Preston Candover CE Primary School

ICT and Internet Acceptable Use Policy

Reviewed by: IT Lead
Last Review Date: April 2026
Next review date: April 2029

Inspire learning for life

Encourage each other and build each other up - 1 Thessalonians 5:11

Love Hope Justice

Contents

1. Introduction and aims 2
2. Relevant legislation and guidance 3
3. Definitions 3
4. Unacceptable use 3
5. Staff (including governors, volunteers, and contractors) 4
6. Pupils 11
7. Parents/carers 122
8. Data security 133
9. Protection from cyber attacks 15
10. Internet access 16
11. Monitoring and review 16
12. Related policies 16
Appendix 1: Acceptable use of the internet: agreement for parents and carers 17
Appendix 2: Acceptable use agreement for staff, governors, volunteers and visitors 18
Appendix 3: Acceptable use agreement for pupils 19
Appendix 4: Glossary of cyber security terminology 20
Appendix 5: Using Images and Videos Multimedia Consent Form 212
Appendix 6: Facebook Cheat Sheet for Staff 24

---

1. Introduction and aims

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

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

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur 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

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors, visitors, and anyone who has access to our IT and communication systems.

Misuse of IT and communications systems can damage our school and our reputation. Breaches of this policy may be dealt with under our staff code of conduct and supporting policies.

2. Relevant legislation and guidance

This policy refers to, complies with, or otherwise has regard to, 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
- Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2025
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- 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, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 4 for a glossary of cyber security terminology.

4. Unacceptable use

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

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity

- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral
- 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 school, its pupils, or other members of the school community
- Using the school's systems to participate in internet chat rooms, post on internet message boards or blogs, unless approved by authorised personnel
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the internet and network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

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

4.1 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.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on staff code of conduct which can be found in the Key Policies folder in the staff room/ school office.

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

5.1 Access to school ICT facilities and materials

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

- Computers, tablets, mobile phones and other devices

- Access permissions for certain programmes or files

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

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Headteacher and then Agile ICT if permission is granted

5.1.1 Use of mobile phones, cameras and wearable technologies

The school does not permit the use of personal mobile phones and cameras by staff and visitors where children are present

Staff and visitors will not carry personal mobile phones while working. This protects staff from being distracted from their work, and from allegations of inappropriate use. Staff phones will be kept either in the staffroom or in their bags or in a secure cupboard.

If staff have a break time during their working hours, they may use their mobile phones during these times, in the PPA room or behind the school office, away from the children.

Where it is essential for staff to make a personal call during a session, they should (with the agreement of SLT) make this in an area not used by children.

Staff must give the school telephone number to their next of kin, in case it is necessary for the staff member to be contacted, in an emergency during session hours.

Mobile phones will be taken on whole-group outings in accordance with guidance. This will be used only to communicate with other teachers, school, emergency professional, or parents when appropriate and in an emergency. Mobile phones will not be used to take photos during these outings. School camera or iPads will be used following the online safety policy requirements.

In the case of school productions and events, parents are requested to only take photos of their child/ren and not to post on social media sites.

In EYFS – no assessment photos can be taken by staff on their mobile phones these must be taken on a school ipad as per school policy.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business.

No child is allowed a mobile in school. If a child brings a mobile for a special circumstance or by 'mistake' the phone will be taken to the office for safe keeping for the duration of the day and handed over to the parents at home time.

The school displays a notice advising visitors and parents/carers that mobile phones are not to be used in the school. If they need to use their mobile phone they will be asked to use this away from the children. Visitors will be asked to switch their phones onto silent while in school

No videos, photos are allowed at social events such as plays/ performances/ sports day unless told permission is granted by the headteacher. In these cases, individual 1 on 1 photos can be taken as long as no other child is present and it is the child of the designated parent or guardian.

All parents/ guardians are requested not to put these images on social networking sites

If a child needs to contact his/her parents/carers they will be allowed to use the school phone. If parents need to contact their children urgently they should phone school office and leave a message and this message will be relayed to the child and/or child's teacher.

