Mill Green School

ICT and Internet Acceptable Use Policy

including the Use of Social Media

Policy Status:	**NON-STATUTORY**
Person Responsible:	**Stephanie Shipley**
Issue Date:	**September 2025**
Review Date:	**September 2026**

Contents

Introduction

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for young people, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school. However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, young people, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching young people safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, young people, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under the School Disciplinary Procedures

Relevant Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

Definitions

When reading this policy, the following definitions should be referred to:

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, young people, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

Unacceptable Use of ICT & the Internet

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute

- Sharing confidential information about the school, its young people, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher or Deputy Headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

Any exceptions are considered on a case-by-case basis and require the staff member to submit a request for exemption directly to the headteacher, including a robust rationale as to why an exemption is required.

Sanctions

Young people and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies and procedures including the staff code of conduct and School Disciplinary Procedure.

Additional sanctions may include, but are not limited to restriction or revocation of permission to use school systems, safely storing staff personal mobile devices in a central, secure location e.g. the school office where brought into school.

Staff (including governors, volunteers and contractors)

Access to school ICT Facilities and Materials

The school's School Business Manager and ICT Technician manage access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices

- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the School Business Manager in the first instance.

Additional requests for ICT support, including requests to access files / facilities can be made via the Agilisys Hornbill icon from any desktop or laptop device.

Use of phones and email

The school provides each member of staff with an email address on the @millgreen.org.uk domain.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s) where required.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents/carers and young people, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email, especially to external email addresses. Any attachments containing sensitive or confidential information should be encrypted using the facility in the Outlook email client so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the School Business Manager immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or young people. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out within this policy.

Personal Use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Headteacher may withdraw or restrict this permission for an individual at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time with young people.
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no young people are present
- Does not interfere with their jobs, or prevent other staff or young people from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities as outlined within this policy. Where breaches of this policy are found, disciplinary action may be taken.

Staff are permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Mobile Phone Policy. This should not take place during contact time or during the working day, when young people are on site, other than in a non-learner accessible space such as the Staff Room, when staff are on their break.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where young people and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media (see appendix 1) and use of email to protect themselves online and avoid compromising their professional integrity.

Personal Social Media Accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times (see appendix 1). They should also ensure that their social media profiles are restricted to prevent unwanted stakeholder access.

School Social Media Accounts

The school has an official X, Instagram, Facebook and LinkedIn accounts, managed by agreed members of staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

Remote Access

We allow staff to access the school's ICT facilities and materials remotely. This is either via Microsoft 365 Cloud access or by connecting in using the LGfLFreedom2Roam virtual private network (VPN) via the AnyConnect Client

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions as the ICT Technician may require against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

Monitoring and Filtering of the School Network and use of ICT Facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The school uses LGfL to filter what is accessible through the school network and has active monitoring of all internet, computer and iPad use through Securus. These systems ensure that Mill Green is able to be both proactive and responsive to any safeguarding concerns relating to the use of ICT within the school and also ensures compliance with the DfE filtering and monitoring standards.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing body is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns

It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

Young People

Access to ICT Facilities

- Computers and equipment in the school's ICT suite and ICT Resource Base e,g. iPads are available to young people only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff

Search and Deletion

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search young people and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or young people, and/or
- Is identified in the school rules as a banned or prohibited item for which a search can be carried out and/or
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children

- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other young people and staff. If the search is not urgent, they will seek advice from a member of the Senior Leadership Team
- Explain to the young person why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the young person's co-operation

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a young person was in possession of a banned or prohibited item. A list of banned and prohibited items is available within the school behaviour policy.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of young people will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Behaviour Policy

Any complaints about searching for, or deleting, inappropriate images or files on young people' devices will be dealt with through the school complaints procedure.

Unacceptable use of ICT and the Internet outside of School

- The school will sanction young people, in line with our Behaviour Policy], if a pupil engages in any of the following at any time (even if they are not on school premises):
- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other young people, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Parents / Carers

Access to ICT facilities and materials

Parents/carers do not have access to the school's ICT facilities as a matter of course.

However, parents/carers working for, or with, the school in an official capacity (for instance, as a staff member, volunteer or as a member of the PTFA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

Communicating with or about the school online

We believe it is important to model for young people, and help them learn, how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

Data Security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, young people, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or young people who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the School Business Manager & ICT Manager

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the School Business Manager & ICT Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT Manager.

