ACCEPTABLE USE OF ICT POLICY

Date of approval by the Trust Board	**15 October 2025**
Review cycle	**Two years**

Introduction

ICT is an integral part of the way our Trust and schools work, and is a critical resource for pupils, staff, Trustees, Governors, volunteers (where applicable) and visitors. It supports teaching and learning, pastoral and administrative functions of the trust and schools.

However, the ICT resources and facilities our schools use also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of all Trust ICT resources for staff, pupils, parents, Trustees and Governors.
- Establish clear expectations for the way all members of the school community engage with each other online.
- Support the Trust and schools' policy on data protection, online safety, and safeguarding.
- Prevent disruption to the schools through the misuse, or attempted misuse, of ICT systems.
- Support the schools in teaching pupils safe and effective internet and ICT use.

This policy covers all users of all Trust ICT facilities, including Trustees, Governors, staff, pupils, volunteers, contractors, and visitors.

Breaches of this policy may be dealt with under our school's behaviour policies or the Trust Disciplinary Policy and 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

In applying this policy, the Trust will not unlawfully discriminate in respect of any of the protected

characteristics as defined under the Equality Act and specified below:

- Age.
- Disability.
- Gender reassignment.
- Pregnancy and Maternity.
- Race.
- Religion or Belief.
- Sex.
- Sexual Orientation.
- Marriage and civil partnership.

Head Teachers/Heads of School, will monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

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

- Safeguarding and Child Protection.
- Behaviour.
- Staff Code of Conduct.
- Data Protection.

Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of trust/school policy may result in disciplinary or behaviour proceedings (see section below).

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.
- Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, its pupils, 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 program, tool or item of software designed to interfere with the functioning of the 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 ICT facilities.
- Removing, deleting, or disposing of ICT equipment, systems, programs, or information without permission by authorised personnel.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed 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 mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

Using AI tools and generative chatbots (such as ChatGPT and Google Bard):

- During assessments, including internal and external assessments, and coursework
- To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

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

Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Head Teacher'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 and/or discipline. Copies of these policies may be found on the school website and at https://alternativelearningtrust.org.uk as appropriate.

Sanctions for unacceptable ICT use may include revoking permission to use the school's systems.

Staff (including Trustees, Governors, volunteers and contractors)

Access to school ICT facilities and materials

The school's ICT provider (each school currently has its own individual IT provider) manages access to the trust and school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobiles and any other devices.
- Access permissions for certain programs or files.

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

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Head Teacher / and or ICT Network Manager.

Use of phones and email

The school provides each member of staff with an email address. All work-related business should be conducted using the email address the school has provided. This email account should be used for work purposes only. The Trust is working towards enabling multi-factor authentication on school email account(s).

Staff must not share their personal email addresses with parents and pupils 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. Any attachments containing sensitive or confidential information should be encrypted 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 which contains the personal information of another person, they must inform their Head Teacher immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. 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 above.

Staff who would like to record a phone conversation should speak to the Head Teacher.

All non-standard recordings of phone conversations must be pre-approved, and consent obtained from all parties involved. For example, you may grant requests to record conversations when:

- Discussing a complaint raised by a parent/carer or member of the public.
- Calling parents to discuss behaviour or sanctions.
- Taking advice from relevant professionals regarding safeguarding, special educational needs assessments, etc.
- Discussing requests for term-time holidays.

Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Head Teacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during working time.
- Does not constitute 'unacceptable use', as defined above.
- Takes place when no pupils are present.
- Does not interfere with their jobs,or prevent other staff or pupils 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 below).

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 mobile phone/device 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 pupils and parents could see them.

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

Personal social media accounts

Members of staff should ensure that their use of social media is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook, X (Twitter), Linkedin, etc accounts (see Appendix 1).

Remote access

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

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 the Head Teacher may require from time to time 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.

School social media accounts

If your school has an official social medial account, e.g. Facebook/X (Twitter) page, staff members who have not been authorised to do so must not access, manage, or post to the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

Monitoring of school network and use of ICT facilities

Trust schools reserve the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited.
- Bandwidth usage.
- Email accounts.
- Telephone calls.
- User activity/access logs.

- Any other electronic communications.

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

Trust schools monitor ICT use 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.

Pupils

Access to ICT facilities

ICT facilities are available to pupils in school during lessons from time to time under the supervision of staff.

Remote Learning

The Trust recognises that children may be required to undertake learning off school premises from time to time. This may be due to government decisions to open schools for restricted and/or specific pupils only or due to the health requirements of an individual pupil.

Where pupils are required to access learning remotely, pupils will be required to follow the local school policy.

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, schools have the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

Trust schools can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Unacceptable use of ICT and the internet outside of school

Trust schools will sanction pupils, in line with their 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 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.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
  Sharing confidential information about the school, other pupils, 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 ICT facilities or materials.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.

Please refer to the school's Behaviour Policy for information relating to sanctions that may be given in these circumstances.

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 Head Teacher'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.

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.

We ask parents / carers to sign the agreement in Appendix 2.

