"Let Your Light Shine"

Frieth C.E.C. School

Online Safety and Cybersecurity Policy

(Including Acceptable Use Agreements)

Member of staff responsible: Headteacher

Governing body committee responsible: Curriculum

Reviewed: Annually

Headteacher's signature: Martin Gosling

Chair of Governor's signature: Jill Dean

Review date: 23.2.26

This policy should be read in conjunction with:

- ICT Policy
- Anti-Bullying Policy
- Safeguarding and Child Protection Policy
- Mobile Phone Policy
- Keeping Children Safe in Education (KCSIE) 2024

At Frieth C.E.C. School we operate within a culture of vigilant safeguarding. We recognise that many forms of abuse can occur online as well as offline and understand the role that technology can play in these. This policy forms part of a whole-school approach to safeguarding, supported by robust infrastructure, clear responsibilities, and secure digital systems.

The school benefits from a modern, cloud-based IT environment managed by **Vocosa Limited**, who migrated the school from on-site servers to the Cloud in late 2024, ensuring secure, resilient data storage and reducing reliance on ageing hardware. The school also uses **SIMS Connected**, a cloud-hosted MIS where the entire service is hosted and processed within the Azure cloud environment.

1. Roles and Responsibilities

The Designated Safeguarding Lead (DSL)

The DSL has overall responsibility for safeguarding and child protection, including online safety. This includes understanding the school's filtering and monitoring systems, cloud-based services, and data protection responsibilities.

The ICT Lead

The ICT Lead will:

- support the DSL with up-to-date information;
- liaise with Vocosa to ensure the safety of pupils;
- understand SIMS Connected security controls, including encryption, hosting, and access management;
- promote safe use of technology across the curriculum.

The Headteacher

The Headteacher ensures appropriate funding for online safety, cybersecurity, and technical infrastructure (including firewall, cloud services and SIMS Connected).

The Governing Body

Governors receive safeguarding and online safety training, including understanding filtering, monitoring, and data protection responsibilities.

All Staff

Staff must:

- follow online safety expectations;
- evaluate websites before use;
- maintain professional conduct online;
- understand that SIMS contains sensitive personal data such as medical information, SEN and welfare information, behaviour, assessment and attendance.

Parents

Parents are expected to support safe internet use at home and reinforce the Acceptable Use Agreements.

Pupils

Pupils must follow their Acceptable Use Agreements and report concerns immediately.

2. Internet Access

The school uses a secure, cloud-based system managed by Vocosa. SIMS Connected is hosted in UK and EEA Azure datacentres, with redundancy across multiple locations.

Filtering and Monitoring

- Watchguard firewall and filtering managed by Vocosa.
- Monitoring tools detect “viruses, intrusions, bots and potentially harmful websites.”

- SIMS Connected monitors service performance but “does not actively track users,” collecting only anonymous telemetry.
- Leadership regularly reviews filtering and monitoring effectiveness.

Supervised Access

Pupils may only use the internet under direct supervision. Staff must pre-check websites and apps before use.

Approach to AI

Our school takes a careful, responsible approach to the use of AI. All pupils and parents sign our Acceptable Use Agreement and Online Safety Rules, which state that no names or personal details will be added to any AI system under any circumstances. Parents confirm that they have discussed these rules with their child, ensuring shared understanding at home. In line with advice from Buckinghamshire Council, the school uses Microsoft Copilot, and all staff follow strict guidance, agreeing not to enter any personal information when using AI tools. This approach keeps safety, privacy and digital responsibility at the centre of our practice.

The school recognises that Microsoft Copilot, offers benefits for staff in reducing workload and supporting teaching and learning. However, in line with the Department for Education’s *Generative Artificial Intelligence in Education* guidance (2025) and statutory safeguarding duties under *Keeping Children Safe in Education* (KCSIE 2025), the use of AI must always prioritise pupil safety, data protection, and responsible practice.

Age-Appropriate and Supervised Use

- Generative AI tools have minimum age requirements, typically 13 years old (e.g., Microsoft Copilot). Primary-aged pupils must not use generative AI tools unsupervised under any circumstances.

Where the school chooses to use AI with pupils, this will only occur:

- under direct adult supervision
- using school-approved tools with appropriate filtering and monitoring
- #Pupils will not create accounts for AI tools, nor will they be encouraged to input personal data, images, or identifiable information into any AI system.

Staff Use of AI

- Staff may use generative AI to support planning, resource creation, and administrative tasks, but must apply professional judgement and check all AI-generated content for accuracy, appropriateness, and bias, as recommended by the DfE.
- AI must not replace professional decision-making or the teacher–pupil relationship.

