

ICT Code of Conduct – Staff

| | |
|--|----------|
| Contents | |
| Purpose | 2 |
| Related Policies | 2 |
| Definition | 2 |
| General Policy | 2 |
| Username / Password | 3 |
| User Network Area..... | 3 |
| Internet Use | 3 |
| Portable Storage/Devices | 3 |
| Cloud Storage/Google Drive | 4 |
| E-mail | 4 |
| Confidentiality / GDPR | 4 |
| Misuse | 5 |
| Account Management | 5 |
| General Advice | 6 |
| Software, Applications and Websites | 6 |
| SIMS | 7 |
| Firefly | 7 |
| Firefly Communication and Messaging:..... | 7 |
| ClassCharts | 8 |
| CPD Genie | 8 |
| CPOMS | 8 |
| Parents Booking | 8 |
| Other School Systems and Applications | 8 |
| Social Networking | 9 |
| General Advice on Digital Records and Communication | 9 |
| Implementation of the policy and sanctions | 10 |



Purpose

The School network, software, applications and communication facilities connected to it are critical to the administrative, teaching and learning, communication and research activities of Silcoates School.

In order to maintain the stability, integrity and security of the School ICT systems, a policy statement outlining acceptable use provides a framework and guidelines for staff use. The objectives of this policy are to:

- Ensure that the School network and computing facilities are adequately protected against misuse or abuse.
- Ensure that all users understand their own responsibilities for protecting the effective operation of the school network.
- Protect the School's reputation.
- Uphold General Data Protection Regulations.

Related Policies

Please also refer to the following school policies, in conjunction with this document:

- E-Safety, Social & Digital Media Policy
- Privacy Notice
- Retention of Records Policy
- Remote Teaching and Learning Policy (Junior & Senior School versions)
- Taking, Storing & Using Images of Children Policy

These policies can be found on Firefly - [Policies](#) and on the Silcoates School website - [Website policies](#).

Definition

The School ICT systems means the Information Technology infrastructure that exists within the school domain and includes both hardware and software, e.g. computers, laptops, e-mail, on-line learning platform, software applications, printers, photocopiers/scanners, phones and voice mail, including those which are cloud-based.

General Policy

The following general policy statement applies to all computers in school:

- Access to any network connected computer must be via a log-on process that authenticates and authorises the user.
- Any networked system should be locked if left logged on and unattended.
- Any networked system should be shut down overnight. The correct shutdown process should be followed and devices should not be turned off by disconnecting its power source.
- User accounts should be removed and associated material deleted when a member of staff ceases employment.



- Lists of users and their data (such as user ID) must not be shared.
- Users must not deliberately interfere with or attempt to interfere with the operation of the network or computer systems.
- The School ICT systems must not be used for personal gain or profit, including the conduct of business or trading on behalf of yourself or any third party.
- Users must not use the School ICT systems in contravention of the law.
- Be careful when viewing or working on personal data. Users should position screens in a way that avoids casual viewing by others.
- Only software and/or applications approved by the Network Manager may be used.
- Any data protection issues or concerns must be immediately communicated to the Data Protection Officer, Mrs R Thompson – dpo@silcoates.org.uk

Username / Password

- Authorised users are allocated a username and password. They must ensure that nobody else uses it. The user is responsible for the confidentiality of the username and password.
- Users must not use anyone else's username / password.
- Users must not obtain or try to obtain anyone else's password.
- Users must inform the Network Manager immediately if they suspect someone else of using their username / password.
- School computers must not be left unattended when logged on, unless a password protection is used by pressing Ctrl-Alt-Del and then choosing the option to lock the computer, or by holding <Windows> key and letter <L> key together.

User Network Area

- Users must not gain access or attempt to gain access to any files owned by someone else, unless the owner has specifically granted access.
- Users must not download or install software without prior consent from the Network Manager. Use of unauthorised systems/applications is not permitted.
- Users should delete unwanted files on a regular basis and keep personal files to a minimum.

Internet Use

The School network allows connections to the Internet with appropriate monitoring and filtering in place which promote on-line safety, and support the School's Safeguarding and E-Safety Policies. It should be noted that staff access may be monitored and filtered to ensure appropriate use.

Portable Storage/Devices

Personal/portable storage devices, including memory sticks, hard/SSD drives, laptops and mobile phones, must not be connected to the School network unless authorisation has been given by the Network Manager and the device encrypted.



Users should not save files containing personal information (e.g. pupil data) on portable storage devices unless required for specific tasks. These files should be deleted immediately after use.

Users are responsible for taking appropriate steps to prevent portable storage devices from being accessed by unauthorised persons, and from being lost or stolen.

Cloud Storage/Google Drive

Google Workspace and Google Drive have been selected as the School's approved cloud-based storage and resource sharing solution. Users should not store or save School files, documents or other resources in any other cloud-based storage facility.

School Google Drive is linked to users' School accounts and should, therefore, not be used for storage or sharing of personal (non-School related) information or documents. Access to Google Drive is permanently disabled when staff members leave the School and all content is deleted.