School accepts no responsibility theft, loss or damage relating to mobile phones. It is the responsibility of staff and parents to ensure that mobile phones are properly insured

5.1.2 Use of email

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

This email account should be used for work purposes only. These will be accessed via a username and password.

All work-related business should be conducted using the email address the school has provided. Personal email addresses will not be used.

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.

All digital communications should be professional in tone.

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 subject access requests from individuals under the UK GDPR and 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 using a strong, state-of-the-art encryption standard so that the information is only accessible by the intended recipient.

If staff send an email in error that contains the personal information of another person, they must inform the Headteacher/ Senior Leadership Team immediately and follow our data breach procedure.

Email is covered by the Data protection and freedom of information act and safe practise will be followed in using email to ensure confidentiality. School email addresses may be monitored at any time in accordance with the acceptable use policy.

All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.

All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Our school includes a standard disclaimer at the bottom of all outgoing emails (see below).
Preston Candover CE Primary School email disclaimer:

> This e-mail and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent Preston Candover CE Primary School. If you are not the intended recipient, you must not use, disseminate, forward, print or copy this e-mail or its contents. If you have received this e-mail in error, please contact the sender. Please note that e-mail may be monitored in accordance with both school policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.

5.1.3 Video Conferencing

In our school the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing (Teams, Google Meets).

- Approval by the Headteacher shall be obtained in advance of other video conference taking place outside of remote learning. All sessions should be logged including the date, time and the name of the external organisation/ person(s) taking part.
- Pupils using video conferencing equipment should be supervised at all times.
- All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to stop or hang up the call.
- Copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.

5.1.4 Use of Digital Media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues.

On admission, all parents/carers will be asked to sign the consent for photos to be taken in school or by the media for use in relation to promoting/publishing the school e.g school prospectus/school website/school displays.

This consent will last for a maximum of 7 + 1 years only. The consent will be gained when the child starts school at Preston Candover CE Primary School (Reception class) The consent can be changed at any point, in writing, by contacting the school office.

This does not cover any other agency and if any other agency requests to take photographs of any child then separate consent before photographs are taken will be sought. Images will not be displayed if parents do not agree and will be removed if children leave the school.

Our policy is to only use images where groups of children are involved in activity that represent the work that pupils are doing thus enabling the school to celebrate our achievements to others.

We allow parents/carers to take photos of special events/ school activities when invited **but to not focus on any child but their own.**

In order to support this policy, we would ask parents/carers not to use any images of our pupils on social networking sites (i.e. Facebook). This includes any professional photos that have been purchased through the school and any photos taken during school concerts or sports events etc. It is acknowledged that often photographs may contain other children in the background.

Staff can photograph and record events on school equipment.

5.1.5 Storage of Photographs/ Video

Under General Data Protection Regulation, the school must seek parental consent to take photographs and use video recorders. Parents will be asked to sign a pupil ‘Using images & video Multimedia Consent form’ at the beginning of the academic year.

Photographs are displayed in school; on the website; in the school prospectus as well as in the media. Photographs for school use and taken for school purposes must only be taken with school equipment and remain on school premises.

These images/videos must only be stored on school equipment in school. Pupils must be appropriately dressed for the activity they are par taking in considering health and safety and hygiene.

Images of staff at work are not allowed to be used on social media and can only be used in media/the school website if permission is given for each individual photo/image. This will be removed if staff leave their position. Photos of staff taken outside of school are not affected by this but it should be considered as to whether images on social media will bring into disrepute your integrity, as well as the potential misuse of these images.

The following disclaimer is visible on both school website and virtual learning environment:

NB: Preston Candover CE Primary School are not responsible for information and images outside of this website. We will endeavour to add links to appropriate materials only but we cannot monitor links from these websites to new ones. We teach your child about keeping safe online and would encourage you to do so. All displayed photos/videos etc. are displayed in accordance with parental consent forms.

Photographs are securely stored and should not be removed from the school environment unless for a specific purpose and with the head teacher's consent. In this instance the data must be kept secure and must be erased after use. This could include storage of images on portable devices e.g. laptops or tablets.

