Seckford Foundation
a foundation for life

Acceptable Use Policy

Version Number:	V 1.0
Applies to:	Whole Foundation
Author (s):	Head of IT Services
Review Frequency:	Annual
Policy category (1, 2, 3, 4):	2
Created:(previously incorporated within another policy)	Michaelmas term 2026
Next review due by:	Michaelmas term 2027
Approved on (date):	Published pending approval
Committee (s) Responsible:	C & R
References (including legal and others eg ISBA).	(relevant publication of) Keeping Children Safe in Education (KCSIE)
ISI Reg:	N/A
Other related policies and documents:	• SF Cyber Security Policy • SF Data Protection Policy • Safeguarding Policies (Care, WBS and SF) • WBS Online Safety Policy • WBS Staff Social Media Policy • WBS Artificial Intelligence Policy • Privacy Notices • Staff Handbooks and Codes of Conduct • WBS Taking, Storing and Using Images of Children Policy SF and WBS Data Retention Schedule and Guidelines

Contents

1. Introduction 2
2. Scope 2
3. Devices and Systems 2
4. Data and system security 3
5. Personal devices and remote working 4
6. Use of Artificial Intelligence 4

7. Reporting Concerns 5
8. Compliance and Monitoring arrangements 5
Appendix A – Unified Acceptable Use Handout 7

1. Introduction

The Seckford Foundation supports the positive use of technology for learning, care, work and organisational development. Technology must be used safely and managed well to protect people, information and systems.

Everyone who uses Foundation technology must do so lawfully, professionally, securely and respectfully. This includes staff, pupils, residents, agency and locum staff, volunteers, Governors, contractors, visitors and other authorised users. Each user must read this policy and follow the rules that apply to them.

This policy sets the Foundation's minimum requirements for using technology. It is intended to support legitimate use while managing security, privacy and safeguarding risks.

Breaking this policy may lead to access being limited, suspended or withdrawn. It may also lead to disciplinary or contractual action. The Foundation may report suspected crimes to the relevant authorities.

2. Scope

This policy applies whenever an authorised user accesses or uses Foundation technology, systems, services, networks or information, whether on Foundation premises or elsewhere. It covers Foundation-owned and personal devices used for Foundation work, including computers, mobile phones, tablets, cameras, storage devices, email, cloud services and network access.

Read this policy together with the relevant Code of Conduct and the Foundation's safeguarding, data protection, cyber security and People Team policies.

The examples in this policy do not cover every situation. All use of technology must follow the law, Foundation policies, safeguarding guidance, contractual requirements and the Foundation's values. If you are unsure what to do, ask your line manager, the Data Protection Officer, a safeguarding lead or IT Services before you continue.

Access to Foundation systems is not intended to confer status of employment on any contractors.

3. Devices and Systems

Only authorised users may use Foundation equipment and services. They are provided primarily for Foundation activities. Staff may make limited and reasonable personal use where it does not affect their work, create extra cost or risk, break another policy, or give access to an unauthorised person. Family members and other unauthorised people must not use Foundation equipment or accounts. The Foundation may restrict or withdraw

personal use at any time. Excessive or inappropriate personal use may lead to disciplinary action.

Any personal device used for Foundation activities must meet the security requirements set by IT Services. Do not use a personal device to work directly with pupils or residents, or to record, store or send their personal information, unless you have written permission. Use Foundation-managed devices and approved services for official contact with pupils and residents.

4. Data and system security

Follow the Foundation's Cyber Security Policy and these rules:

- Lock or sign out of a device before leaving it unattended.
- Use a strong, unique password. Passwords must contain at least 12 characters. A passphrase of four to seven unrelated words is recommended.
- Set up multi-factor authentication when it is available. Never approve a sign-in request that you did not start.
- Take reasonable steps to protect Foundation devices from loss, theft, damage and unauthorised access. Report any loss or theft immediately to IT Services, the Director of Operations and your line manager.
- Keep passwords, authentication codes and other security details private. Do not share them or leave them where another person can find them.
- Use only your own account. Do not use, or try to use, another person's login details. If you need access for your work, ask your line manager, the People Team or IT Services.
- Do not open unexpected links or attachments. If a message may be malicious, report it using the phishing-reporting tool in Outlook, then delete it.
- Do not install or connect software, hardware or services unless IT Services has approved them.
- Handle personal information in line with data protection law and the Foundation's data protection policies.
- Keep Foundation information in approved Foundation systems. Do not send or copy it to removable media, personal accounts or other services unless this is necessary and an approved secure method is used.
- Do not enter, upload or copy personal or confidential information into an unapproved system. A system is approved only when the required data protection assessment, contract and security checks are in place.
- Do not register for or use a system or service for Foundation activities unless the Data Protection Officer and IT Services have approved it. Do not ask pupils or residents to use an unapproved service.
- Do not store Foundation information or documents on a personal device.

