ICT and Internet Acceptable Use Policy

Reviewed By	Version	Date	Shared with
Governing Body	1.0	01.2025	All staff
Governing Body	2.0	04.2026	All staff

Contents

Introduction and aims

Information and communications technology (ICT) underpins teaching, learning, administration and safeguarding. This policy sets clear rules for safe, lawful and effective use of ICT, the internet and digital devices; defines responsibilities; and supports the school's Child Protection, Online Safety, Behaviour, Data Protection and Staff Code of Conduct policies.

This policy aims to:

- Keep pupils and staff safe online, including managing risks from misinformation, disinformation and conspiracy theories.
- Set expectations for acceptable use of the internet, email, AI tools, mobile phones and smart devices.
- Meet DfE filtering and monitoring standards and ensure proportionate monitoring of school systems.
- Protect personal data and maintain cyber resilience.

Scope

This policy covers all ICT facilities, systems, services and devices used on site or remotely for school business, whether school-owned or, where authorised, personally owned. Breaches of this policy may be dealt with under our disciplinary policy and staff code of conduct.

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 2025
- 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 (update March 2024)
- 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 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, pupils, 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
- **Smart device**: any device capable of messaging/notifications, audio/video capture or internet access (e.g., smart watches).

See appendix 5 for a glossary of cyber security terminology.

Roles and responsibilities

- Governing board: ensures compliance with DfE filtering/monitoring standards; receives regular assurance reports.
- Headteacher/DSL: leads online-safety culture; ensures systems, training, incident response and escalation are in place.
- ICT Manager/SBM: maintains secure systems, filtering/monitoring (e.g., Senso), access controls, backups and updates.
- All staff: follow this policy and report concerns promptly; model safe, responsible online behaviour.

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.
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 or sending illegal, harmful or inappropriate content; bullying or harassment; extremist or discriminatory content.
- 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 without authority; infringing copyright; introducing malware or interfering with security controls.
- 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 any other relevant member of staff 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

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour/discipline/staff discipline/staff code of conduct/etc.

Staff (including governors, volunteers, and contractors)

Access to school ICT facilities and materials

The school's ICT manager and/or school business manager (SBM). manages 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's ICT manager and/or school business manager (SBM).

Use of phones and email

All staff are provided with a school email address for work use only. Multi-factor authentication must be enabled.

All work communication must be sent from the school email account. Personal email addresses must not be shared with parents/carers or pupils, nor used for any work-related communication.

Staff must ensure emails are professional, accurate and appropriate. Improper or careless wording can lead to claims such as discrimination, harassment, defamation or breach of confidentiality/contract.

Emails may need to be disclosed in legal proceedings or under the Data Protection Act 2018. Deleting an email does not guarantee it cannot be retrieved.

Extra care must be taken when sending sensitive or confidential information. Attachments containing such information must be encrypted and sent only to the intended recipient.

If an email is received in error, staff must inform the sender and delete it. Sensitive information must not be used or shared.

If an email containing someone's personal information is sent in error, staff must inform the ICT manager and/or SBM immediately and follow the data breach procedure.
Staff must not share personal phone numbers with parents/carers or pupils. All work calls must be made using school-issued phones.
School phones are for work purposes only. Staff with school-issued mobile phones must follow all ICT acceptable use rules.
Any non-standard recording of phone conversations requires prior approval and consent from all parties.

Personal use

Staff may use school ICT facilities for occasional personal use, but this must be reasonable. Permission may be withdrawn at any time by the ICT manager or SBM.
Personal use is allowed only when:

- It is outside teaching/contact time and break-free periods.
- No pupils are present.
- It does not interfere with work duties or stop others from using the equipment.
- It does not involve any form of *unacceptable use*.

Staff must not store personal files (e.g., photos, videos, music) on school ICT systems.
Personal use will still fall under the school's ICT monitoring. Breaches may lead to disciplinary action.
Staff may use personal devices (e.g., phones, tablets) in accordance with the school's safeguarding policy.
Personal ICT use outside school may still affect employment if it makes personal information public or visible to pupils or parents/carers.
Staff must follow the school's social media and email guidelines (see Appendix 1) to protect themselves and maintain 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.
The school has guidelines for staff on appropriate security settings for social media accounts (see appendix 1).