Incident Response

If inappropriate content is accessed, pupils must turn off the monitor and alert staff immediately. The DSL and Vocosa will review the incident and take appropriate action.

3. Other Restrictions

- Only school-provided email systems may be used.
- Only educational video conferencing is permitted.
- Pupils may not use mobile phones in school.
- Staff must store phones securely and never use personal devices to photograph pupils.

4. ICT Provision

Infrastructure

The school's infrastructure includes:

- Cloud-based storage via Microsoft 365
- Watchguard T45 Firewall
- Meraki 48-port switch
- WPA3 secure Wi-Fi
- Endpoint protection and MFA
- SIMS Connected cloud MIS hosted in Azure

- VPN access for staff

SIMS Data Security Controls

SIMS Connected implements:

- encryption at rest and in transit
- firewalls and anti-virus
- patch management
- penetration testing
- vulnerability scanning
- intrusion detection and prevention
- disaster recovery and business continuity
- access control reviews

Data Processing

The school is the Data Controller. ESS and Vocosa act as Data Processors under written contracts.

Data Entry and Transfer

SIMS supports secure data import via CTF, admissions files, Excel, B2B, and DeX. During onboarding, “the data is encrypted and retained within a secure holding area.”

Data Retention

Offboarded SIMS data is deleted within 30 days.

5. Digital Images

Images of pupils may only be uploaded with parental permission and stored on school equipment. SIMS may store linked documents, but only under the school’s control as Data Controller.

6. The School Website

Only authorised staff and governors may upload or modify content. Passwords must be changed regularly. The Internet Safety Team checks for copyright compliance.

7. ICT at Home and Supporting Parents

Parents are encouraged to:

- supervise internet use;
- use parental controls;
- avoid allowing children to upload personal information;
- report cyberbullying concerns promptly.

Microsoft Teams is used for homework distribution, with usage monitored and logged.

A biannual online safety workshop is delivered to parents, equipping them with practical strategies and guidance to help ensure their children use ICT safely and responsibly at home.

8. Computer Misuse Act and ICT Use in School

Pupils must not delete files, alter settings, or introduce viruses. SIMS Connected supports compliance through access controls, audit logs, and secure authentication.

9. Guidelines for Staff

Staff must:

- avoid using personal devices for photography;
- manage social media responsibly;
- ensure school laptops are used appropriately at home;
- avoid accessing inappropriate material on school devices.

SIMS Connected supports GDPR compliance through rights-based tools (access, rectification, erasure, portability).

10. Ensuring Safer Online Activity in the Classroom

Staff must pre-check websites, use safe search tools, and direct younger pupils to pre-approved sites. If inappropriate material appears, staff must turn off the

monitor, reassure pupils, and report the incident to the ICT Lead. Staff will request site blacklisting through Vocosa.

11. Acceptable Use Agreements (KS1 & KS2)

Frieth Primary School

Acceptable Use Agreement / Online Safety Rules

KS1 Pupils

Think before you click

- ✓ I will only use school technology for school purposes to help me learn.
- ✓ I will only go on to websites that my teacher has chosen for me to use.
- ✓ I will not tell other people my passwords.
- ✓ I will only open/delete my own files or documents.
- ✓ I will make sure that all contact with other children and adults is responsible, polite and sensible.
- ✓ If I see anything that makes me uncomfortable, I will turn the screen off and tell an adult immediately.
- ✓ I will not give out my own details such as my name, address or phone number.
- ✓ When using MS Teams and other technology, I will be responsible for my behaviour and actions.
- ✓ I will not record or take photographs or screenshots of my classmates or teachers during a face-to-face session on MS Teams.
- ✓ I will not share any school content (resources, videos etc.) on social media platforms.
- ✓ I understand that when using MS Teams and other applications provided by the school, my use can be monitored and logged and can be made available to my teachers.
- ✓ I will not make contact with a member of staff through video chat.
- ✓ I will only contact my teacher through the 'chat' if I have a question related to my learning.
- ✓ I will only contact other children through 'chat' if I have a question about my learning.
- ✓ I will not add names and personal details into any AI systems under any circumstances.
- ✓ I will follow these rules because they are to keep me safe.

Pupil

As a user of the school network and learning platform, I agree to comply with these rules on its use.

Pupil name _____ Date: ___/___/2025

Parent

I have discussed these rules with my child. As a responsible parent, I support school policies on digital technology and the Internet. I will monitor my child's use of the Internet. I will also act as a positive role model and will use social media responsibly and in line with the school's values in respect of all matters relating to the school.