Protection from Cyber Attacks

Please see the glossary (appendix 2) to help you understand cyber security terminology.

The school will:

- Work with governors and Agilisys make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
  - Check the sender address in an email
  - Respond to a request for bank details, personal information or login details
  - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
  - **Proportionate**: the school, via Agilisys will verify this using a third-party audit to objectively test that what it has in place is effective
  - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
  - **Up to date:** with a system in place to monitor when the school needs to update its software
  - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data on a daily basis and store these backups securely.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to Agilisys.
- Make sure staff:
  - Dial into our network using a virtual private network (VPN) when working from home
  - Enable multi-factor authentication where they can, on things like school email accounts
  - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification

Monitoring and Review

The Headteacher, School Business Manager and ICT Manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every two years.

Appendix 1: Addendum – Staff Use of Social Media

Introduction

The internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as Facebook to keeping up with other people's lives on X and maintaining pages on internet encyclopedias such as Wikipedia.

Whilst the widespread availability and use of social networking applications brings opportunities to engage and communicate with audiences in new and exciting ways, it is important to ensure that we balance this not only with our legal responsibilities to safeguard and protect our children and staff but also with the need to safeguard the school image and reputation.

The school E Safety Policy which includes a wider range of information on home and school ICT use, security & safeguarding issues (including how all school staff will be made aware of relevant issues and whom they should contact within the school if any concerns arise) should be read alongside this policy, as well as all relevant school policies concerning data and technology in all aspects.

Purpose

The purpose of this policy is to:

- support safer working practice by setting out the key principles and expected standards of behaviour when using social networking media
- ensure all children are safeguarded
- ensure the reputation of the school (its staff, young people and governors at the school) are not damaged or compromised
- ensure that any users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the School
- minimise the risk of misplaced or malicious allegations being made against those who work with young people
- reduce the incidence of positions of trust being abused or misused
- ensure the school, its governors and staff are not exposed to legal risks

Scope

This policy applies to the governing body, all teaching and other staff, whether employed by St Helens Borough Council or employed directly by the school, individual governors, external contractors providing services on behalf of the school or the Council, teacher trainees and other trainees, supply staff, agency workers, volunteers and other individuals who work for, or provide services on behalf of, the school. These individuals are collectively referred to as 'staff members' in this policy.

This policy cannot cover all eventualities and, therefore, staff members should consult the Headteacher, ICT Manager and/or Data Protection Officer if they are in any way unsure about what is and isn't acceptable use of social media.

Legal Framework

Mill Green School is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of the law and professional codes of conduct.

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. young person and employee records protected by the Data Protection Act 1998
- Information divulged in the expectation of confidentiality
- School or St Helens Borough Council business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media.

Mill Green School and St Helens Borough Council could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc. or who defame a third party while at work may render the school or the Council liable to the injured party.

Definition of Social Media

Social media is the term commonly used for websites which allow people to interact with each other in some way by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook, X (formerly Twitter), Instagram and TikTok are perhaps the most well- known examples of social media but the term also covers other web-based services such as blogs, mircoblogs, chatrooms, fora, video and audio podcasts, open access online encyclopaedias such as Wikipedia, message boards, photo document, social bookmarking sites such as del.icio.us and content sharing sites such as Flickr and YouTube.

This definition of social media is not exhaustive. The internet is a fast-moving technology and it is impossible to cover all circumstances or emerging media. However, the principles set out in this policy must be followed irrespective of the medium.

For the purpose of this policy, the term social media also applies to the use of communication technologies such as mobile phones, tablet devices, Smart Watches, Home Assistants e.g. Alexa / SIRI, other smart devices and any other emerging forms of communications technologies.

Principles - Social Media Practice

Staff members need to be aware (and should assume) that everything they post online is public, even with the strictest privacy settings. Once something is online, it can be copied and redistributed and it is easy to lose control of it. They should therefore assume that everything they post online will be permanent and will be shared.

Staff members must be conscious at all times of the need to keep their personal and professional lives separate and to always maintain appropriate professional boundaries.

Staff members are responsible for their own actions and conduct and should avoid behaviour which might be misinterpreted by others or which could put them in a position where there is a conflict between their work for Mill Green School or St Helens Borough Council and their personal interests.

They must use social media in a professional, responsible and respectful way and must comply with the law, including equalities legislation, in their on-line communications.

Staff members must not engage in activities involving social media which might bring the school or the Council into disrepute.

They must not represent their personal views as those of the school or the Council on any social medium.