Staff use of mobile phones and smart watches

- Personal devices should be silenced and out of sight during contact time; no personal calls/messages in the presence of pupils except in emergencies.
- Images/video of pupils must not be taken on personal devices.

Remote access

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

- Our OneDrive is managed by the school's ICT manager and/or school business manager (SBM).
- Monitoring remains in place

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 school's ICT manager and/or school business manager (SBM) 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 help keep pupils and staff safe, the school has the right to filter and monitor all use of its ICT network and devices.
We use Senso, a comprehensive filtering and monitoring system that helps ensure school technology is used safely and responsibly. Senso allows staff to oversee and manage all school-owned devices used by both adults and children, helping us maintain a secure online environment.
Senso's AI-driven visual threat analysis, known as *Safeguard Cloud*, continuously monitors activity on school devices. It provides real-time alerts and reports about potential safeguarding concerns, ensuring that inappropriate or unsafe content is both filtered and flagged quickly. This helps the school identify risks early and respond appropriately. This system supports schools in meeting online safety requirements while promoting a safe digital learning space.
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. We use SENSO to monitor.
- 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 board 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.

Pupils

Access to ICT facilities

- Use the internet/devices for learning with staff permission and supervision; keep passwords private.
- Never try to bypass filtering/monitoring; do not use VPNs or anonymising tools.
- Only use AI tools when a teacher says it is appropriate, and never to deceive or submit unacknowledged work.

- Report anything upsetting or unsafe to an adult immediately.

Education, curriculum and attendance link

Online safety is taught through computing/PSHE and integrated across the curriculum, including recognising misinformation, disinformation and managing online conduct and contact.

Mobile phones, smart watches and wearable technology (pupils)

To provide a calm, safe environment and reduce safeguarding risks, the school operates a phone- and smart-device-free environment by default.

- Pupils must not wear or use smart watches or smart devices in school. Non-connected time/fitness watches may be worn.
- If a phone or smart device is brought to school, it must be handed in on arrival and collected at the end of the day.
- Devices must not be used to take photos, videos or record audio on school premises.

Search and deletion

Under the Education Act 2011, the headteacher – and any staff authorised by them – may search pupils and confiscate mobile phones, computers or other devices if they have reasonable grounds to suspect the device:

- Poses a risk to staff or pupils
- Is a banned item under school rules
- Contains evidence of an offence

Examples include (but are not limited to):

- Pornographic material
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (e.g., threats of violence)

Before a Search

If an authorised staff member believes a search is justified, they will:

1. Assess how urgent the situation is and consider risks to pupils and staff.
- If not urgent, they will seek advice from the Headteacher or DSL.

2. Explain to the pupil:
- Why they are being searched
- How and where the search will happen
- Allow them to ask questions

3. Seek the pupil's co-operation.

After / During a Search

Authorised staff must:

- Inform the DSL (or deputy) of any search where a banned item was suspected.
- Involve the DSL immediately if the search reveals a safeguarding concern.

Examining or Deleting Data on Devices

Staff may examine – and in exceptional cases erase – data or files if they believe there is a good reason, such as reasonably suspecting the data:

- Has been or could be used to cause harm
- Undermines the school's safe environment or disrupts teaching
- Is linked to an offence

If inappropriate material is found:

- The Headteacher/DSL will decide the appropriate response.
- If staff believe someone may be at risk, a safeguarding response will be considered first.

Staff must not delete material if it could be evidence of an offence.
In these cases, the device must be handed to the police as soon as possible.
If the material is not suspected to be evidence of an offence, staff may delete it if:

- Keeping it is likely to cause harm, and/or
- The pupil/parent refuses to delete it themselves

If Staff Suspect a Device Contains an Indecent Image of a Child

Staff must not:

- View the image
- Copy, print, share, store or save it

They must:

- Confiscate the device
- Report immediately to the DSL (or deputy)
- Allow the DSL to decide next steps in line with:
- DfE guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes

Compliance With Guidance and Policies

All searching of pupils will follow:

- DfE guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes
- The school's behaviour policy

Any complaints about searching or deleting content on a pupil's device will be handled through the school complaints procedure.

