ENCOURAGING EXCELLENCE, NURTURING TALENT!

SPORTING CHANCES GROUP

INTERNET & EMAIL USAGE POLICY

Lead	David Johnson
Last Reviewed	November-2026
Next Review Date	November-2027

To be reviewed **annually**.

This policy is enforced across **all** Sporting Chances Group provisions.

SPORTING CHANCES SURREY

SPORTING CHANCES OUTREACH

SPORTING CHANCES MINI

CREATIVE HAIR&LASHES

SPORTING CHANCES ONLINE

SPORTING CHANCES FITNESS

SC FOOTBALL ACADEMY

CONTENTS

Terminology Disclaimer 3

1. Introduction 3

2. Authorisation 3

3. Legislation & Guidance 3

3.1 UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 & Data (Use and Access) Act 2025 3

3.2 Computer Misuse Act 1990 4

3.3 Copyright, Designs & Patents Act 1988 4

3.4 Defamation Act 2013 4

3.5 Protection from Harassment Act 1997 4

3.6 Counter-Terrorism & Security Act 2015 (Prevent Duty) 4

3.7 Children Act 1989 / Keeping Children Safe in Education (KCSIE) 4

3.8 Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 5

4. Responsibilities 6

4.1 All users are responsible for: 6

4.2 Use of the Internet: 6

4.3 Use of Email / Instant Messaging: 6

4.4 Use of Social Media: 7

4.5 Use of Artificial Intelligence (AI) 7

5. Legitimate Access to Prohibited Material 8

6. Remote Working & Personal Devices 8

7. Filtering & Monitoring 9

8. Penalties for Improper Use 11

9. Policy Review 11

TERMINOLOGY DISCLAIMER

When the terms '*employee*', '*staff member*,' '*staff*,' '*team*,' '*team member*,' '*you*,' '*your*,' '*yours*,' or '*they*' are used in this document and in all Sporting Chances Group (SCG) documentation this is pertaining to self-employed staff, the individual contractor, collective contractors, and volunteers. When you sign this document, you are signing this document to say that you understand that you are a self-employed contractor irrespective of what term is used to describe you.

1. INTRODUCTION

1.1 This policy outlines the obligations and expectations for all SCG staff, including contractors, volunteers and temporary staff, who use the SCG's IT facilities. These facilities are provided to support daily work and learning activities. Responsible use is essential, and all users must understand their legal, professional, and ethical responsibilities.

2. AUTHORISATION

2.1 All users must be authorised by their line manager before using SCG's IT facilities. Unauthorised access is strictly prohibited and may result in disciplinary action, up to and including termination of employment, and may also be subject to criminal prosecution.

3. LEGISLATION & GUIDANCE

All users must comply with relevant legislation and guidance, including but not limited to:

3.1 UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 & Data (Use and Access) Act 2025

This legislation governs the processing of personal data. All personal information held by the SCG, including emails, is subject to these regulations. **Users must:**

- Ensure data is accurate and up-to-date
- Ensure that personal information is processed and shared lawfully, fairly and transparently, in accordance with SCG's Data Protection Policy and the applicable lawful

basis for processing.

- Retain personal information only for as long as necessary
- Ensure appropriate safeguards are in place for transfers of personal data
- Ensure appropriate safeguards are in place for international transfers of personal data
- Adhere to the SCG's data protection policy and procedures.
- Report any data breaches immediately to their line manager and the SCG's Data Protection Officer (DPO), David Johnson

3.2 Computer Misuse Act 1990
This Act prohibits unauthorised access to computer systems, including hacking and the introduction of malware.

3.3 Copyright, Designs & Patents Act 1988
Copyright protects intellectual property. Copying software, music, videos, or other copyrighted materials without permission is illegal.

3.4 Defamation Act 2013
Publishing untrue statements that harm the reputation of an individual or organisation is unlawful. This applies to online communications, including emails and social media.

3.5 Protection from Harassment Act 1997
Harassment, including online harassment, is illegal. This includes any action that creates an intimidating, hostile, degrading, humiliating, or offensive environment.

3.6 Counter-Terrorism & Security Act 2015 (Prevent Duty)
SCG has a duty to prevent people from being drawn into terrorism. Users must not access or share extremist material online.

