



ICT Acceptable Use Policy (September 2026)

This policy is for the whole nursery and school

Written by: RS GU	September 2026
Current version no: 1	
Reviewed:	September 2026
Approved by the Governing Body:	September 2026
Next review:	September 2027

Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for students, 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:

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

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

Breaches of this policy may be dealt with under our disciplinary policies.

Relevant legislation and guidance

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

- o [Data Protection Act 2018](#)
- o 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](#)
- o [Computer Misuse Act 1990](#)
- o [Human Rights Act 1998](#)
- o [The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)



Sancton Wood School

- o [Education Act 2011](#)
- o [Freedom of Information Act 2000](#)
- o [Education and Inspections Act 2006](#)
- o [Keeping Children Safe in Education 2022](#)
- o [Searching, screening and confiscation: advice for schools 2022](#)
- o [National Cyber Security Centre \(NCSC\): Cyber Security for Schools](#)
- o [Education and Training \(Welfare of Children\) Act 2021](#)
- o UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- o [Meeting digital and technology standards in schools and colleges](#)

Definitions

- 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 which 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, students, 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 or contractors 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 5 for a glossary of cyber security terminology.

Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

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



Connecting any device to the school's ICT network without approval from authorised personnel

- o 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
- o Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- o Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- o Causing intentional damage to the school's ICT facilities
- o Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- o Causing a data breach by accessing, modifying, deleting, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- o Using inappropriate or offensive language
- o Promoting a private business, unless that business is directly related to the school
- o Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- o 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 Senior Leadership Team 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.

Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies for students and staff.

Staff (including governors, volunteers, and contractors)

Access to school ICT facilities and materials

The school's Network Manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- o Computers, tablets, mobile phones and other devices
- o 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, must contact the IT Helpdesk.

When not using the schools ICT facilities staff must ensure that screens are locked (Windows Key + L or ctrl + alt + del on the keyboard).

Use of phones and email

The school provides each member of staff with an email address. This email account must be used for work purposes only.

Multi-factor authentication is enabled for the email account when not connected to the school network. All work-related business must be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and students 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 of 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. Any attachments containing sensitive or confidential information must be encrypted so that the information is only accessible by the intended recipient.

When sending emails to multiple recipients, the blind carbon copy (BCC) facility should be used to ensure email addresses are not visible to other recipients. This is especially important for external emails.

If staff receive an email in error, the sender must 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 Director of Operations and Network Manager immediately and follow our data breach procedure.



Staff must not give their personal phone number(s) to parents or students. 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 in section 4.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

Passwords

Passwords must be a mix of uppercase and lowercase, numbers and special characters (i.e. #, &, !), must be at least six characters in length and must not be disclosed to anyone else.

Your password should be difficult to guess, for example, you could base your password on something memorable that no-one else would know.

Passwords should be changed regularly (for example term) and your updated password should not be similar to the previous one (for example do not change your password by just adding a number each time, e.g. orchard1, orchard2, orchard3 etc).

Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else.

Passwords must not be written down.

Portable Media Devices

Portable media devices (USB drives, portable hard drives, DVD etc.) should only be used when provided by the school and encrypted in case of accidental loss.

If portable media devices are lost or stolen, this must be reported immediately to the Director of Operations.

Remote Working (off-site working)

We allow some staff to work remotely and access the school's ICT facilities and materials remotely.

When working remotely staff must

- Ensure only the minimum required information is taken off-site (e.g. a teacher organising a field trip might need to take with her information about student medical conditions (for example allergies and medication etc). If only eight out of a class of twenty students are attending the trip, then the teacher must only take the information about the eight students.)
- Ensure access to any information cannot be seen by unauthorised people. This includes paper copies and computer screens.
- Never leave a device unattended.



- o Secure both ICT devices and paper documentation when not in use (e.g. Ensure in a bag, hidden from casual site).

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 take such precautions as ensuring that security software is installed and working.

When working remotely staff must be careful that their facilities and materials are secure and cannot be overlooked to prevent any data breaches. Any breach or loss/theft must be reported immediately to the Director of Operations and the Network Manager. If ICT facilities must be used remotely, appropriate measures should be taken to prevent inadvertent data breaches (e.g. overlooking of the screen) by using devices like privacy filters and laptop locks.

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.

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 school may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

Does not constitute 'unacceptable use', as defined in section 4 ➤ Takes place when no students are present

Does not interfere with their jobs, or prevent other staff or students 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 (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Code of Conduct Policy.

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 students and parents 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 (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.



Personal email accounts

Personal email accounts must not be used for school related work or to contact parents or students.

Personal cloud storage

Personal/private cloud storage must not be used to hold any school data. Each teacher is provided with a school OneDrive account when cloud storage is required.

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.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

Paper documents

Paper documents must be kept in a locked, secure location (e.g. desk drawers or filing cabinets) when not in use and not left unattended on desks.

Sensitive and confidential documents must be kept in secure cabinets when not in use.

Paper records containing any school data must be disposed of securely by placing them in the confidential waste bins provided around the school. They must never be placed into general waste.

