Unique Policy Number: 28

Acceptable Use of ICT Policy

The Children's Endeavour Trust comprises:

Abbot's Hall Community Primary School
Bosmere Community Primary School
Broke Hall Community Primary School
Chilton Community Primary School
Combs Ford Primary School
Freeman Community Primary School
Springfield Junior School
Whitehouse Community Primary School

Document Control

Version	*Date*	*Author*	*Comments*
Issue 1	July 2024	**KW**	*Updated policy*

Owner: DPO
Approver: Trust Board
Statutory Policy: Yes
Review Cycle: Annual
Approval date: 11th July 2024

Policy Contents

1. Introduction and Aims

The Children's Endeavour Trust and its schools (collectively referred as "CET" or "Trust") is committed to protecting the rights and freedom of all individuals in relation to the processing of their data.

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

Breaches of this policy may be dealt with the Trust Disciplinary Policy. 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

Headteachers will monitor the implementation of this policy, including ensuring that the Trust is notified if changed need to be made to reflect the needs and circumstances of their school.

2. Legislation and guidance

This policy meets the requirements of:

- 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
- Data Protection Act 2018 (DPA 2018)
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications Regulations 2000
- Education Act 2011
- Freedom of information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- National Cyber Security Centre (NCSC): Cyber Security for Schools

3. Unacceptable Use

The following is considered unacceptable use of the school's and Trusts ICT facilities by any member of CET. Any breach of this policy may result in disciplinary or behaviour proceedings (see section below). Unacceptable use of the school's ICT facilities includes:

- Using the school's or Trust's ICT facilities to breach intellectual property rights or copyright.
- Using the school's or Trust's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's or Trust'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 or harmful.
- Activity which defames or disparages the school's or Trust, or risks bringing CET into disrepute.
- Sharing confidential information about the school, its pupils, or other members of CET.
- Connecting any device to the school's or Trust's ICT network without approval from authorised personnel.
- Setting up any software, applications, or web services on the school's or Trust'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 or Trust'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 or Trust's filtering mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way.
- Online gambling, inappropriate advertising, phishing and/or financial scams

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

3.1 Exceptions from unacceptable use

Where the use of school or Trust ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted by the school's Head Teacher or CEO's discretion.

3.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the Trust's Disciplinary Procedure/Behaviour Policy.

The Disciplinary Procedure is available on the Trust Website:

The Behaviour Policy is available on the individual school websites.

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

4. Staff (including Trustees, Governors, volunteers and contractors)

4.1 Access to school ICT facilities and materials

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

- Computers, laptops, Chromebook, tablets, iPads, mobiles and any other devices.
- Access permissions for certain programmes 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, Office manager and or ICT staff/provider.

4.2 Use of phones and email

The schools provide each member of staff with an email address. The Trust provides each member of the central team with an email address.

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

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

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

Initial contact to parents should be made by a generic admin/office email rather than the staff members own work email.

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 must be either password protected, with a separate email containing information to open the protected document. Or shared on either SharePoint or Google Workspace, so that the information is only accessible by the intended recipient.

Full first and surnames of staff or pupils must not be emailed or sent, use initials along with the pupil's class. First name with the initial of the surname is excepted for staff members.

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 the staff member is unsure of what to do, they must contact their school's Data Champion for advice.

If staff send an email in error that contains the personal information of another person, they must inform their school's Data Champion immediately and follow the CET Data Breach policy.

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 in section 3.

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

If you record calls, callers must be made aware that the conversation is being recorded and the reasons for doing so. Your school's phone system probably has an automated option you can use/adapt. Explain when you record phone conversations and why. For instance:

- "All calls to the school office are recorded to aid administrators"
- "Calls are recorded for use in staff training"

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, an incident, suspensions or exclusions.
- Taking advice from relevant professionals regarding safeguarding, special educational needs assessments, etc.
- Discussing requests for term-time holidays.

4.3 Personal use

Staff are permitted to occasionally use the Trust 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 or CEO 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 or Trust 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 or Trust ICT facilities for personal use may put personal communications within the scope of the Trust's ICT monitoring activities (see section below).

Where breaches of this policy are found, disciplinary action may be taken.

Staff may not connect their own personal devices, such as phones or smart watches to the school's or Trust WIFI.

Staff must not use their personal devices such as phones or smart watches to take photos or videos.

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 Trust guidelines on social media (see Appendix 1) and use of email, set in section 4.2. To protect themselves online and avoid compromising their professional integrity.

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

4.5 Remote access

Some of our schools allow access to ICT facilities and materials remotely where appropriate.

Staff that access their school's or Trust 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 their school's or Trust ICT facilities outside the school and take such precautions as the Head Teacher or CEO 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.

4.6 School social media accounts

Some of our schools have official social media accounts e.g. X, staff members who have not been authorised to do so must not access, manage, or post to the account.

See appendix 1 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.

4.7 Monitoring of 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 Trust reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

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

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

The Trust monitors 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

Our Governing and Trustee board is responsible for making sure that:

- The schools and Trust meet the DfE's filtering and monitoring requirements
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
- For leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- Regularly review the effectiveness of the filtering and monitoring within the Trust.

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

Where needed, staff may raise a concern about monitored activity and log with MyConcern or Cpomms, depending with app their school uses. Then their school's DSL and ICT staff will be notified accordingly and appropriate action will be taken.