Parent Signature _____ Date ___/___/_____

Frieth Primary School

Acceptable Use Agreement / Online Safety Rules

KS2 Pupils

Think before you click

- ✓ I will only use school technology for school purposes to help me learn.
- ✓ I will only access websites that a responsible adult has chosen for me to use.
- ✓ I will only open emails and attachments from people I know.
- ✓ I will not tell other people my passwords.
- ✓ I will only open/delete my own files or documents.
- ✓ I will make sure that all contact with other children and adults is polite and sensible and reflective of our school values.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or offensive. If I accidentally find or am sent something like this I will turn the screen off and tell an adult immediately.
- ✓ I will not give out my own details such as my name, address or phone number.
- ✓ I will not arrange to meet someone that I have met online unless my parent/carer has given their permission and a responsible adult comes with me.
- ✓ I will never share pictures or personal information with people I don't know
- ✓ I will not record or take photographs or screenshots of my classmates or teachers during a face-to-face session on MS Teams.
- ✓ I will not share any school content (resources, videos etc.) on social media platforms.
- ✓ I understand that when using MS Teams and other applications provided by the school, my use can be monitored and logged and can be made available to my teachers.
- ✓ I will not make contact with a member of staff through video chat.
- ✓ I will only contact my teacher through the 'chat' if I have a learning related question.
- ✓ I will only contact other children through 'chat' if I have a question about my learning.
- ✓ I will not add names and personal details into any AI systems under any circumstances.

- ✓ I will be responsible for my behaviour and actions when using TEAMS and other technology because I know these rules are to keep me safe.

Pupil

As a user of the school network and learning platform, I agree to comply with these rules on its use.

Pupil name _____ Date: ___/___/____

Parent

I have discussed these rules with my child. As a responsible parent, I support school policies on digital technology and the Internet. I will monitor my child's use of the Internet. I will also act as a positive role model and will use social media responsibly.

12. Data Protection Impact Statement (DPIS)

12.1 Purpose of this DPI Statement

Frieth C.E.C. School processes significant volumes of personal data relating to pupils, parents, staff, governors, and external agencies. This Data Protection Impact Statement outlines how the school identifies, assesses, and mitigates risks associated with digital systems, online activity, and cloud-based services, including SIMS Connected and Microsoft 365.

This statement supports the school's compliance with the UK GDPR, Data Protection Act 2018, and KCSIE 2024.

12.2 Systems in Scope

This DPI Statement covers:

- - SIMS Connected (cloud-hosted MIS)
- - Microsoft 365 (email, Teams, SharePoint, OneDrive)
- - Watchguard firewall and filtering
- - Cloud-based backups and storage
- - School laptops, iPads, and networked devices
- - Monitoring and safeguarding tools
- - VPN access for staff
- - Website and digital communication platforms

12.3 Nature of the Data Processed

SIMS Connected stores extensive personal data. As stated in the SIMS overview, this includes:

"Name, date of birth, gender, ethnicity, nationality, religion… medical information… SEN and welfare information… behaviour, assessment, attendance and examination details."

Microsoft 365 stores staff and pupil documents, emails, Teams messages, and shared resources.

Vocosa-managed systems store device logs, filtering data, and security alerts.

12.4 Legal Basis for Processing [UK General Data Protection Regulation (UK GDPR)]

As Data Controller, the school processes personal data under:

- Public Task (Article 6(1)(e))
- Legal Obligation (Article 6(1)(c))
- Vital Interests (Article 6(1)(d))
- Consent (Article 6(1)(a)) for optional activities (e.g., photography)

For special category data (e.g., medical, SEN, safeguarding), the school relies on:

- Substantial Public Interest (Article 9(2)(g))
- Safeguarding of children and individuals at risk (Article 9(2)(c))

12.5 Data Controllers and Data Processors

• Frieth C.E.C. School is the Data Controller for all personal data entered into SIMS, Microsoft 365, and school systems.

• ESS (SIMS Connected) is a Data Processor. As stated in the SIMS document:

"ESS is the Data Processor… our customers are the Data Controllers."

• Vocosa Limited is a Data Processor for infrastructure, filtering, monitoring, and device management.

• Microsoft is a Data Processor for Microsoft 365 services.

All processors operate under written contracts compliant with UK GDPR.

12.6 Data Hosting and Transfers

SIMS Connected data is hosted in:

• UK and EEA Azure datacentres, with redundancy across multiple locations.

Microsoft 365 data is hosted in UK/EU datacentres.

No routine transfers occur outside the UK/EEA.

