamatory, or that is intended to annoy, harass or intimidate another person, and shall not present personal opinions as those of Saving Faces.

1.1.7 Users may not upload, download, or otherwise transmit commercial software or (other than in the ordinary course of business) any copyrighted materials belonging to Saving Faces or any third parties, and may not reveal or publicise confidential information.

1.1.8 Users may not download software from the Internet, or execute or accept any software programs or other code on the Internet unless it has first been authorised by the Data Protection Officer in accordance with Saving Faces' policies and procedures.

1.1.9 Users will not seek to avoid and will uphold Saving Faces' anti-malware policy and procedure, will not intentionally interfere in the normal operation of the network or take any steps that substantially hinder others in their use of the network, and will not examine, change or use another person's files or any other information asset for which they do not have the owner's explicit permission.

1.1.10 User will not carry out any other inappropriate activity, as identified from time to time, either in writing or verbally by Saving Faces and, although limited use of Saving Faces facilities for minor personal administrative tasks such as (for example) banking is permitted, will not waste time or resources on non-organisation business. This includes downloading bandwidth-intensive content such as streaming video and MP3 music files, sharing digital photographs, etc.

1.2 Acceptable email and communication activities

1.2.1 Saving Faces email facilities may not be used for sending defamatory emails, or using email for harassment, unauthorised corporate purchases, or for publishing views and opinions (defamatory or otherwise) about employees, workers, suppliers, partners or customers of Saving Faces.

1.2.2 Saving Faces email may only be used for the communication of official business information or appropriate personal information. Employees/Staff will have no privacy rights over emails sent using Saving Faces email.

1.2.3 Outgoing email attachments must be protected in line with their classification, using cryptographic controls.

1.2.4 Users must not open incoming email attachments that originate with unknown third parties or that, even if they appear to have been sent by a known party (however important that party may appear), were not expected. These attachments may contain viruses, worms or Trojans, and any such emails must be deleted immediately, and on no account should they be forwarded, or copied on, to anyone, whether inside or outside the network. Where more than three such emails are received within a 24-hour period, the instance must be reported to the Data Protection Officer for further investigation.

1.2.5 Viruses and hoax virus messages: users are required to report any third-party emails they receive about viruses to the Data Protection Officer immediately, by telephone or in person, and on no account should it be forwarded, or copied on, to anyone, whether inside or outside the network. See Information Governance Policy and Information Security Guidance for Staff.

1.2.6 Users are required to comply with Saving Faces' Information Security Staff Guidelines

1.2.7 Employees/Staff are required to delete non-essential emails as soon as possible and, on a regular basis, to clear email boxes of correspondence that is no longer required.

1.2.8 Breaches of these requirements may be dealt with under Saving Faces' disciplinary policy.

1.2.9 Use of passwords must always be in line with Access Control Procedure.

ACCEPTABLE USE POLICY

Document Control
Reference: ACCEPTABLE USE POLICY
Issue Date: 23/06/2022
Issue No: 2

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 SF.

A current version of this document is available to all/specified members of staff in Saving Faces' Dropbox.

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

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	Fran Ridout	10.12.2019
2	Updated SF staff roles and references to related policies	Sam Merrett and Iain Hutchison	23.06.2022