Remote Learning

Where children are required to access learning remotely, pupils and parents will be required to follow the Trust's Remote Learning Policy.

Keeping Children Safe On-Line

It is important to have regular conversations about staying safe online and to encourage children to speak to you if they come across something worrying online.

Parents are encouraged to talk to their child about the importance of creating a safe online environment, including keeping any log-in details and passwords safe.

There are a range of resources available that will support you to talk to your child about a range of online safety issues, set up home filtering in a child-friendly way and set up age-appropriate parental controls on digital devices:

- Thinkuknow by the National Crime Agency - Child Exploitation and Online Protection command (NCA-CEOP) - resources for parents and carers and children of all ages to help keep children safe online.
- Childnet has developed guidance for parents and carers to begin a conversation about online safety, as well as guidance on keeping under-fives safe online .
- Parent Info is a collaboration between Parent Zone and NCA-CEOP - support and guidance for parents and carers related to the digital world from leading experts and organisations.
- National Society for the Prevention of Cruelty to Children (NSPCC) - guidance for parents and carers to help keep children safe online.
- UK Safer Internet Centre - tips and advice for parents and carers to keep children safe online - you can also report any harmful content found online through the UK Safer Internet Centre.
- Inclusive Digital Safety Hub and Online Safety Hub, created by South West Grid for Learning in partnership with Internet Matters - support and tailored advice for young people with additional learning needs and their parents or carers.
- Parents' Guide to Age Ratings explains how the British Board of Film Classification rates content, and gives parents advice on choosing online content well.

What harms might my child experience online?

Parents may have concerns about specific harms which children can experience online. There are more resources to help parents understand and protect their child from these, including:

1. child sexual abuse – a definition.
2. child criminal exploitation – a definition.
3. exposure to radicalising content.
4. youth-produced sexual imagery ('sexting').
5. cyberbullying.
6. exposure to age-inappropriate content, such as pornography.
7. exposure to harmful content, such as suicide content.

1. Child sexual abuse

If you are concerned call 999.

If your child has been a victim of child sexual abuse – online or offline – and you believe they are in immediate danger, call 999 and ask for the police. The police will continue to respond to emergency calls.

If you are concerned that your child has been a victim of online sexual abuse or you are worried about the way someone has been communicating with your child online, you can report it to NCA-CEOP.

These resources provide information and support for parents and carers on what to do if you're worried about child sexual abuse:

- you can contact the NSPCC helpline (0808 800 5000) for support and advice if you have concerns about your own or another child's safety. The Together, we can tackle child abuse campaign also provides information on the signs of child abuse and neglect.
- Thinkuknow by NCA-CEOP has developed activities to support your child's safe use of the internet.
- the Lucy Faithfull Foundation's Parents Protect website has advice on how to help prot,ct children from child sexual abuse including a Harmful Sexual Behaviour Prevention Toolkit.
- if you see sexual images or videos of someone under 18 online, report it anonymously to the Internet Watch Foundation who can work to remove them from the web and help to identify victims and survivors.
- you can contact Stop It Now! for information and advice if you have concerns about someone's behaviour, including children who may be displaying concerning sexual behaviour.
- you can contact The Marie Collins Foundation help@mariecollinsfoundation.org.uk for support, including advice and individual counselling, for your child if they have been subjected to online sexual abuse - support is also offered to parents and carers.

2. Criminal exploitation and county lines, violence and gangs

Our page of advice to parents and carers on keeping children safe from abuse and harm has information on this.

3. Radicalising content

If you are concerned that any family member, friend or loved one is being radicalised, you can call the police or 101 to get advice or make a Prevent referral, so that they can get safeguarding support.

Support is tailored to the individual and works in a similar way to safeguarding processes designed to protect people from gangs, drug abuse, and physical and sexual exploitation. Receiving support through Prevent is voluntary, confidential and not a form of criminal sanction.

If you need more help, you can also contact your local authority safeguarding team.

- Educate Against Hate Parents' Hub - resources and government advice for parents and carers on keeping young people safe from extremism, including online.
- Let's Talk About It - support for parents and carers to keep children safe from online radicalisation.
- Any member of the public can report terrorist content they find online through the GOV.UK referral tool - more information about what to report and what happens when you do can be found on the Action Counters Terrorism campaign.

4. 'Sexting' (youth-produced sexual imagery)

If you are worried about your child sending nude images or videos (sometimes referred to as 'youth- produced sexual imagery' or sexting), NSPCC provides advice to help you understand the risks and support your child.

If your child has shared nude images, Thinkuknow by NCA-CEOP provides advice on talking to your child and where to get help.

So You Got Naked Online created by South West Grid for Learning, has advice for young people and parents affected by sexting, also available in a SEND (Special Educational Need and Disability) version.

5. Cyberbullying

If you are concerned about cyberbullying, you can find government advice and information about how you can protect your child and tackle it if it happens.

6. Age-inappropriate content and parental controls

If you have downloaded new apps or bought new technology to help stay connected at this time, remember to review and adjust privacy and safety settings if you or your child is signing up to a new online service.