Unacceptable use of ICT and the internet outside of school

The school may take action, in line with the behaviour policy, if a pupil engages in any of the following – at any time, even when not on school premises:

- Breaching copyright or intellectual property rights using ICT or the internet
- Using ICT or online platforms to bully, harass or promote unlawful discrimination
- Breaking any of the school's policies or procedures
- Taking part in illegal activity, or making statements that support illegal actions
- Accessing, creating, storing, linking to or sending pornographic, offensive, obscene or otherwise inappropriate material
- Sharing nude or semi-nude images or videos, whether consensual or not (sometimes referred to as "sexting" or youth-produced sexual imagery)
- Posting or sharing anything that disparages the school or could bring the school into disrepute
- Sharing confidential information about the school, pupils, staff or the wider school community
- Attempting to access restricted parts of the network or password-protected information without permission
- Encouraging or enabling others to gain unauthorised access to the school's ICT systems
- Deliberately damaging ICT equipment, devices or digital materials
- Causing a data breach by accessing, modifying or sharing data (including personal data) without authorisation

- Using inappropriate or offensive language online

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 volunteer or as a member of the PTA) 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 pupils, and help them learn, how to communicate respectfully with, and about, others online.

Communicating with parents/carers about pupils' activities

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 we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.
In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.
Parents/carers 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, pupils, 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.
The ICT Manager or SBM will generate passwords for pupils using a generator and keep these in a secure location in case pupils lose or forget their passwords.
All school-provided passwords must be reset by staff to ensure they remain secure and comply with best practices for data protection. Staff and pupils are responsible for maintaining the confidentiality of their passwords at all times.
Members of staff or pupils 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 ICT Manager and/or School Business 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 ICT Manager and/or School Business 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 and/or School Business Manager.

Protection from cyber attacks

Please see the glossary (appendix 5) to help you understand cyber security terminology.
The school will:

- Work with governors and the IT lead to 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 will verify this using a third-party audit (such as 360 degree safe), 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 and store these backups.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to the ICT Manager and/or School Business Manager
- 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
- 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
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident.
- Maintained schools: Work with our LA to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

Internet access

The school's wireless internet connection is secure.

- We use filtering a monitoring (SENSO)
- Schools WiFi is not available to staffs' own devices

Pupils

- Schools WiFi is not available to pupils' own devices.
- School devices are all on our WiFi

Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- 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

Implementation is monitored by the Headteacher/DSL and ICT Manager/SBM. The governing board reviews this policy annually, or sooner if national guidance changes, and receives an annual filtering/monitoring assurance report.

Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection

Appendix 1: What we expect to see for staff

Do not accept friend requests from pupils on social media

- **Protect your identity**
  Use a variation of your name (e.g., first and middle name, maiden name, or reversed surname) to make your profile less identifiable.
- **Use a professional or neutral profile picture**
  Choose an image that does not identify you clearly, or ensure it is appropriate and professional.
- **Check your privacy settings regularly**
  Make sure only trusted contacts can see your posts, photos, and personal information.
- **Be cautious when tagging colleagues**
  Always consider their privacy and professionalism before tagging staff members in posts or photos.
- **Think before you post**
  Never share anything publicly that you wouldn't be comfortable showing your pupils or the wider school community.
- **Avoid using social media during school hours**
  Keep personal online activity to your own time, not during the working day.
- **Do not comment about school matters online**
  Avoid posting anything about your job, colleagues, pupils or the school—once shared, it can't be taken back.
- **Do not link your profile to the school**
  Avoid listing the school as your workplace or "checking in" at school events.
- **Keep work and personal accounts separate**
  Don't connect your work email to social media platforms. Anyone with your email or phone number can find your profile.
- **Consider removing social media apps from your phone**
  Apps can use shared WiFi networks to suggest connections—this may include parents or pupils.