3.7 Children Act 1989 / Keeping Children Safe in Education (KCSIE)
States that schools and alternative provisions have a safeguarding responsibility to protect children from harm. Users must be aware of online safety risks and report any concerns about child safety, such as; cyberbullying, online grooming, sharing of nude or semi-nude images - including AI-generated images and deepfakes - or online radicalisation. KCSIE provides detailed guidance on safeguarding and online safety, and our Child Protection & Safeguarding Policy outlines our safeguarding procedures around this.

3.8 Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

While these regulations allow for monitoring of communications for specific business purposes, schools and alternative provisions must adhere to data protection legislation and ensure transparency with staff and young people regarding monitoring practices. Any monitoring should be proportionate and necessary.

3.9 Online Safety Guidance

SCG refers to the latest online safety guidance from organisations such as the UK Safer Internet Centre, the National Cyber Security Centre (NCSC), and the Department for Education (DfE).

4. RESPONSIBILITIES

4.1 All users are responsible for:

- Using IT facilities responsibly and ethically
- Protecting their login credentials and not sharing them with others
- Reporting any accidental damage or disruption to IT services immediately to their line manager. This could include;
  - Suspicious emails, phishing attempts and malicious links
  - Lost or stolen devices
  - Suspected unauthorised access or compromised passwords
  - Accidental disclosure or misdirection of confidential information
  - Inappropriate, harmful or potentially illegal online content
  - Any online safeguarding concern involving a child or young person
- Understanding and complying with this policy

4.2 Use of the Internet:

- Internet use should primarily be for educational and work-related purposes
- Reasonable personal use is permitted during non-instructional time (e.g., lunch breaks), but it should be limited and not interfere with work duties or network performance
- Users must not access, view, or download illegal or inappropriate content, including pornography, hate speech, violent content, extremist material, or content that promotes self-harm
- Downloading software or other copyrighted material without permission is prohibited
- Users must not engage in online activities that could bring the SCG into disrepute
- Online gambling and social media use during provision hours (other than for legitimate educational purposes) are generally prohibited

4.3 Use of Email / Instant Messaging:

- SCG email and instant messaging systems are primarily for SCG-related communication
- Personal use should be limited and appropriate
- Users must not send offensive, harassing, discriminatory, or defamatory messages
- Confidential information should be handled with care and not shared inappropriately

via email

- Users should follow email best practices, including using a professional tone, avoiding excessive attachments, and managing their inbox effectively
- When appropriate, staff should set up automated "out of office" email replies. These replies should inform senders who to contact if their matter is urgent. Staff should also notify the designated colleague about this arrangement and, with their colleague's agreement, either grant them access to their email account or make other arrangements for that colleague to monitor their incoming emails during their absence.

4.4 Use of Social Media:

- Users should be mindful of their online presence and avoid posting anything that could damage SCG's reputation
- When representing SCG online (e.g., on social media accounts), users must adhere to the SCG's Social Media, Digital Safeguarding & Media Use Policy
- Personal social media use should be kept separate from SCG-related activities

4.5 Use of Artificial Intelligence (AI)

- Staff may only use AI tools and services that have been approved by SCG for legitimate work-related purposes.
- Staff must not enter personal, confidential or sensitive SCG information, including information relating to children and young people, into AI tools unless specifically authorised in accordance with SCG's Data Protection Policy and AI Framework.
- AI-generated content must be reviewed by the user for accuracy, appropriateness, bias and copyright before it is used, shared or relied upon. Staff remain responsible for all content and decisions supported by AI.
- AI must not be used in a way that compromises safeguarding, confidentiality, professional conduct or the security of SCG systems.
- All staff must follow the **SCG Artificial Intelligence (AI) Use, Safety & Security Framework** for further guidance.

5. LEGITIMATE ACCESS TO PROHIBITED MATERIAL

5.1 In rare circumstances, access to prohibited material may be necessary for legitimate educational or sporting purposes (e.g., research, media studies). Any such access must be authorised by a senior leader and conducted under strict supervision.