Any exceptional access (e.g., SIMS support escalations) is safeguarded by Standard Contractual Clauses.

12.7 Security Controls

SIMS Connected

- encryption at rest and in transit
- firewalls and anti-virus
- patch management
- penetration testing
- vulnerability scanning
- intrusion detection and prevention
- disaster recovery and business continuity
- access control reviews

School Infrastructure (Vocosa)

- Watchguard T45 firewall
- Meraki switching
- WPA3 secure Wi-Fi
- Endpoint protection
- Cloud-based backups
- VPN access for staff
- Monitoring of threats, intrusions, and harmful content

Microsoft 365

- MFA
- Conditional access
- Encrypted storage
- Audit logs

- Data Loss Prevention (DLP) tools

12.8 Risks Identified and Mitigations

Risk	Impact	Mitigation
Unauthorised access to SIMS data	High	MFA, role-based access, encryption, SIMS access controls
Data breach via email or cloud storage	High	Microsoft 365 security, staff training, DLP
Inappropriate online content	Medium	Watchguard filtering, monitoring, supervised access
Device loss/theft	Medium	Encrypted devices, secure login, remote wipe
Human error (mis-sending data, weak passwords)	High	Annual training, password policies, monitoring
Cyber-attack (malware, phishing, intrusion)	High	Firewall, endpoint protection, Vocosa monitoring
Excessive data retention	Medium	SIMS deletion rules (“all data deleted within 30 days” after offboarding)

12.9 Data Subject Rights

SIMS Connected supports:

- Right of access (SAR reports)

- Right to rectification

- Right to erasure

- Right to data portability (CTF transfers)

12.10 Data Retention

- SIMS support files are deleted within 90 days of incident closure.

- Offboarded SIMS data is deleted within 30 days.

- School retention schedules follow IRMS guidance.

12.11 Residual Risk Assessment

After applying all mitigations, the school assesses the residual risk as Low to Medium, appropriate for a primary school environment with strong technical controls, secure cloud hosting, and robust safeguarding oversight.

12.12 Review Cycle

This DPI Statement, as part of the Online Safety and Cyber Security Policy, will be:

- reviewed annually,

- updated following any major system change,

- approved by the Headteacher and Governing Body

Appendices

1. Online Safety and Cyber Security Guidelines for Adults in School
2. ESS (Education Software Solutions) SIMS Connected Security and Privacy Overview

References

GOV.UK, UK General Data Protection Regulation (UK GDPR).

Available at: https://www.legislation.gov.uk/eur/2016/679/contents (Accessed 17th February 2026)

GOV.UK, Data Protection Act (2016)

Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (Accessed 17th February 2026)

GOV.UK, Keeping Children Safe In Education (2025)

Available at: https://www.gov.uk/government/publications/keeping-children-safe-in-education--2 (Accessed 19th February 2026)

Appendix 1

Device Security Guidelines for Adults in School

1. Protect Access to All Devices

- Always lock your computer, laptop, or tablet when leaving it unattended (ctrl+alt+delete).
- Use strong, unique passwords for all school related accounts.
- Enable two step verification on any personal device used to access school systems, drives, or email .
- Never share login details with others, excepting trusted members of school staff.
- Store passwords securely.

2. Keep School Devices Secure

- Use only school approved devices for accessing sensitive information.
- Ensure school devices are updated with the latest security patches (Vocosa).
- Report lost or stolen devices immediately.
- Supervise children at all times when they are using school devices.

3. Use of Personal Devices

- Do not use personal devices to photograph or video children.
- Avoid accessing sensitive school information on personal devices unless Multi-Factor Authenification is enabled.
- Never store school data on personal devices.

4. Handling Images of Children

- Only take photographs or videos of pupils using school owned devices.
- Follow all school photography and safeguarding policies.
- Do not post images of pupils on personal social media.
- Share images only on official school platforms with recorded parental permission.
- Store images securely and delete them when no longer required.

5. Safe Use of the Internet and Online Platforms

- Visit and evaluate all websites, apps, and online tools before using them in lessons.
- Log out of school platforms after use, especially on shared devices.
- Avoid using public Wi Fi for school systems unless using a secure connection.
- Be cautious of phishing emails, suspicious links, and unexpected attachments.

6. Working From Home

- Keep school and personal workspaces separate.
- Ensure home Wi Fi is password protected and uses WPA2/WPA3.
- Store school devices securely when not in use.

7. Professional Conduct Online

- Maintain professional boundaries on all digital platforms.
- Avoid discussing pupils, parents, or colleagues on personal social media.
- Follow school policy for communication with parents and pupils.