Parent / Carer Acceptable Use Policy Agreement

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 disciplinary policy/behaviour policy/staff discipline policy/staff code of conduct.

Conduct

- Your child is expected to recognise the importance of following all online safety rules, the same way as they are expected to follow all other school rules.
- Your child will sign an Acceptable Use Agreement which clearly outlines the expectations of online learning behaviours.
- Your child will respect the no tolerance for online bullying (cyber-bullying) activities, and will not partake in any of this.
- Where pupils fail to respect these rules, parents will be informed and it will be addressed in school, with sanctions as outlined in our school's anti-bullying policy.
- As often as needed, your child will be taught how to keep safe in a world of online learning, through a series of online safety lessons.
- Your child has his/her own log in user name and password for various log in systems and online learning platforms associated with our school, and must always keep their details private.
- Your child must take responsibility for using their log in details are used.
- On a regular basis, your child's online use in school will be monitored and you will be contacted if there is misconduct of use.

Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy through our Staff code of conduct, disciplinary or behaviour policy

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 Head teacher 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.

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 these must be discussed with them.

Content

- Our school regularly monitors and filters its systems and using a ICT software system to ensure appropriate use, in order to provide a safe online learning environment for your child. We will teach your child about the importance of keeping safe when engaging with online platforms and technological devices we encourage parents to support us with this at home too.
- Age inappropriate online gaming sites and devices are not allowed at our school, since these can sometimes include inappropriate language and content for your child. It can also enhance the risk of unknown adults making unwanted contact with your child in the online world, which can lead to many online as well as physical mishaps.
- Each day, age appropriate learning platforms and websites are used at our school. We are aware that on occasions, you may permit your child to access social media platforms and other sites which may not be age appropriate. Where this is evident, as a parent/carer, you will need to monitor and take ownership for any issues which may arise and which may cause online distress to your child, as a result of this.

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 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 are 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 wireless internet connection is secure.

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 as appropriate.

Contact

- Our school staff should only contact parents and/or children through the agreed school systems, which includes Class Dojo, SIM's text or email, telephone conversations and school emails as agreed by the Headteacher of the school. With this in mind, we should avoid initiating friend requests with staff or students on social networking sites.

- Your child can contact other children within their class/year group, via the agreed online learning platforms, which may include emails; Class Dojos – but may not be limited to only these in given circumstances as it may arise.

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use digital cameras to record evidence of learning and activities. These images may then be used in presentations in subsequent lessons or to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published the young people can not be identified by the use of their names.

Permission Form

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Parent / Carers Name		Date	
Student / Pupil Name			

- As the parent / carer of the above student, I give permission for my son / daughter to have access to the internet and Computing/ICT systems at school. I know that my son / daughter has signed an Acceptable Use Agreement (AUP) and has received, or will receive, online safety education to help them understand the importance of safe use of Computing/ICT – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and Computing/ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's / daughter's activity on the Computing/ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the AUP.
- I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.
- I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Home Use of the Internet

We hope you will reinforce the issues contained in the Student Acceptable Use Policy when your child uses the internet at home. In order to do this, we recommend that you:

- Ensure that children access the internet in a communal room and that there is appropriate supervision for the age of your child (including supervising all internet use by younger users).
- Set appropriate rules for using the Computing/ICT and the internet safely at home. The school rules could provide a starting point.

- Inform the school of any concerns that the school could help to address through teaching.
- Ask your child about the sites they are visiting.
- Ensure that family computers are password protected and have robust anti-virus software which is regularly updated.
- Ensure content is appropriately filtered for younger users.
- Ensure that your child knows that any protection system does not stop all unsafe content and that they need to tell you if they access something inappropriate or get an upsetting message.
- Reassure your child that if they talk to you about a problem they are having on the internet you will not ban them from using it as this will discourage them from telling you.
- Ensure that your child knows not to leave computers logged on with their user name or logged on to sites with personal details entered as others could use them.

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

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.

In order to support those parents who may be less familiar with use of the internet we have listed a variety of additional measures that you could take at home to support your child's safe use of the internet.

Additional Guidance on Safe Use of Computing/ICT at Home Keeping Safe

- Discuss user names with children and talk about how to choose them carefully to protect their identity.
- Talk to young people about the information they should keep private in order to prevent them being contacted or traced including full name, address, telephone no, school, places they do regularly.
- Talk to young people about the need to limit access to their own information by using the safety and privacy features of sites to only give access to people they know and being careful who they add as friends.
- Model safe behaviour in your use of ICT/Computing.

Research and Fun on the internet

- Talk to your child about the fact that any information published on the web can be read by anyone and that they should only publish information they would be happy for anyone to read.
- Check information that younger users are publishing on the web before it is posted to ensure that they are not putting themselves at risk.
- Check that they are old enough for the sites they are using.

Communicating

- Discuss the need for young people to be polite to others online and that they should not use bad language or comments which might upset others.
- Discuss the fact that e-mails / messages can be intercepted and forwarded on to anyone (including parents, head teacher or future employer!).
- Ensure that young people know they should not open messages if the subject field contains anything offensive or if they do not recognise who it is from and that the safest thing to do is to delete it without opening it.
- Recognise that there is a difference between online friends who you will never meet and real-world friends. Talk to your child about their online friends.
- Remind your child that people they talk to online may not be who they seem.

Sharing

- Ensure your child knows that downloading games and music that is copyrighted without paying for it is illegal

School social media accounts

The school has an official site for promoting the school these are Face book Instagram and X account; these are managed by senior leadership team. Staff members who have not been authorised to manage, or post on, 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. The school will not engage with pupils on any of these sites

Buying and Selling Online

- Help young people to tell the difference between web sites for information and web sites selling things.
- Discuss how to recognise commercial uses of the internet e.g. I Tunes, mobile phone downloads, shopping.
- Remind young people that if an offer looks too good to be true it probably is and that they should not respond to unsolicited online offers.
- Remind young people that they should not purchase or download anything that costs money without asking permission and that they should not use someone else's identity to buy things online.

Detecting Problems

- Ensure that they know that if they receive an offensive or worrying message / e-mail they should not reply but should save it and tell you.

<u>Protection from cyber attacks</u>

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, including:
- The methods hackers use for tricking people into disclosing personal information, including phishing
- Online safety and password security
- Social engineering, including not using websites that host unsuitable material, and could also contain malware and viruses
- The physical security of devices, for example not leaving a laptop unlocked and unattended
- The school does not use removable storage media, such as USBs
- Multi-factor authentication
- How and when to report a cyber incident or attack
- How and when to report a data breach
- Data protection for all staff. Staff who are exposed to higher-risk data will have more frequent training
- 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 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

- Critical data should be backed up regularly, ideally at least once per day. Backups should be stored using cloud-based backup systems or external hard drives that are not connected to the school network and can be securely 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
- 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 certification
- We will develop, review, and test an Incident Response Plan in collaboration with the IT department. The plan will outline how the school will respond to cyber incidents, including how communication will be maintained if normal systems are unavailable, who will be contacted and when, and who is responsible for notifying relevant stakeholders of the incident.
- The Incident Response Plan will be reviewed regularly, tested through exercises, and updated following any significant incident to ensure continuous improvement. The school will use guidance from the **UK National Cyber Security Centre (NCSC)** to support the development, testing, and review of this plan.

- 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
- Appoint a digital lead (from the senior leadership team) to oversee cyber risk assessment

Related policies

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

- Online safety
- Social media
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote education

Date agreed by governing body on March 2026	**Signature of Chair or Vice Chair**
Date agreed for review Autumn 2027	**Frequency of Review** Annually
Responsibility for Review PPC Committee	