- Do not store personal photos, files, music or financial information on Foundation systems. The Foundation is not responsible for personal material stored on its systems.
- Do not use a Foundation email address to register for personal mailing lists, services or subscriptions.
- Use Foundation systems only for lawful and authorised purposes. Do not access, change or interfere with computer systems or information without permission.
- Do not bypass or try to bypass filtering, monitoring or security controls.
- Report a faulty, damaged or compromised device or system to IT Services immediately.
- Respect copyright, licences and intellectual property rights. Do not copy, share or distribute material without permission or a valid licence.
- Install updates promptly when asked. Do not delay them without a valid reason.
- Do not use Foundation systems to distribute malicious software, damage or interfere with another system, gain unauthorised access, or carry out illegal activity.
- Do not access, create or share content that is illegal, abusive, threatening, bullying, discriminatory, pornographic, obscene, deliberately deceptive, extremist, violent, unsafe or likely to raise a safeguarding concern.
- Use respectful and professional language in all digital communications.
- Treat email with the same care as any other formal written communication.
- Do not send sensitive information by email unless an approved encryption or secure-sharing method is used.
- Use only approved, monitored Foundation systems for digital communication with pupils, parents and residents. Do not use personal email, personal messaging services or personal social media accounts for these communications.

5. Personal devices and remote working

Use a Foundation-owned and managed device for Foundation, School and Care Home activities wherever possible. If you are authorised to use a personal device, it must run a supported operating system, have current security updates and anti-malware protection, and be protected by a passcode or equivalent control. Do not share the device while Foundation systems are open or accessible. IT Services may block or remove access if the device does not meet these requirements.

Do not download or store sensitive or confidential Foundation information on a personal device or personal service. When remote access is authorised, use an approved browser or managed application and do not keep a local copy.

6. Use of Artificial Intelligence

Artificial intelligence can support efficient working, but it also creates security, privacy and safeguarding risks. Use only AI tools approved by IT Services and the Data Protection Officer for Foundation activities. Where relevant, approved tools must prevent Foundation

information from being used to train public models, keep information in approved environments, respect user access permissions, and apply suitable security and content-safety controls.

You may use an approved AI tool for tasks such as drafting, summarising, research, proofreading and generating ideas. Check every output for accuracy, bias, suitability, confidentiality, copyright and legal compliance before you use or share it. You remain responsible for all AI-assisted work.

AI must not make a decision about a person or a Foundation process. It must not be the only basis for decisions about admissions, employment, discipline, care or safeguarding. Any approved use of AI to support these activities must include meaningful review by an authorised person and follow the relevant policy and approval process.

Respect copyright, licences and intellectual property rights when creating or using AI-generated content.

Do not assume that an AI tool is private or secure. Never enter sensitive or confidential information into a public or unapproved AI tool. Report any suspected security, privacy or safeguarding concern immediately.

If you are unsure whether an AI tool or proposed use is approved, stop and ask IT Services or the Data Protection Officer before entering information or continuing.

7. Reporting Concerns

Report welfare, safety, data protection and safeguarding concerns promptly through the route set out in the relevant policy. Report technology faults, suspected cyber incidents, lost or stolen devices, unauthorised access, information sent to the wrong person, and suspected data breaches to IT Services immediately. Do not investigate, hide or delay reporting an incident.

The Foundation may investigate unsafe, unprofessional or inappropriate use of its devices, systems or information. Action may include restricting access, disciplinary or contractual action, and recovering losses where the law allows. The Foundation may report a matter to the police, a regulator, a safeguarding authority or another relevant body when it reasonably suspects a crime or has a legal duty to report.

8. Compliance and Monitoring arrangements

The Foundation may monitor, record and review activity on its systems, networks, accounts and devices for lawful reasons. These include cyber security, safeguarding, service management, compliance, investigating possible misconduct, and protecting people and property. Monitoring will be necessary, proportionate and carried out in line with data protection, privacy, employment and human rights law. Authorised staff may access information held or sent through Foundation systems, including email and web-use records,

when there is a lawful and legitimate reason. Users should not expect activity on Foundation systems to be private, subject to their legal rights.

This policy will be subject to a thorough review process by the policy owner including consideration at the Compliance and Risk Committee on an annual basis. This will ensure that practice across the whole Foundation is in line with this policy, the Complaints Procedures and with current guidance and legislation. It will also be reviewed after a significant incident or a major change in technology or the organisation. The review will involve relevant leaders and specialists, and will check that this policy remains consistent with safeguarding, online safety, data protection, cyber security and People Team policies.

Appendix A – Unified Acceptable Use handout

General Principles

- Use Foundation systems and devices responsibly, safely and respectfully.
- Use technology to support approved Foundation, School or Care Home activities.
- Protect your privacy and respect the privacy of others.
- Misuse may lead to restricted access, disciplinary or contractual action, or referral to an external authority.

Responsibilities of All Users

- Use systems and devices only for appropriate and authorised purposes.
- Keep your login details secure and never share your password.
- Report online-safety concerns, inappropriate content and suspicious activity to a safeguarding lead or IT Services.
- Do not use personal devices or accounts for Foundation communication unless you have permission.
- Do not bypass or try to bypass security filters or restricted access.
- Report anything online that may be unsafe or raises a safeguarding concern.
- Use devices discreetly and do not disrupt learning, care or other Foundation activities.
- You are responsible for the security of your personal device. The Foundation is not responsible for its loss, damage or theft.

Monitoring and Enforcement

The Foundation may monitor its digital systems for the lawful purposes set out in this policy. Breaking this policy may lead to:

- access to systems being limited, suspended or withdrawn;
- disciplinary or contractual action; or
- referral to an external authority where required or appropriate.

Agreement

By using Seckford Foundation systems, devices or internet access, you agree to follow this policy.