6. REMOTE WORKING & PERSONAL DEVICES

6.1 This policy applies to all users, regardless of whether they access SCG's IT facilities, systems and information on SCG premises, remotely or within the community.

6.2 Staff working remotely must:

- Use authorised SCG accounts, platforms and communication systems when carrying out SCG-related work.
- Ensure that devices used to access SCG systems are password-protected and have appropriate security measures in place, including up-to-date operating systems, software and security updates.
- Keep login credentials, passwords and authentication details secure and never share them with others.
- Take reasonable precautions to prevent unauthorised individuals from viewing, accessing or overhearing SCG information, particularly when working in shared or public environments.
- Avoid accessing or handling confidential or sensitive SCG information over unsecured public Wi-Fi networks unless an appropriate secure connection is in place.
- Ensure that physical documents and digital information are stored securely and are not left accessible to unauthorised individuals.

6.3 Where personal devices are authorised for accessing SCG systems or **information, users must:**

- Obtain appropriate authorisation before using personal devices for SCG-related work where required by SCG's IT arrangements.
- Ensure that devices meet SCG's minimum security requirements and are protected by a secure password, PIN or biometric authentication.
- Only access SCG information through approved applications, accounts and services.
- Not download, copy, store or transfer confidential or personal information onto personal devices unless specifically authorised.
- Not share devices used for SCG work with other individuals in a way that could expose SCG information or accounts.
- Report any loss, theft, suspected compromise or unauthorised access involving a device used for SCG work immediately to their line manager and designated IT contact.

6.4 Any suspected loss, disclosure or compromise of SCG information, accounts or devices must be reported immediately in accordance with SCG's Data Protection Policy and relevant IT security procedures.

6.5 SCG reserves the right to restrict or withdraw access to its systems where a device or working arrangement presents an unacceptable security or safeguarding risk.

7. FILTERING & MONITORING

7.1 SCG uses appropriate filtering and monitoring arrangements to help protect staff, children and young people from illegal, inappropriate and potentially harmful online content and activity. These arrangements form part of SCG's wider safeguarding, online safety and IT security procedures.

7.2 SCG reserves the right to monitor the use of its IT facilities, devices, networks and communication systems to ensure compliance with this policy and to protect the safety and security of SCG and its users. Monitoring may include reviewing internet history, email content, files stored on SCG devices and relevant system activity. All monitoring must be proportionate, necessary and carried out in accordance with applicable data protection legislation and SCG's Data Protection Policy.

7.3 SCG management and its designated IT support are responsible for ensuring that appropriate filtering and monitoring arrangements are in place, maintained and reviewed. Responsibilities must be clearly assigned, including where technical services are provided by an external IT provider.

7.4 Filtering and monitoring arrangements must be reviewed at least annually, and following significant changes to technology, working practices or identified safeguarding risks. Reviews should consider whether existing arrangements remain appropriate and effective, whether any gaps or failures have been identified, and whether further action is required.

7.5 All users are responsible for:

- Not attempting to bypass, disable or interfere with SCG's filtering, monitoring or other security controls, including through unauthorised VPNs, proxy services, software or applications.
- Reporting inappropriate or harmful content encountered online, including content that has not been blocked by SCG's filtering systems.
- Promptly reporting suspected failures of filtering or monitoring systems, unauthorised access or attempts to circumvent security controls to their line manager or designated IT contact.
- Following SCG's safeguarding procedures where online activity gives rise to a concern about the safety or wellbeing of a child or young person.

7.6 SCG recognises that filtering and monitoring systems cannot prevent or identify every online risk. They must therefore be supported by appropriate staff supervision, professional judgement, safeguarding procedures and regular review.

7.7 Users must be made aware of SCG's monitoring arrangements, including the purposes of monitoring, the types of information that may be collected and how monitoring information is handled. Further information is provided in SCG's Data Protection Policy and relevant privacy information.

8. PENALTIES FOR IMPROPER USE

8.1 Violations of this policy may result in:

- Restriction or withdrawal of access to IT facilities
- Disciplinary action, up to and including termination of employment
- Referral to law enforcement authorities, where appropriate

9. POLICY REVIEW

9.1 This policy will be reviewed regularly and updated as necessary to reflect changes in legislation, guidance, and best practices.