Users are able to share files and documents with nominated persons within the School community, including pupils. Care should be taken to ensure that such sharing is appropriate and that sensitive information is protected. Sharing with external accounts is not permitted.

Silcoates School does not separately back-up Google Drive contents. If a file is deleted, it can be recovered from Google servers within a maximum period of 25 days.

In specific circumstances, and where authorised, staff (including Governors) may use the School's Office 365/Sharepoint environment to store and/or share documents or other resources. Access is restricted and strictly controlled by the School's IT Support staff.

E-mail

Confidentiality / GDPR

- E-mail content is disclosable under the 'access to information' data protection regulations; be aware that anything written in an e-mail may be made public.
- E-mail content must be relevant and accurate, and any opinions or comments should be objective in nature and expressed professionally.
- E-mail which is confidential or of a sensitive nature should not be sent unless appropriate precautions are taken to ensure that distribution is limited to relevant parties only.
- E-mailed content or files (attachments) containing sensitive data should be encrypted; get help from the Network Manager.



- If you are sending a message to a number of people (parents) at their personal e-mail address, use the 'Bcc:' field (blind carbon copy) to hide the identity of who the e-mail has been sent to.
 - The Firefly messaging system allows users to send a message to multiple parties without sharing contact details and is the preferred method of communicating with parents.

Misuse

- Users are prohibited from forging or modifying e-mail messages from any other person.
- Users are prohibited from sending pornographic or obscene messages/attachments, or messages/attachments which are abusive, insulting, annoying, malicious, discriminatory (whether on the grounds of sex, race, disability, religion or belief, sexual orientation, age or otherwise), or defamatory about any other person or company.
- Do not forward chain letters / hoaxes or reply to spam. Consult the Network Manager if you are unsure, or delete the e-mail.

Account Management

- Users must not send or distribute large files or attachments without the permission of the Network Manager as their size could have a significant impact on the performance of the School network.
- Attachments to e-mails should only be opened if they come from a known and trusted source. Attachments can contain viruses or other programs that could severely compromise our network. Similarly, links contained in e-mails should be treated with caution and only clicked on when sent from a known or trusted source. Phishing attacks (where attacks appear to come from a reputable source) are becoming increasingly sophisticated and targeted. Users should therefore exercise caution, even when the email may appear genuine. The School uses specialist phishing simulation software to mimic these types of attacks and deliver automated training where appropriate, to help inform how to protect themselves from these types of emails. Any suspicious email should be reported to the IT Helpdesk for further advice, before replying or clicking on any embedded links or opening any attachments.
- If an e-mail containing material of a violent, dangerous, racist, or inappropriate content is received, such a message must be reported immediately to the Network Manager.
- The sending of an e-mail containing content likely to be unsuitable for schools is strictly forbidden.
- Empty your mail boxes (including the 'Sent' and 'Deleted' boxes) on a regular basis.



- E-mail is designed as a communication tool only, and shouldn't be used as a filing system. Save any attachments in a network drive or secure paper files.
- Consider using the 'save as' function to save the e-mail in an electronic location. This will help to locate information, in the event of an 'information access' request.

General Advice

- Do not request 'delivery' or 'read' receipts unless essential.
- Read and check an e-mail before you send it; double check recipients and content for accuracy.
- Avoid blanket e-mailing; make sure your recipients are restricted to your target audience only. Use the e-mail distribution groups to assist with this.
- Use the 'Out of Office' facility if you are going to be absent.
- It is possible to enter into a contract by e-mail in the same way as by letter or phone. Users must ensure that they do not inadvertently enter into contracts by e-mail, using the normal school purchase procedures instead.

Software, Applications and Websites

Only use software and applications which have been authorised for use in School, following an appropriate Data Protection Impact Assessment.

Any website which requires users to register is likely to involve sharing of personal data, rendering it subject to a data protection assessment, regardless of how limited the personal data may be.

Software and applications must not be purchased, installed or used without the appropriate consent.

The current list of authorised systems and applications is in the Tech Support section on Firefly: <https://silcoates.fireflycloud.net/tech-support/authorised-applications--systems--websites>

Please contact ITHelpdesk@silcoates.org.uk for further information.

The following guidelines apply to the use of applications and software by school users:

- No unauthorised access – approved school users only
- Do not share login credentials with other users – use your own login
- Make use of Multi-Factor Authentication, where available
- Do not share information with unauthorised users or third parties
- Take steps to protect (potentially sensitive) data from being shared
- Do not download/export personal data unless required for specific tasks
- Ensure any data or information recorded is **accurate, factual and relevant**, especially where information may be opinion-based



- Securely destroy any output reports containing personal information/data after use (using confidential waste disposal methods)
- Do not leave your screen unattended whilst logged into any applications, software or websites
- If accessing from outside of school, do not save or store any data files on an external device or network, e.g. your home PC
- Any remote access to on-site applications must be via secure, encrypted VPN connection which has been authorised and configured by the Network Manager
- Notify the Data Manager - data@silcoates.org.uk - as soon as possible if a mistake is found or if you are informed of a change to details held in any School system or database.

SIMS

Silcoates School uses SIMS as its Management Information System (MIS) to enter, store, manipulate and retrieve information about the School, staff and pupils. This data is confidential and should not be shared with any person or organisation outside of school. Data held electronically is subject to the General Data Protection Regulations.

