ICT and Internet Acceptable Use Policy 2023

Cotswold Beacon Academy Trust

Berkeley Primary School
Callowell Primary School
Cam Woodfield Junior School
Marling School

Version Control

Date	Version	Amendments/Comments	Reviewer/s
September 2023	**1.0**		**ELG**

1. Introduction and aims

This policy aims to:

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

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

2. 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 2022
- 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
- UKCIS 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

3. Definitions

- **ICT facilities:** all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets including Chromebooks, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the Trust's ICT service
- **Users:** anyone authorised 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 Trust to perform systems administration and/or monitoring of the ICT facilities

- **Materials:** files and data created using the Trust's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

4. Unacceptable use

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

Unacceptable use of the Trust's ICT facilities includes:

- Using the ICT facilities to breach intellectual property rights or copyright
- Using the ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Trust or School's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the Trust, any Trust School, its pupils, or other members of the school community
- Connecting any device to the Trust's ICT network without approval from the IT Services Team
- Setting up any software, applications or web services on the Trust's network without approval by the IT Services Team, or creating or using any programme, tool or item of software designed to interfere with the functioning of the Trust'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 Trust's ICT facilities
- Causing intentional damage to the Trust's ICT facilities
- Removing, deleting or disposing of the Trust'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 Trust'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 Trust reserves the right to amend this list at any time. The CEO and Headteacher, with support from the IT Services Team will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Trust School's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of Trust 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 CEOs discretion.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the Trust's policies on Behaviour, Disciplinary, and Code of Conduct for All Adults.

Failure to comply with this policy may lead to the Trust taking any one or more of the following actions:

All Users

- Any illegal activity will be reported to the police.

Staff

- The issue of a verbal warning.
- The issue of a written warning.
- The suspension of a user's account.

Or in serious cases:

- The termination of a user's account.
- The commencement of formal disciplinary proceedings.
- Taking legal action.

Students

- Inappropriate use of the Internet may result in restriction of some or all internet or IT access.
- All other sanctions will be in line with the Behaviour Policy.
- Serious offences will be reported to the Senior Leadership Team and may result in a fixed term or permanent exclusion.

Visitors

- Devices will be blocked from connectivity and accounts deactivated.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to Trust ICT facilities and materials

The Trust IT Services Team manages access to the Trust's ICT facilities and materials for all 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 Trust'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 IT Services Team.

5.1.1 Use of phones and email

The Trust provides each member of staff with an email address.

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

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

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 that contains the personal information of another person, they must inform the Trust Data Protection Officer (DPO@CBAT.academy) immediately and follow the data breach procedure.

Staff should seek approval from their Headteacher to use their personal mobile to conduct work-related business. Staff must not give their personal phone number(s) to parents or pupils.

School phones are available to conduct work-related business such as trips. School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

The Trust can record incoming and outgoing phone conversations in schools but this does not happen automatically.

Staff who would like to record a phone conversation should speak to their Headteacher.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved with a clear rationale for the purpose of making a recording.

5.2 Personal use

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

Personal use is permitted provided that such use:

- Does not take place during the school day (8.30 – 3.30) except during break and lunchtime.
- Does not constitute 'unacceptable use', as defined in section 4
- 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 Trust'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 Trust's ICT facilities for personal use may put personal communications within the scope of the Trust's ICT monitoring activities. 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 this Policy.

Staff should be aware that personal use of ICT (even when not using Trust 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's guidelines on use of social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts.

5.3 Remote access

Staff accessing the Trust'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 ICT facilities

outside the school and take such precautions as the IT Services Team may require against importing viruses or compromising system security.

Trust 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 the data protection policy.

5.4 School social media accounts

Trust schools have official social media accounts, managed by the Headteachers. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

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

Students should, under no circumstances be given administrative rights to any school's social media accounts.

5.5 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the 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

Only the IT Services Team may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

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

Where appropriate, authorised personnel may raise concerns about monitored activity with a School's designated safeguarding lead (DSL) and IT Services Team, as appropriate.

The Trust monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with policies, procedures and standards
- Ensure effective Trust and School 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

The Trust Board will regularly review the effectiveness of the school's monitoring and filtering systems.