Images should be stored on tablets for the minimal amount of time. Only images intended for a specific purpose should be stored. They must be stored securely and be deleted once they have been used

Staff should not store images on personal equipment e.g. tablets, laptops or USB storage devices.

Staff should not store personal images on school equipment unless they have a clear purpose e.g. to support in the teaching of a lesson. Once used, the images should be deleted.

Access to photographs / videos stored on school's equipment is restricted to school staff.

Should a parent withdraw permission the class teacher is responsible for the removal and deletion of images and may be assisted by the ICT subject leader.

Photographs sent electronically must be sent securely. This is done using staff accounts on the HCC e-mail system.

5.1.6 Social Media

In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

- Social networking sites (i.e. Facebook) are becoming increasingly popular amongst the adult population and young people. However, many sites do have age restriction policies where the minimum acceptable age is 13 years. **Any child who sets up or uses such a site and is below the acceptable age is in clear breach of these age-restriction policies and anyone providing false information is violating the site 'Statements of rights'**.

- For this reason, we would actively discourage pupils in our school using any social networking sites where these restrictions apply. Pupils who are found to be misusing websites where derogatory comments against other pupils, members of staff or the school are being made will have their internet access rights in school removed and in serious cases further action will be taken. Staff must also consider the security settings of these sites and if it will compromise their position in school. If this occurs staff may be disciplined or in extreme cases, outside agencies may become involved.

Please see our Social Media Policy on our school website for further information.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. We will update our policy to reflect what we consider to be acceptable and unacceptable use of these as and when required and this is an ongoing process.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Headteacher 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 teaching hours/ contact 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 (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

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/carers could see them.

Staff should take care to follow the school's guidelines on use of social media (see social media policy on our website) and use of email (see section 5.1.2) 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 social media accounts (Facebook Cheat Sheet- Appendix 6)

5.3 Remote access

Remote Access in school is limited and only granted following a discussion with the Headteacher.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions as the network manager may require against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy which can be accessed on the school website.

5.4 School social media accounts

The school has an official Instagram account, managed by the admin 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 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.

Please see our school Social Media Policy on our website for more information.

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

To comply with Department for Education (DfE) guidance on meeting digital and technology standards, and to safeguard and promote the welfare of children and provide them with a safe environment to learn, the school 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 authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The school's network provider has in place the necessary filtering and monitoring systems and shares any relevant information with the Headteacher.

The school reserves the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the school, including for the following purposes

- To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy
- To find lost messages or retrieve messages lost due to computer failure
- To help in the investigation of alleged wrongdoing
- To comply with any legal obligation

The list above is not exhaustive.

The school monitors ICT use in order to:

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

Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
  - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

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

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

5.6 Dealing with Incidents relating to Unacceptable Use

Our school will consider the types of incidents that may occur and how these will be dealt with.

An incident log will be completed to record and monitor offences. This is kept with the Online Safety, Mobile Technology and Acceptable Use Policy in the Headteachers office. These will be audited on a regular basis by the Headteacher and reviewed by the Governing Body H & S Committee. All staff are aware of the different types of Online Safety incident (illegal and inappropriate) and how to respond appropriately. Pupils are informed of these procedures via assemblies, in class and through reading and signing the AUP. The head teacher will decide at which point parents or external agencies are involved.

The school uses the Online Safety Incident/Escalation Procedures document – See Online Safety Policy- as a

framework for responding to incidents.

Illegal Offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who will refer this to external authorities, e.g. Police, CEOP, and Internet Watch Foundation (IWF). We will **never personally investigate, interfere with or share evidence as this may cause us to inadvertently commit an illegal offence.** We will always report illegal content to the IWF as they are licensed to investigate – we are not!

Correct procedures will be followed when preserving evidence to protect those investigating the incident and are as follows:

- Turn off the monitor (Do NOT turn off the system)
- Ensure the system is NOT used or accessed by any other persons (inc technical staff)
- Make a note of the date/time of the incident along with any relevant summary details
- Contact our school's neighbourhood policing team for further advice

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

Inappropriate Use

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and are proportionate to the offence. The school will decide what constitutes inappropriate use and the sanctions to be applied. Some examples of inappropriate incidents are listed below with suggested sanctions.