Access to SIMS is restricted, password protected and reserved for the explicit purpose of supporting effective school administration.

Firefly

Silcoates School uses an on-line learning platform, Firefly, for pupils and staff. It also serves as a Parent Portal, displaying key information about pupils and provides a facility for communicating with parents.

Access to Firefly content should be restricted according to intended audience by making use of the built-in permissions functionality. Be aware of how the hierarchical nature of permissions affects access. Seek assistance from the IT Helpdesk/Data Manager where required.

Content creators/owners should ensure that it is appropriately sited within Firefly and is regularly reviewed to ensure it is up-to-date.

Firefly Communication and Messaging:

- Only authorised users should send messages to parents via Firefly.
- Only authorised users should publish communications (including newsletters and pupil progress reports).
- Message content should be factual and written in a professional manner.
- Messages are set to enable replies, by default. This may be disabled, or changed to other response types, where necessary.
- Check to ensure recipient selections are validated before message publication.
- Refer to the guidelines on the use of e-mail, provided in this policy, as the same rules and best practice apply to communications sent via Firefly.



- Please refer to [SchoolPost instructions](https://silcoates.fireflycloud.net/tech-support/training-and-user-guides/sims-user-guides/user-guides/schoolpost) on Firefly for further information and guidance. <https://silcoates.fireflycloud.net/tech-support/training-and-user-guides/sims-user-guides/user-guides/schoolpost>

ClassCharts

ClassCharts is a cloud-hosted software application designed to record and manage both positive and negative behavioural events, and is integrated with SIMS.

CPD Genie

CPD GENIE is a cloud-hosted software application designed to record and manage staff professional development [currently limited to Teaching staff]. Access is restricted, password protected and reserved for the explicit purpose of supporting professional development of employees.

CPOMS

CPOMS is a cloud-hosted software application designed to record and manage safeguarding information relating to pupils, including behavioral issues, bullying, special educational needs, domestic issues and other pastoral matters of a sensitive nature.

Access to CPOMS is restricted to designated users only, who have additional responsibility for safeguarding within their role. Access is password protected and reserved for the explicit purpose of supporting safeguarding and pastoral concerns.

Parents Booking

Parents Booking, accessed via Firefly, provides parents with on-line appointment booking functionality for parents' evenings and provides teachers with access to their parent-teacher meeting schedules. Parents Booking is also able to facilitate virtual parents' evenings, should this be required.

Care should be taken to ensure that the parent contact details, available in the Parents Booking system, are protected and kept confidential.

Other School Systems and Applications

New technologies are evolving, and being adopted, on an ongoing basis (see section on **Software, Applications and Websites**)

Other applications/websites approved for use in School, including those which may have limited functionality, remain subject to the same principles for responsible use. The guidance provided in this policy applies to all systems used in the course of conducting School related business, teaching and learning.



Social Networking

All staff have a responsibility to uphold a professional image, which can be affected on-line conduct. In accordance with the **E-Safety, Social & Digital Media Policy**, you must ensure these directions are followed:

- Do not accept pupils (or ex-pupils who are minors) as 'friends' on social networking sites.
- Do not initiate 'friendships' with pupils.
- Do not make public any posts which may be deemed to be defamatory, obscene or libellous.
- Consider whether a particular posting puts your effectiveness or reputation as a school employee at risk.
- Post only what you are happy for the world to see. Imagine students and their parents visiting your social networking area and consider whether they would be shocked or offended by what they might see.
- Do not publicly discuss pupils, parents or colleagues or criticise school policies or personnel.
- Do not post images that include pupils.
- Be aware of your on-line accessibility and review your privacy settings on any social media accounts.

General Advice on Digital Records and Communication

All digital communication content is disclosable under the 'access to information' data protection regulations. This could include, but not limited to:

- E-Mail
- Firefly messaging
- Social media platforms
- WhatsApp
- Text messaging
- Messenger

Be aware that anything recorded digitally may be made public in exactly the same way as written records and should always be factual, objective and accurate and in a professional style.



Implementation of the policy and sanctions

The responsibility for implementing this policy rests with the Assistant Head (Teaching and Learning). Any breach of network security should be reported to the Assistant Head (Teaching and Learning), the Network Manager and the Data Protection Officer, who will ensure that appropriate action is taken. In the event of a suspected or actual breach of security, the user's account may need to be disabled until further investigations have been carried out.

Failure of a member of staff to comply with this policy may lead to the instigation of the relevant disciplinary procedures. In the event of a serious infringement, the School reserves the right to institute legal proceedings.

The School is fully committed to ensuring that the application of this policy is non-discriminatory in line with the UK Equality Act (2010). Further details are available in the School's Equal Opportunity Policy document.

| | | | |
|-----------------------------|--|-----------------------------|------------|
| Reviewed by: | Michael Collinson (Network Manager) Mrs Redfearn – Assistant Head (Teaching and Learning) Rebecca Thompson (Data Protection Officer) | | |
| Date of last review: | April 2023 | Date of next review: | April 2024 |

