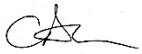
September 2023

Data Protection Policy

Issue date: September 2023

Signed: 

Review period: Annually

IT AND COMMUNICATIONS SYSTEMS POLICY ISSUES AND UPDATES

PAGES	ISSUE / CHANGES	DATE
Full review	1	23/07/2023
About this Policy	Reword to include	
Sara Young to Catherine Deans		25/07/2023

The following policy has been approved by the Senior Leadership Team and the Board of Trustees.

The policy will be reviewed on an annual basis unless circumstances arise requiring the policy to be reviewed earlier.

Approved by Board of Trustees: 27/07/2023.

Board signatory: Jon Drown

Planned review: July 2023

CONTENTS

IT AND COMMUNICATIONS SYSTEMS POLICY

1 ABOUT THIS POLICY

1.1 This policy is designed to facilitate effective communication and promote efficient working practices through our IT and communications systems. It establishes the guidelines that must be followed when utilising these systems, outlines our monitoring practices, and specifies the actions that will be taken in the event of a breach of these standards.

1.2 The ultimate responsibility for this policy lies with the Catherine Deans, Northampton Saints Foundation Managing Director, who is also responsible for regularly reviewing its contents.

1.3 Any violation of this policy may be addressed through our Disciplinary Procedure, and in severe cases, it may be considered gross misconduct, leading to immediate termination of employment.

1.4 It is important to note that this policy does not constitute a contractual agreement between the company and its employees. We retain the right to modify this policy at any time.

2 EQUIPMENT SECURITY AND PASSWORDS

2.1 You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this policy. You should use passwords on all IT equipment, particularly items that you take out of the office. You should keep your passwords confidential and change them regularly.

2.2 You must only log on to our systems using your own username and password. You must not use another person's username and password or allow anyone else to log on using your username and password.

2.3 If you are away from your desk, you should log out or lock your computer. You must log out and shut down your computer at the end of each working day.

3 SYSTEMS AND DATA SECURITY

3.1 You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

3.2 You must not download or install software from external sources without authorisation from the **Managing Director.** Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.

3.3 You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from the Managing Director.

3.4 We monitor all e-mails passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

3.5 Inform the **Managing Director** immediately if you suspect your computer may have a virus.

4 EMAILS

4.1 Adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail. You should also include our standard e-mail signature and disclaimer.

4.2 Remember that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

4.3 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.

4.4 You should not:

4.4.1 send or forward private e-mails at work which you would not want a third party to read;

4.4.2 send or forward chain mail, junk mail, cartoons, jokes or gossip;

4.4.3 contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to others who do not have a real need to receive them; or

4.4.4 send messages from another person's e-mail address (unless authorised) or under an assumed name.

4.5 Do not use your own personal e-mail account to send or receive e-mail for the purposes of our business. Only use the e-mail account we have provided for you.

5 USING THE INTERNET

5.1 Internet access is provided primarily for business purposes. Occasional personal use may be permitted as set out in paragraph 6.

5.2 You should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

5.3 We may block or restrict access to some websites at our discretion.

6 PERSONAL USE OF OUR SYSTEMS

6.1 We permit the incidental use of our systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions. Personal use must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

6.2 Personal use must meet the following conditions:

6.2.1 it must be minimal and take place substantially outside of normal working hours (that is, during your lunch break, and before or after work);

6.2.2 personal e-mails should be labelled "personal" in the subject header;

6.2.3 it must not affect your work or interfere with the business;

6.2.4 it must not commit us to any marginal costs; and

6.2.5 it must comply with our policies including the Equal Opportunities Policy, Anti-harassment and Bullying Policy, Data Protection Policy and Disciplinary Procedure.

7 MONITORING

7.1 Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, your use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise.

7.2 We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

7.2.1 to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;

7.2.2 to find lost messages or to retrieve messages lost due to computer failure;

7.2.3 to assist in the investigation of alleged wrongdoing; or

7.2.4 to comply with any legal obligation.

8 PROHIBITIED USE OF OUR SYSTEMS

8.1 Misuse or excessive personal use of our telephone or e-mail system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

8.2 Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

8.2.1 pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

8.2.2 offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;

8.2.3 a false and defamatory statement about any person or organisation;

8.2.4 material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);

8.2.5 confidential information about us or any of our staff or clients (except as authorised in the proper performance of your duties);

8.2.6 unauthorised software;

8.2.7 any other statement which is likely to create any criminal or civil liability (for you or us); or

8.2.8 music or video files or other material in breach of copyright.