They must not discuss personal information about young people, their family members, school or Council staff or any other professionals or organisations they interact with as part of their job on social media.

They must not name or otherwise identify young people, former young people or their parents, family members, colleagues etc. in social media conversations.

They must not use social media or the internet in any way to attack, insult, abuse, defame or otherwise make negative, offensive or discriminatory comments about young people, their family members, colleagues, other professionals, other organisations, the school or the Council.

They must not browse, download, upload or distribute any material that could be considered inappropriate, offensive, defamatory, illegal or discriminatory.

They must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

Personal Use of Social Media

Staff members need to be aware of the dangers of putting personal information such as addresses, home and mobile phone numbers, email addresses etc. onto social networking sites.

Staff members should ensure that they set the privacy levels of their personal sites at the maximum and opt out of public listings on social networking sites to protect their privacy.

Staff members should keep any passwords confidential, change them often and be careful about what is posted online. It is a good idea to use a separate email address just for social networking so that any other contact details are not disclosed.

Staff members should not identify themselves as employees of the school Council or service providers for the school in posts on social media including message boards, fora etc. This is to prevent information on these sites being linked with the school or the Council. Where applicable, staff should add a disclaimer such as “these are my own views and opinions and not those of my employer” e.g. on professional social media platforms such as LinkedIn

Taking the steps outlined above will avoid the potential for staff members to be contacted by young people or their families or friends outside of the school environment and will reduce the chances of them becoming victims of identity theft.

All staff members should try to regularly review their social networking sites to ensure that information available publicly about them is accurate and appropriate. This should be suggested to new staff when they join the school. It is also good practice to close old accounts as they may contain personal information about you.

Staff members must not give their personal contact details including details of any blogs or personal social media sites or other websites to young people or former young people. It is also important to be aware that ex-young people may still have siblings in the school.

Staff members must not have contact through any personal social medium with any young person, whether from this or any other school, unless the young person is a family member / family friend or it is through school approved sites as part of official collaborative work.

The school does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.

It is strongly recommended that staff members do not have contact with young people’s family members through personal social media.

Staff members must not establish, or seek to establish, social contact via social media/other communication technologies with young people or ex-young people and must never ‘friend’ a young person or ex- young person through social media. These actions could be construed as being part of a ‘grooming process’ in the context of sexual offending. In the case of some social networking sites it is possible to be ’followed’ by a pupil without

your consent. If this is the case, then you should inform the Headteacher and the young person 'follower' blocked / deleted.

Staff members must never use or access young people' social networking sites.

Staff members must decline 'friend requests' from young people they receive in their personal social media accounts. If they receive such requests from young people who are not family members, they must discuss these in general terms in class and signpost young people to become 'friends' of the official school site or follow the school's own policy.

Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss or publish inappropriate information. Staff members must therefore make sure that they do not publish confidential information that they have access to as part of their employment on their personal webspace. This includes personal information about young people, their family members, colleagues, St Helens Borough Council staff and other parties as well as school or St Helens Council related information. This requirement continues after they have left employment.

Similarly, photographs, videos or any other types of image of young people and their families or images depicting staff members wearing clothing with school logos or images identifying sensitive school or Council premises) must not be published on personal social media / webspace.

The school logos must also not be used or published on personal webspace.

Staff members must not use school email addresses and other official contact details for setting up personal social media accounts or for communicating through such media.

Staff members must not edit open access online encyclopaedias such as Wikipedia in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

Staff members are advised to be cautious about inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and this may make it difficult to maintain professional relationships or embarrassing if too much personal information is known in the work place.

On leaving the service of Mill Green School School, staff members must not contact Mill Green School young people by means of personal social media sites. Similarly, staff members should not contact young people from their former schools by means of personal social media.

Breaches of the Policy

Any breach of this policy may lead to disciplinary action, including the possibility of dismissal being taken against the staff member/s involved in line with the Schools Disciplinary Procedures.

Contracted providers of Mill Green School or St Helens Borough Council services must inform the School Business Manager / Headteacher immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school and the Council.

Any action against breaches should be according to contractors' internal disciplinary procedures.

Appendix 2: Glossary of Cyber Security Terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

Term	Definition
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.

Term	Definition
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

Mill Green School

Lansbury Avenue

St Helens

Merseyside

WA9 1BU

Telephone: 01744 678760

Email: millgreen@millgreen.org.uk

Website: www.millgreen.org.uk