<table>
<tr><th>INCIDENT</th><th>PROCEDURE AND SANCTIONS</th></tr>
<tr><td>ACCIDENTAL ACCESS TO INAPPROPRIATE MATERIALS</td><td>- Minimise the webpage/turn the monitor off
- Tell a trusted adult
- Enter the details in the Incident Log and report to filtering services if necessary
- Persistent 'accidental' offenders may need further disciplinary action</td></tr>
<tr><td>USING OTHER PEOPLE'S LOGINS AND PASSWORDS MALICIOUSLY</td><td rowspan="4">- Inform Headteacher
- Enter details in the Incident Log
- Additional awareness raising of Online Safety issues and the AUP with individual child/class
- More serious or persistent offenses may result in further disciplinary action in line with Behaviour Policy
- Consider parent/carer involvement</td></tr>
<tr><td>DELIBERATELY SEARCHING FOR INAPPROPRIATE MATERIALS</td></tr>
<tr><td>BRINGING INAPPROPRIATE ELECTRONIC FILES FROM HOME</td></tr>
<tr><td>USING CHATS AND FORUMS IN AN INAPPROPRIATE WAY</td></tr>
</table>

6. Pupils

6.1 Access to ICT facilities

- Computer 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
- 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 Headteacher
- 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 Headteacher 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.

6.2 Encryption

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

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

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

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with our 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 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 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 the 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

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

7. Parents/carers

7.1 Access to ICT facilities and materials

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

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

Where parents/carers are granted access in this way, they must abide by this policy.

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

We ask parents/carers to sign the agreement in appendix 1.

7.3 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.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

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

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

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Users are prompted to review their passwords occasionally for increased security.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. You must keep these passwords confidential and change them regularly.

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 use the password manager required by the network manager to help them store their passwords securely. Teachers will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.

8.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any incoming files should always be virus-checked by the computer software installed before they are downloaded.

Any personal devices using the school'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 school's data protection policy which can be accessed on the school website or in the Key Policies folder in the staff room/ school office.

In line with the requirements of General Data Protection Regulation, sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

1. Accurate
2. Kept safe and secure
3. Used fairly and lawfully
4. Used for limited, specifically stated purposes
5. Handled in accordance with the data subject's rights
6. Adequate, relevant and not excessive
7. Kept no longer than absolutely necessary
8. Only transferred to others with adequate protection
9. All laptops are password protected

Our school ensures that data is appropriately managed both within and outside the school in the following ways:

- School equipment, including laptops, must only be used for school purposes and do not contain personal information eg, personal images, personal financial details, music downloads, personal software. Computers are accessed via a safe username and password and it is the responsibility of the individual to keep this secure at all times.
- School equipment must not be used for non-educational purpose, for example for online gambling, dating websites, home shopping, booking holidays, social networking BOTH at home and in school.
- Any breaches in security must be reported immediately to the Data Protection Officer (DPO).
- Staff are aware of the school's procedures for disposing of sensitive data, eg, shredding hard copies, deleting digital information, deleting usernames and passwords from network and deleting email accounts when children leave.
- The school's policy is to remove sensitive data prior to disposal or repair of equipment and all staff are aware of the person responsible.
- School data shall NOT be stored on personal equipment, eg, home computer or mobile phone.
- Staff are allowed to use personal storage devices, eg, external hard drives, pen drives in school to transfer planning from home but this must be kept secure with encryption, passwords and virus checkers ran on device before usage and not contain any personal data.
- Staff must ensure they log out of computers when out of use and all computers will go to the screen saver screen after 10 minutes only allowing access to those with a password. No confidential information is stored on individual computers so to limit its accessibility.

8.4 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 Headteacher.

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 Headteacher 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 school makes sure that its devices and systems have an appropriate level of encryption.

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

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

9. Protection from cyber attacks

Please see the glossary (appendix 4) to help you understand cyber security terminology.

