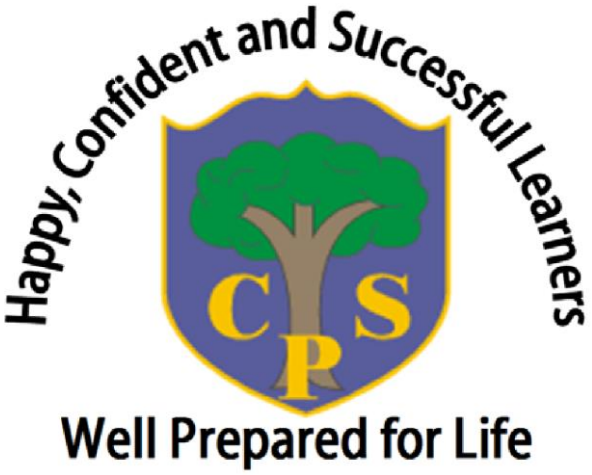

The Coppice Primary School

Staff (and Volunteer) ICT Acceptable Use Policy and Agreement

Written by	Val Juneman / William Hutt
Approved by Trustees	May 2022
Date for Review	May 2023

Contents

1. Introduction and aims

1.1. Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

1.1. However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

1.2. This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Ensure that all users of internet and digital technologies in school are responsible and stay safe whilst using them for educational, personal and recreational use.
- Protect pupils from reaching undesirable materials or undesirable contacts whilst using the internet and digital technologies.
- Ensure that school systems and users are protected from accidental or unacceptable use that could put the security of the systems and users at risk.
- Ensure that staff and pupils are protected from potential risk in their use of technology in their everyday work.
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

1.3. This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors who are representing the school.

1.4. Breaches of this policy may be dealt with under our disciplinary policy and staff code of conduct.

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The General Data Protection Regulation
- 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

- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2021
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

3. Definitions

- "**ICT facilities**": includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- "**Users**": anyone authorised by the school to use the 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
- "**Authorised personnel**": employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- "**Materials**": files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs
- "**Undesirable materials**": for example but not limited to; abusive, discriminatory or obscene text of images
- "**Undesirable contacts**": for example but not limited to; digital messages from unknown or unverified parties, who seek to establish a child's identity and/or to communicate with them, such as for advertising or potentially criminal purposes

3.1. See appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

4.1. The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings.

4.2. Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, 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 (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, 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, anti-Semitic or discriminatory in any other way

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

4.4. Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion by asking the headteacher / SLT directly.

4.5. Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour and discipline. Copies of which can be found on the shared drive area.

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

5.1. Access to school ICT facilities and materials

The school's ICT Lead in conjunction with the SBM manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

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

All devices must be locked or shut down if left unattended to ensure their security both in and away from school. Usernames and/or passwords must be kept confidential, secure and changed as required.

Passwords should never written down or stored in places where it is possible that someone unauthorised may see or steal it.

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 ICT Lead or SBM.

5.2. Use of phones and email

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

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 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 school's Data Protection Officer 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 in this policy.

No personal mobile devices (ie mobile phones) should be used around children at any time, unless is it an emergency or as agreed by the Headteacher or SLT.

If you record calls, callers must be made aware that the conversation is being recorded and the reasons for doing so.

Staff who would like to record a phone conversation should speak to the school's Data Protection Officer in advance of recording.

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

Requests may be granted 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 (SEN) assessments, etc.

5.3. 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 headteacher 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 non-break time
- 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 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. 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 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 and use of email to protect themselves online and avoid compromising their professional integrity.

5.4. Personal social media accounts

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

5.5. Remote access

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

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 ICT Lead 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.

The school's data protection policy can be found on the school website.

5.6. School social media accounts

The school has an official Facebook page managed by the school office and EYFS Twitter and Instagram accounts managed by the EYFS team. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access 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.

5.7. Monitoring of school network and use of ICT facilities

5.8. The school reserves the right to monitor, capture and record 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

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

5.10. The school monitors, captures and records ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Pupils

6.1. Access to ICT facilities

Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff.

Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff.

Pupils will be provided with an account linked to the school's virtual learning environment, which they can access from any device by using the following URL www.coppice.worcs.sch.uk

All pupils' digital activity is filtered, monitored, captured and recorded when using the school's digital technology and communication systems and this helps protect them from harm. As such, all pupils' digital activity must be closely supervised and only on devices that are managed by the school.

All pupils must follow a rigorous and up-to-date Online Safety and Digital Literacy scheme of work and teaching staff are responsible for ensuring its delivery.

Only Year 6 and Year 5 pupils are allowed to bring personal mobile phones into school. They must be stored in a secure location and handed in at the start of the day and returned at the end. They can never be used to access the school network or internet.

Pupils must never intentionally seek offensive material on the internet. Any transgression should be reported to the DSL and the evidence recorded as below. Any incident will be treated through the school's Behaviour Management system.

Every reasonable step has to be taken to prevent exposure of children to undesirable materials on digital devices or the internet. It is recognised that this can happen not only through deliberate searching for such materials, but also unintentionally when a justifiable internet search yields unexpected results.

6.2. Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has 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.

The school 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.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

6.3. Unacceptable use of ICT and the internet outside of school

The school 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 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
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other 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

7. Parents

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

Where parents 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

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.

8. Data security

8.1. The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.2. Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

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

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

Teachers will generate passwords for pupils using a password manager/generator and keep these in a secure location in case pupils lose or forget their passwords.

8.3. Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will 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.

8.4. Data protection

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

Further information can be found in the school's Data Protection (Including GDPR) policy.

8.5. Access to facilities and materials

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

These access rights are managed by the ICT Lead.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the ICT Lead or SBM 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.

8.6. Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

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

9. Protection from cyber attacks

9.1. Please see the glossary (appendix 6) to help you understand cyber security terminology.

9.2. The school will:

- Work with Trustees and the ICT Lead to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
    - Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
    - Investigate whether our IT software needs updating or replacing to be more secure
    - Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - 'Proportionate': the school will verify this using an audit at least annually, to objectively test that what it has in place is up to scratch
    - 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 up to scratch and secure as they can be
- Back up critical data regularly (overnight) and store these backups offsite.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our ICT service providers and ICT Lead.
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the ICT Lead, for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify

Action Fraud of the incident. This will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

10. Internet access

10.1. The school wireless internet connection is secured and protected with a Smoothwall firewall.

10.2. Parents and visitors

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

10.3. 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

11.1. The headteacher, ICT Lead and SBM monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

11.2. This policy will be reviewed every three years and approved by the Trustees.

12. Related policies

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

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

13. Agreement

13.1. I have read and understand the above policy and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out work related to the school) within these guidelines.

Staff/Volunteer Name: _____

Signed: _____

Date: _____