- Internet Matters has step-by-step guides on how to set up parental controls so that you can control what content your child can access online.
- the UK Safer Internet Centre has guidance on how to switch on family-friendly filters to prevent age-inappropriate content being accessed on devices in your home.
- the NSPCC has more information for parents or carers with concerns about their child seeking inappropriate or explicit content online.

Apps to help children stay safe online

The BBC has a website and app called Own It. The website helps children navigate their online lives, and the free smartphone app comes with a special keyboard which can intervene with help and support in the moments that children need it the most. It can be downloaded for free in the Google Play Store and Apple App Store.

SafeToNet is an app for parents to help them protect their children from online risks like cyberbullying and sexting, while respecting their child's rights to privacy. The SafeToNet Foundation is providing UK families with free-for-life access to SafeToNet during the coronavirus (COVID-19) outbreak.

Mental health

If you are worried about your child's mental health, the government has published guidance for parents and carers on supporting children and young people's mental health and wellbeing during the coronavirus outbreak.

If you are worried that someone you know is suicidal, including your child, Samaritans provides advice on how you can support others.

Support for children

If your child is worried or needs support, they can get advice and support from Childline (0800 1111) or download the 'For Me' app.

If you need help to support your child's mental wellbeing, this list of online education resources for home education includes mental wellbeing resources on how to support the wellbeing of children and young people

Data security

Trust schools take steps to protect the security of its computing resources, data and user accounts. However, schools cannot guarantee security. Staff, pupils, parents and others who use school ICT facilities should use safe computing practices at all times.

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 where appropriate, for setting permissions for accounts and files they control.

Where there has been a password breach, passwords must be changed immediately and the incident must be reported to the Head Teacher immediately. Members of staff or pupils who deliberately disclose account or password information may face disciplinary action. Parents 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 antivirus products will 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 Head Teacher.

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 Head Teacher 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 closed down completely at the end of each working day.

Encryption

The school ensures that its devices and systems have an appropriate level of encryption. School staff may only use personal devices (including computers) which are encrypted to access school data or work remotely., If USB drives are used, they must be encrypted and only used with an encrypted laptops. No personal data (such as pupil information) should be taken out of school.

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

Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.
The school will:

- Work with governors and the IT department 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 Secure Schools annually], 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 happens overnight automatically. Backup is stored in a cloud based setup
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to [our cloud-based provider/our IT department (if you use an on-premises provider)]
- Make sure staff:
- Dial into our network using a virtual private network (VPN) when working from home
- Enable multi-factor authentication where they can,especially in high-risk areas such as Payroll, HR & IT where this is a requirement by the external service provider.
- Make sure ICT staff conduct annual access reviews as a minimum 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
- Conduct vendor assessment 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.

The Trust working towards achieving Cyber Essential School certification for each of the schools. Presently the Trust supports schools with cyber security using third party providers such as Secure School.

Internet access

The school wireless or LAN internet connection is secured.

However, web filters are not fool proof. You must report inappropriate sites that the filter has not identified (or appropriate sites that have been filtered in error) to the Head Teacher/ IT Support.

Pupils

Pupils may not use school Wi-Fi.

Parents / carers and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the Head Teacher.

The Head Teacher 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 the PTA).
- Visitors need to access the school's Wi-Fi 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 Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

Further Information

If you would like any further regarding this policy and procedure, please contact Trust HR at hr@alternativelearningtrust.org or Tel: 0208 652 1157.

Person/s responsible for updating this policy

ICT Manager with the Deputy CEO/Director of School Improvement

Appendix 1 Facebook, X (Twitter), Linkedin, etc cheat sheet for staff

Do not accept friend requests from pupils on social media

10 rules for school staff on Facebook, X (Twitter), Linkedin, etc

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead.
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional.
3. Check your privacy settings regularly.
4. Be careful about tagging other staff members in images or posts.
5. Do not share anything publicly that you wouldn't be just as happy showing your pupils.
6. Do not use social media sites during school hours.
7. Do not make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there.
8. Do not associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event).
9. Do not 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.
10. Consider uninstalling the Facebook, X (Twitter), Linkedin, etc 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 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 have shared and look at your pictures if they are friends with anybody on your contacts list.
- Do not 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 have **'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 do to 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 will have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages.
- Notify the Head Teacher about what is 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.
  - Pupils 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, consider drafting a standard response to let the parent know that you are doing so and notify the Head Teacher.

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 e.g. X (Twitter), Linkedin 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 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 should consider contacting the police.
- Notify the Head Teacher about what is happening.

Appendix 2 Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of student:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Email/text groups for parents (for school announcements and information) • Our virtual learning platform Parents/carers also set up independent channels to help them stay on top of what is happening in their child's class. For example, class/year Facebook, X (Twitter), Linkedin groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: • Use private groups, the school's Facebook, X (Twitter), Linkedin page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way • Use private groups, the school's Facebook, X (Twitter), Linkedin page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors

Adapt this agreement to reflect your school's approach, in line with any changes you made to this policy.

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote any private business, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: 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.

term	definition
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.