Only print documents where necessary. The school uses a 'follow me' print method where printing is only started when you are at the printer. Some locked offices and classrooms have local printers which are only accessible to devices usually located in those rooms.

Once a document is printed, it must be taken straight away and not left on the printer to prevent it being read or taken by anyone else.

School social media accounts

Any school social media accounts must only be managed by authorised staff members.

Unauthorised staff members must not attempt to manage, or post to, 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.



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:

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

Only authorised personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The effectiveness of any filtering and monitoring will be regularly reviewed.

Where appropriate, authorised personnel may raise concerns about monitored activity with the school's designated safeguarding lead (DSL) and Director of Operations, as appropriate.

The school monitors ICT use in order to:

- o Obtain information related to school business
 - o Investigate compliance with school policies, procedures and standards
 - o Ensure effective school and ICT operation
 - o Conduct training or quality control exercises
 - o Prevent or detect crime
 - o Comply with a subject access request, Freedom of Information Act request, or any other legal obligation
- The governing board will regularly review the effectiveness of the school's monitoring and filtering systems.

Students

Access to ICT facilities

Students are provided with access to the school ICT systems and facilities as necessary for the education

- Computers and equipment in the school's ICT suites and laptop trolleys are available to students 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
- Students will be provided with an Office 365 account which they can access from any device by using the following URL <https://office.com>

Search and deletion

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

- o Poses a risk to staff or students, and/or



- Is identified in the school rules as a banned item for which a search can be carried, 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 students and staff. If the search is not urgent, they will seek advice from the designated safeguarding lead or a member of the senior leadership team.

➤ Explain to the student 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 student's co-operation The authorised staff member must:

➤ Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a student was in possession of a banned item.

- 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, 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 the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team 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 if there is a good reason to erase data or files from a device, staff members will consider if 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 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 student 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) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of students will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy / searches and confiscation policy

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

Unacceptable use of ICT and the internet outside of school

The school will sanction students, in line with the behaviour policy, if a student 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 students, 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, deleting, 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

Access to ICT facilities and materials

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



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

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

Communicating with or about the school online

The school's policy is that it is important to help students to learn by modelling how to communicate respectfully with, and about, others online.

Parents 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.

Parents are therefore asked to sign the agreement in appendix 2.

Communicating with parents about student activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When students are asked to use websites or engage in online activity by the school, the school will communicate the details of this to parents in the same way that information about homework tasks is shared.

In particular, staff will let parents know which (if any) person or people from the school students will be interacting with online, including the purpose of the interaction.

Parents may seek any support and advice from the school to ensure a safe online environment is established for their child.

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, students, parents and others who use the school's ICT facilities should use safe computing practices (e.g. locking the computer when not at the computer, not downloading unknown files, not opening attachments on emails unless known to be safe, reporting any concerns to the IT Helpdesk) 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:

- o Firewalls
- o Security features
- o User authentication and multi-factor authentication



Sancton Wood School

- o Anti-malware software
- o Passwords

All users of the school's ICT facilities must set strong passwords for their accounts and keep these passwords secure. Passwords must be a minimum of 8 characters long and include three of the following levels of complexity – upper case, lower case, number and special characters (e.g. !#%&*)

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 students 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.

All passwords have an expiry after which they must be changed. This is typically set to 180 days and can only be reset when on the school network. New passwords must not utilise the old password (e.g. a password of 'orchard1' must not be changed to 'orchard2').

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 controls 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 according to the school's information and cyber security standards.

Data protection

All personal data processes and / or stored on the school's ICT must be processed and stored in line with 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 schools IT department and Network Manager.

Users must 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 must alert the Network Manager immediately.



Users must always log out of systems and lock their devices when not in use to avoid any unauthorised access. Devices and systems must always be logged out of and shut down completely at the end of each working day.

Encryption

The school appropriately encrypts data held on its devices and systems.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as student 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 Network Manager.

Internet access

The school's wireless internet connection is secure.

Access to the internet through the wireless network is filtered.

Staff have access to a separate network for their devices, which has access restrictions to the rest of the network and different filtering policies.

Students

Students must only use school provided devices on the schools' network. They are not permitted to connect any personal devices to either the wired or wireless network.

Parents and visitors

Parents and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by a member of SLT.

A member of SLT will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of SWPA)
- Visitors need to access the school's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)
- Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

Monitoring and review

The Headteacher and Director of Operations 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 three years (or if required by national guidance or statute).
The governing board is responsible for approving this policy.

Related policies

This policy should be read alongside the school's policies on:

- o Child Protection and Safeguarding
- o Behaviour
- o Staff Code of Conduct and Conduct Policy
- o Data Protection
- o E Safety



Appendix 1: Facebook cheat sheet for staff

10 rules for school staff on Facebook

Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead

Change your profile picture to something unidentifiable, or if you don't, ensure that the image is professional

Check your privacy settings regularly

Be careful about tagging other staff members in images or posts

Don't share anything publicly that you wouldn't be just as happy showing your students

Don't use social media sites during school hours

Don't make comments about your job, your colleagues, our school or your students online – once it's out there, it's out there

Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)

Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information

Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or students)

Check your privacy settings

➤ Change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'.