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for all users, including staff, pupils and governors (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- please see Online Safety Policy for more details about this.
  - How to check the sender address in an email
  - How to respond to a request for bank details, personal information or login details
  - How to 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) annually, to objectively test that what it has in place is effective
  - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
  - **Up to date:** with a system in place to monitor when the school needs to update its software
  - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data regularly and store these backups on [cloud-based backup systems/external hard drives that aren't connected to the school network and which can be stored off the school premises]
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to [our cloud-based provider/our IT department (if you use an on-premises provider)]
- Make sure staff:
  - Dial into our network using a virtual private network (VPN) when working from home
  - Enable multi-factor authentication where they can, on things like school email accounts
  - Store passwords securely using a password manager
- 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
- Make sure all necessary firewalls are in place and switched on (and that all areas of the network are secured effectively)
- Make sure effective cyber breach prevention measures and processes are in place, e.g. endpoint detection and response systems
- 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 (or a similarly effective and recognised) certification

- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. 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 our LA to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement
- Conduct a cyber risk assessment at least annually, and revisit it every term, or after a significant event has occurred

10. Internet access

The school's wireless internet connection is secure.

Mobile devices can only access the school's broadband internet connection if set up by the school technician with permission of the Headteacher.

Ipads are now in use at school and online resources used need to pass through the schools strict filtering system. Apps are put on Ipads via ICT leader/Agile.

10.1 Pupils

Wifi is used by pupils on laptops and Ipads in school. These connections are managed by the network provider. Pupils are not given the Wifi access details. Internet is used when permission is granted by a teacher or LSA and under supervision.

10.2 Parents/carers and visitors

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

The headteacher will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The headteacher, SLt and Network Manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 3 years.

12. Related policies

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

- Online safety
- Social media
- Safeguarding and child protection
- Behaviour
- Staff Code of Conduct
- Data protection
- Remote education

Appendix 1: 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 child:

Online channels are an important way for parents/carers to communicate with, or about, our school.
The school uses the following channels:

- Our School Website
- Emails for parents (for school announcements, reminders and general information)
- Our official Instagram Page

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a school-related 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:**

Appendix 2: Acceptable use agreement (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 systems and accessing the internet in school, or outside school on a work device (if applicable), 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 that 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
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share

Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

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

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: Acceptable use agreement (Pupils)





Preston Candover CE Primary School
ICT Acceptable Use
Pupil Agreement/Online Safety Rules

It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the internet.

- I will only use ICT in school for school purposes
- I will only use the internet and/or online tools when a trusted adult is present
- I will not deliberately look for, save or send anything that could be unpleasant or nasty
- I will not deliberately look for, or access inappropriate websites
- I will not use AI tools and generative chatbots (such as ChatGPT or Google Bard) without my teacher's permission
- I will not bring into school any electronic mobile devices e.g. cameras, phones, smart watches etc.
- I agree to use the school iPad camera and microphone functions in a sensible way and under supervision
- If I accidentally find anything inappropriate I will tell my teacher immediately
- I will only communicate online with people that a trusted adult has approved
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not give out my own, or others', details such as names, phone numbers or home addresses
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will not attempt to download or install anything onto the school network without permission
- I will be responsible for my behaviour when using ICT because I know these rules help to keep me safe
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my online safety

Pupil's agreement:
I have read and understand the school rules for responsible internet use and technology.

Pupil's signature: …… Date: ……

Parent/carer signature:
I have read and understand the school rules for responsible internet use and technology. We have discussed this and …… (print child's name) agrees to follow the online safety rules and to support the safe use of ICT at Preston Candover CE Primary School.

Parent/carer name (PRINT): ……

Parent/carer name (signature): …… Date: ……

Appendix 4: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. Many of these terms are from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove viruses and other kinds of malicious software.
Breach	When your data, computer systems or networks are accessed or affected without authorisation.
Cloud	An on-demand, massively scalable service, hosted on a shared infrastructure 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	Any event that threatens the confidentiality, integrity, or availability of data within your computer network, or where the security of your system or service has otherwise been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from unauthorised 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 who uses their technology skills to gain unauthorised access to computers, systems and networks.
Malware	Malicious software. Any kind of software that can damage computer systems, networks or devices, which includes viruses, trojans or any code or content that is harmful.
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 with the end aim of fixing them.
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 or text messages sent to many people asking for sensitive information (such

TERM	DEFINITION
	as bank details or passwords) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems, usually by encrypting your files, until you make a payment (a ransom) for decryption.
Social engineering	Manipulating people into giving information or carrying out specific actions that's of use to an attacker.
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.