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils 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 pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil 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/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
- Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer 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 pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should 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, you or a senior leader should consider contacting the police

Appendix 2: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: EYFS & KS1 AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use school computers or go on the internet, I will:
 	
• Ask a teacher or adult before I start
• Only use websites my teacher/adult says I can use
• Tell my teacher straight away if:
  ○ I click on the wrong website
  ○ Someone I don't know sends me a message
  ○ I see anything that upsets or worries me
• Use school computers for school work only
• Be kind online and never be rude or unkind
• Look after the computers and tell an adult if something is broken
• Only use my own username and password
• Keep my password private
• Never give out my personal information (like my name, address or phone number) without a teacher or parent/carer saying I can
• Save my work on the school network
• Ask my teacher before printing
• Log off or shut down when I finish
 	
Phones, Smart Watches and Wearable Technology
 	
• I will not bring or use smart watches or smart devices in school
(I may wear a simple time-only/fitness watch that is not connected to the internet).
• If I bring a phone or smart device to school, I will hand it in when I arrive and collect it at the end of the day.
• I will never use a device to take photos, videos or record audio on school premises.
 	
Keeping Me Safe Online
 	
I know the school uses filtering and monitoring systems to help keep me safe when I use school devices.
I will always tell a teacher or trusted adult if I see anything online that upsets me or is unkind or wrong.
I understand I must use the school's ICT systems and internet responsibly, and that the behaviour policy may be used if I behave inappropriately online—even if it happens outside school.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: KS2 AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems or the internet, I will:
• Use them sensibly and responsibly, and only for schoolwork
• Only use them with a teacher's permission
• Keep my username and password private
• Keep my personal information (name, address, phone number) safe
• Tell a teacher straight away if:
  ○ I open the wrong website
  ○ I get a message from someone I don't know
  ○ I see anything upsetting, worrying, or inappropriate
• Look after school equipment and report any problems
• Log off or shut down when I am finished
I will not:
• Visit websites that are inappropriate, including social media, chat rooms or gaming sites (unless a teacher has allowed them for learning)
• Open email links or attachments without checking with a teacher
• Use rude or inappropriate language online
• Create or share material that is offensive or inappropriate
• Use someone else's login details
• Arrange to meet anyone offline without my parent/carer and a trusted adult knowing
Mobile Phones, Smart Watches and Wearable Technology
To help keep school calm and safe:
• I must not use or wear smart watches or smart devices in school
(Only simple time-only/fitness watches that are not connected are allowed.)
• If I bring a phone or smart device to school, I will hand it in when I arrive and collect it at home time
• I will not take photos, videos or audio recordings on school premises
Keeping Me Safe Online
• I know the school uses filtering and monitoring systems to help keep me safe
• I will tell a teacher or trusted adult immediately if I see anything online that is unkind, upsetting or wrong
• I understand I must use technology responsibly, and the behaviour policy may still apply if I behave inappropriately online—even outside school	

Signed (pupil):	**Date:**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: KS2 AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems or the internet (in school or on a work device), I will not: • Access or attempt to access inappropriate material, including anything violent, criminal or pornographic • Use devices in a way that could damage the school's reputation • Access social networking sites or chat rooms on school devices • Use improper or inappropriate language online, including in emails or messaging • Install unauthorised software or connect unauthorised devices to the school network • Share my password, or use anyone else's login • Take photos of pupils without approval from parents and Senior Leaders • Share confidential information about pupils, staff, or the school community • Access, change or share any data I am not authorised to use • Promote private businesses, unless directly linked to school work • Access personal music/film streaming accounts on school devices My responsibilities • I will only use the school's ICT systems and internet for educational purposes, my professional role, or as set out in the Acceptable Use Policy. • I understand the school uses Senso monitoring to track use of ICT systems and websites. • I will keep work devices secure and password-protected, especially when used off-site. • I will store and handle all information in line with the school's data protection policy. • I will inform the DSL and ICT manager immediately if a pupil reports harmful content or if I encounter anything unsafe or inappropriate myself. • I will ensure that pupils in my care use ICT safely and responsibly.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 5: 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.

TERM	DEFINITION
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.
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.