Otherwise, students and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list

➤ Don't forget to check your old posts and photos – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

➤ The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster

➤ Google your name to see what information about you is visible to the public

➤ Prevent search engines from indexing your profile so that people can't search for you by name – go to bit.ly/2zMdVht to find out how to do this



➤ Remember that some information is always public: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if ...

A student adds you on social media

- In the first instance, ignore and delete the request. Block the student from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior leadership and/or their parents. If the student persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
Students may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, contact the Director of Operations for guidance on drafting a response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- Do not retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current student or staff member, inform the Headteacher or Director of Operations who will act in accordance to the appropriate policy.
- If the perpetrator is a parent or other external adult this must be reported to a member of the senior leadership team so a senior member of staff can invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime this must be reported to a member of the senior leadership team and you, or a senior leader should consider contacting the police.

Section	Details
---------	---------



Name of Parent/Carer	
Name of Child	
School Communication Channels	- Email & Parent Portal (for school announcements and information) - Microsoft Teams (Virtual Learning Platform) - School Cloud (Parents' Evening Bookings)
Parent/Carer Responsibilities	- Be respectful towards members of staff and the school at all times - Be respectful of other parents/carers and children - Raise complaints via official school channels
Parent/Carer Restrictions	- Do not use private groups, the school's Facebook page, or personal social media to criticise staff - Do not use social media to resolve behaviour issues involving students —contact the school instead - Do not upload/share photos or videos of any child other than your own without permission
Signed	
Date	



Appendix 2: Acceptable Use of the Internet – Agreement for Parents and Carers

Field	Information
Name of parent/carers:	
Name of child:	

The school uses the following channels:

- Email & Parent Portal (for school announcements and information)
- Microsoft Teams (Virtual Learning Platform)
- School Cloud (Parent Evening bookings)

Parent/Carer Agreement	
I will: - Be respectful towards staff and the school at all times - Be respectful of other parents/carers and children - Direct any complaints through official channels	
I will not: - Use social media to criticise staff or resolve behaviour issues - Upload/share images of other children without permission	
Signature	Date

Appendix 3: Acceptable Use Agreement for Students

Field	Information
Name of student:	
Student Rules	
Use only for educational purposes with teacher permission	
Do not access inappropriate websites or social media	
No use of chat rooms	
Check with teacher before opening links/attachments	
Use appropriate language online	
Never share inappropriate images	
Keep passwords private	



No online bullying	
Report upsetting material to staff	
Use ICT responsibly – school monitors all use	
Signed (student)	Date
Signed (parent/carer)	Date

Appendix 4: Acceptable Use Agreement for Staff, Governors, Volunteers and Visitors

Name of staff member/governor/volunteer/visitor:	
Staff Agreement	
Do not access or share inappropriate material	
Avoid harming school reputation	
No access to social media/chat rooms	
Use proper language online	
Do not install unauthorised software	
Do not share passwords or misuse login details	
Respect confidentiality and data protection	
Report safeguarding issues to DSL/ICT Manager	
Use systems responsibly	
Signature	Date

Appendix 5: Glossary of Cyber Security Terminology

Term	Definition
Antivirus	Software designed to detect, stop and remove malicious software.
Breach	When data/systems are accessed in an unauthorised way.
Cloud	Internet-based data storage and access.



Cyber attack	Attempt to damage or disrupt systems maliciously.
Cyber incident	Security breach of systems or services.
Cyber security	Protection of devices, services, and networks from damage.
Download attack	Unintentional download of malware.
Firewall	Constrains network traffic to prevent unauthorised access.
Hacker	Someone who breaks into systems.
Malware	Malicious software, including viruses and trojans.
Patching	Updating software to improve security.
Pentest	Authorised test to find security weaknesses.
Pharming	Redirects users to illegitimate websites.
Phishing	Mass emails asking for sensitive information.
Ransomware	Blocks access to data until payment is made.
Social engineering	Manipulating people into giving information.
Spear-phishing	Targeted phishing pretending to be a known contact.
Trojan	Malware disguised as legitimate software.
Two-factor authentication	Uses 2+ components to verify identity.
Virus	Replicating program that infects software.
VPN	Encrypted network for secure remote connection.
Whaling	Targeted phishing at senior staff.

Appendix 6: Key School Applications

Application	Use	Security Measures
Microsoft Office 365	Email and File Storage	Password protected; staff accounts use MFA
ISAMS	School Management System	Staff access based on role permissions
EVOLVE	Trip planning and consent	Controlled access; finance team have elevated rights
Inventry (BS Only)	Staff and visitor sign-in	Managed by 3 staff members



Sophos	Antivirus for Windows devices	Admin rights limited to IT team
CPOMS	Safeguarding/wellbeing monitoring	Safeguarding team have enhanced access