Appendix 5: Using Images & Video Multimedia Consent Form

Using images & Video Multimedia consent form

To **Name of the child's parent or guardian:** _____

Name of child: _____

Occasionally, we may take photographs or produce videos for business purposes that include our pupils. We may use these images in our marketing or in other printed publications that we produce, as well as on our website, on our social media or on project display boards. We may also make video or webcam recordings for school-to-school conferences, monitoring or other educational use.

From time to time, our school may be visited by the media who will take photographs or film footage of a visiting dignitary or other high profile event. Pupils will often appear in these images, which may appear in local or national newspapers, or on televised news programmes.

To comply with the General Data Protection Regulation of 2018, we need your permission before we can photograph or make any recordings of your child for promotional purposes. Please answer questions 1 to 5 below, then turn over and sign and date the form where shown.

The information you provide (address, contact numbers) will be securely stored and processed within the European Economic Area (EEA) and not be used for any other purpose than confirming your permission to use the material.

Please return the completed form to the school as soon as possible.

	Please circle your answer
1. May we use your child's photograph in printed publications that we produce for promotional purposes or on project display boards?	**Yes / No**
2. May we use your child's image or video on our website?	**Yes / No**
3. May we record your child's image on video or webcam?	**Yes / No**
4. Are you happy for your child to appear in the media	**Yes / No**
School to delete this question where social media not used. 5. Are you happy for your child to appear on Social Media sites used by the school e.g. Twitter and Facebook - *Please note that once images are uploaded, they will be subject to the terms and conditions of the social media site. Neither you nor the school will have control over how those images are further used, amended or reproduced, either by the site or by the public. Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK European law applies.*	**Yes / No**

Conditions of use

1. This form is valid for seven years from the date you sign it, or for the period of time your child attends this school, plus one year. The consent will automatically expire after this time.

2. We will not re-use any photographs or recordings after your child leaves this school.

3. We will not use the personal details or full names (which means first name and surname) of any child or adult in a photographic image on video, on our website, in our school prospectus or in any of our other printed publications without good reason. For example, we may include the full name of a pupil in a newsletter to parents if the pupil has won an award.

4. If we name a pupil in the text, we will not use a photograph of that child to accompany the article without good reason. (See point 3 above.)

5. We will not include personal e-mail or postal addresses, or telephone or fax numbers on video, on our website, in our school prospectus or in other printed publications.

6. We may include pictures of pupils and teachers that have been drawn by the pupils.

7. We may use group or class photographs or footage with very general labels, such as ‘a science lesson’ or ‘making Christmas decorations’.

8. We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.

9. Your consent can be withdrawn at any time in writing.

10. Images and videos will only be stored within the EEA in order to conform to the GDPR of 2018.

11. If we wish to retain any images or video for the schools historical archives, we will sought written permission from a child’s parents with full and transparent reasons to support the request.

12. After a cohort leaves the school we will archive students work for a period of one year. This will securely be stored and hidden from open view on the school network. Parents of students can request evidence of a child’s work for up to one year after that child’s cohort has left the school by submitting a Subject Access Request (SAR) via the school office. After the archive year has passed students data will be completely removed from the school network and become unrecoverable.

Please note that the press have some exemptions from data protection legislation and may want to include the names and personal details of children and adults in the media.
I have read and understood the conditions of use and give my consent for my child’s image/s & videos to be used as described above.

Your signature ……..…….. Date ……
Your name (in block capitals) ……..

Appendix 6: Facebook Cheat Sheet for Staff

Do not accept friend requests from pupils on social media

10 rules for school staff on Facebook

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 bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if …

A pupil adds you on social media

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

- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police