6. Pupils

6.1 Access to ICT facilities

Computers and equipment in the Trust's ICT suites are available to pupils only under the supervision of staff. Specialist ICT equipment, such as that used for Music, Art and Design Technology must only be used under the supervision of staff. Sixth Formers may use computers and equipment independently in the study rooms for educational purposes only and in line with this Policy.

6.2 Search and deletion

Under the Education Act 2011, the CEO, Headteacher, and any member of staff authorised to do so by a 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
- Is evidence in relation to an offence

This includes, but is not limited to:

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

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the 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 (following the Behaviour Policy if this is refused)

The authorised staff member should:

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

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

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

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

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

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

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

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

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and

confiscation and the UK Council for Internet Safety (UKCIS) 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 guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The Behaviour Policy which reflects the updated DfE guidance, which came into force on 1st September 2022.

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

6.3 Unacceptable use of ICT and the internet outside of school

Pupils will be sanctioned, in line with the Behaviour Policy and Section 4.2 of this Policy, if a pupil engages in any of the following **at any time** (even if they are not on Trust 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 or School's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the Trust or School, or risks bringing the Trust or School into disrepute
- Sharing confidential information about the Trust or School, other pupils, or other members of the Trust 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's ICT facilities
- Causing intentional damage to the Trust'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

7. Parents

7.1 Access to ICT facilities and materials

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

However, parents working for, or with, the Trust 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 a school's facilities at the headteacher's discretion.

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

7.2 Communicating with or about the school online

Trustees 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 a school through its website and social media channels.

7.3 Communicating with parents about pupil activity

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

When pupils are asked to use websites or engage in online activity, the details of thiswill be communicated to parents in the same way that information about homework tasks are shared.

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

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

8. Data security

The Trust 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 and others who use the ICT facilities should use safe computing practices at all times. The Trust aims 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

8.1 Passwords

All users of the ICT facilities should set strong passwords for their accounts and keep these passwords secure. The strongest passwords are built using three unconnected words and including a number.

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.

All staff will store their passwords securely and seek support from the IT Services Team if they have any concerns or queries. Where Teachers need to generate passwords for pupils, they will keep these securely in case pupils lose or forget their passwords.

8.2 Software updates, firewalls and anti-virus software

All of the 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 ICT facilities.

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

8.3 Data protection

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

8.4 Access to facilities and materials

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

These access rights are managed by the IT Services 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 the IT Services Team 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.

8.5 Encryption

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

Staff may only use personal devices (including computers and USB drives) to access 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 IT Services Team.

9. Protection from cyber attacks

The Trust will:

- Work with governors and the IT Services Team to make sure cyber security is given the time and resources it needs to make the Trust schools 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 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 Trust will verify this using a third-party audit to objectively test that what it has in place is effective
    - **Multi-layered**: everyone will be clear on what to look out for to keep systems safe
    - **Up to date:** with a system in place to monitor when the Trust 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 on cloud based systems.
- Delegate specific responsibility for maintaining the security of the management information system (MIS) to the IT Services Team
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the Trust 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 Services Team including, for example, how the Trustschool 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'
- Work with external agencies regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

The Trust's wireless internet connection is secure and filtered. If any member of staff identifies an inappropriate site which has not been picked up on the filter, this should be reported immediately to the IT Services Team.

10.1 Pupils

WiFi is available for pupils to use throughout Trust school sites. Pupils should request access from Teaching Staff or the IT Services Team if they are having problems accessing the WiFi.

10.2 Parents and visitors

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

The headteacher will only grant authorisation if:

- Parents are working with a 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.

11. Monitoring and review

The Chief Finance and Operations Officer, Headteachers, and IT Services Team monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the Trust.

This policy will be reviewed at least every two years or after any change in legislation.

12. Related policies

This policy should be read alongside the Trust and School policies on:

• Behaviour Policy	• Contingency Curriculum Policy
• Code of Conduct for All Adults	• General Complaints Policy
• Anti-bullying Policy	• Safeguarding Policy
• Data Protection Policy	• Whistleblowing Policy
• E-Safety Policy	• Disciplinary Policy