5. Pupils

5.1 Access to ICT facilities

ICT facilities and equipment are available to pupils in school during lessons or break times under the supervision of staff.

5.2 Logins

All pupils in key stage 1 and 2 have their own individual school login and password for their school's ICT equipment, such as, but not limited to:

- Computers
- Laptops
- Chromebooks
- iPads
- Tablets

Under supervision in school, pupils are also provided with individual accounts linked to websites that complement the schools' teaching and learning, which they can access in school or from home, for example Times Table Rockstars, Accelerated Reader and Spell Shed.

5.3 Remote learning

The Trust recognizes 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.

5.4 Search and deletion

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

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out. Please see each of our school's behaviour policy, and/or
- Is evidence in relation to an offence.

This includes, but is not limited to:

- Abusive messages, images or videos
- Pornography
- Evidence of suspected criminal behaviour (such as threats of violence or assault)
- Indecent images of children

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 pupils and staff. If the search is not urgent, they will seek advice from their school's headteacher or DSL
- Explain to the pupil 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 pupil's co-operation (if the pupil refuses to co-operate, you should proceed according to your school's behaviour policy)

The authorised staff member should:

- Inform the school's DSL of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item.
- Involve the school's DSL without delay if they believe that a search has revealed a safeguarding risk

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

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

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

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

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

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

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

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

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Each school's behaviour policy / searches and confiscation

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

5.5 Unacceptable use of ICT and the internet outside of school

The Trust will sanction pupils, in line with the 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 Trust'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) Using inappropriate or offensive language.
- Activity which defames or disparages the Trust, or risks bringing the Trust into disrepute
- Sharing confidential information about the Trust or it's schools, other pupils, or other members of each school's 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 Trust and school's ICT facilities
- Causing intentional damage to the Trust and school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

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

6. Parents

6.1 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, a school within the Trust in an official capacity (for instance, as a volunteer or as a member of the PFA/HSA) 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 are granted access in this way, they must abide by this policy as it applies to staff.

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

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

6.3 Communicating with parents/carers about pupil 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.

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

6.4 Keeping children safe online

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 (NCACEOP) - 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.

7. Data security

The schools and Trust are responsible for making sure the appropriate level of security protection and procedures are in place to safeguard its systems, staff and pupils. 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 schools and Trust 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
- Filtering
- Security features
- User authentication and multi-factor authentication

7.1 Passwords

All users of ICT facilities within the Trust are required to set strong passwords for their accounts, these have be at least 8 characters long containing the 3 random word technique. All users must keep their passwords secure.

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

Members of staff or 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.

Please refer to our Password Policy. (add link)

7.2 Software updates, firewalls and anti-virus software

All of the schools and Trust 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 schools and Trust ICT facilities.

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

7.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the Trust's Data Protection and Records Management Policy.

7.4 Access to facilities and materials

All users of the schools and Trust ICT facilities will have clearly defined access rights to school and Trust systems, files and devices. These access rights are managed by the schools and the Trust's central team.

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 their schools ICT staff or provider.

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. Please see our Clear and Clear Screen Policy.

7.5 Encryption

The school/Trust ensures that its devices and systems have an appropriate level of encryption, that all laptops have BitLocker enabled. 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 Head Teacher of their school.

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

8. Protection from cyber attacks

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

The Trust 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 provided by NCSC (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 using the 3-2-1 backup rule recommended by the DfE and National Cyber Security Centre
- Delegate specific responsibility for maintaining the security of our management information system (MIS)
- Make sure ICT staff conduct regular access reviews to make sure each user in within each school and the central team 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 cyber response plan with the Trust's IT development officer 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. This plan will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

9. Internet access

Each of the schools and Trust wireless internet connection is secure.

Filtering and monitoring are used in each school. However, filters aren't fool proof. You must report inappropriate sites that the filter hasn't identified (or appropriate sites that have been filtered in error) to the school's ICT staff/provider.

9.1 Pupils

Pupils can use school devices to access the school WIFI under supervision by teachers and staff members.

9.2 Parents and visitors

Parents and visitors to the schools 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 are working with the school in an official capacity (e.g. as a volunteer or as a member of the PFA/HSA).
- 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 Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. Monitoring

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed annually and shared with the CEO and Trust board.

11. Links with other policies

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

This acceptable use if ICT policy is linked to our:

- Child Protection and Safeguarding
- Behaviour
- Staff disciplinary Procedure
- Data protection
- Clear Screen and Clear Desk

Appendix 1: Facebook and social media cheat sheet for staff

Do not accept friend requests from pupils on social media

10 rules for school staff on Facebook, X, 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 you don't, make sure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. 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)
9. 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
10. 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 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 Facebook help centre 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 Facebook help centre 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

- the first instance, ignore and delete the request. Block the pupil from viewing your profile In
- 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 your 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: 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 pupil:

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Arbor app
- Email and Text groups for parents (for school announcements and information)
- Tapestry

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook 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, 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 unless they are raised in an appropriate way
- Use private groups, 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 the other children's parents/carers

Signed:	**Date:**

Print name:

Appendix 3: Acceptable use agreement for pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me)
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Share my password with others or log in using someone else's name or password
- Bully other people
- Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me, and then submit if as my own work.
- Use my phone or smart watch during school hours

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**
Print Name (pupil):	
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 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 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
- Use my mobile phone or smart watch when in class with pupils

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 staff/provider 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:**

Print name (staff member/governor/volunteer/visitor):

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.
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.