Acceptable Use of Technology Policy

Date reviewed/updated	**March 2026**
Next review date	**March 2027**
Cheryl Chalkley – Headteacher **Signed:** Mrs C. Chalkley **Date:** Charlotte Francis – Chair of Governors **Signed:** Ms. C Francis **Date:**	

Contents

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.

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

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

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 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 or DSL 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.

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 Applications for exemptions should be made in writing to the Headteacher.

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 behaviour/staff code of conduct. Other sanctions, such as, revoking permissions for school systems may also be called upon as a sanction in some cases.

Copies of relevant policies can either be found on the school website or are available, on request, from the school office.

Staff (including governors, volunteers, and contractors)

Access to school ICT facilities and materials

The school's ICT support (NCS) 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 NCS.

Use of school-supplied equipment

School-issued devices (including laptops, tablets and other digital devices) are provided to staff for the purpose of supporting teaching, learning and the efficient running of the school. All school-supplied equipment remains the property of the school and staff must return the equipment at the end of employment, or when it is no longer required. Staff must:

- Use equipment and devices primarily for school purposes and in line with the school's policies on safeguarding, data protection and confidentiality
- Store devices securely when not in use, particularly when travelling. Devices should not be left unattended in public places or in unsecured locations
- Be actively aware of data security and confidentiality and follow best practice when accessing the equipment away from school. E.g. when travelling on public transport, be aware that other passengers may be able to read any documents displayed on the screen of your device
- Lock devices with a password when unattended. Passwords must:
    - Not be shared with others and must be changed regularly
    - Be suitably strong, in accordance with the school's password policy (see below)
    - Not be reused across multiple accounts
    - Update software, operating systems and applications when prompted, or as directed by NCS support staff. Connect to the school network using approved and secure methods.

When connecting to wi-fi networks outside of the school, staff must ensure connections are secure and avoid transmitting sensitive data over public or unsecured networks

- Report any loss, theft, damage or compromise of a school device promptly to the Headteacher, Office Manager, Designated Safeguarding Lead and Data Protection Officer

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. Staff must make sure multi-factor authentication is enabled on their email account(s).

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

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

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 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 Headteacher and Data Protection Officer immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. In circumstances where staff are provided with phones, these staff must use the 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.

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 contact time/teaching hours
- Does not constitute 'unacceptable use', as defined in this policy
- 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 below). 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 the school's Mobile and Smart Technology Policy.

Staff may not store any school-related data on personal devices, on cloud storage or on personal removable storage devices.

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 Mobile and Smart Technology Policy and Social Media Policy and use of email to protect themselves online and avoid compromising their professional integrity.

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 (Social Media Policy)

School social media accounts

The school has an official Instagram account, managed by the Deputy Headteacher. 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 also has an official LinkedIn account which is managed by the Headteacher.

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.

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. Filtering and Monitoring Reports and provided daily to the Headteacher and Deputy Headteacher outlining any attempts at access filtered material. This report is provided by Broadband 4. When appropriate, information is shared with parents.

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
- 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.

Pupils

Access to ICT facilities:

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

Email addresses and passwords are provided to pupils, for educational purposes only. Pupils must not share their passwords with others, or use their email account to share or download files, including software from the Internet or inappropriate content, without the permission from their teacher.

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

Parents/Carers

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.

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 (see appendices).

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.

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

Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Users must not use the same passwords across multiple platforms.

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.

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.

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 should not delete, destroy or modify existing systems, programs, information or data. Users must not download or install software from external sources.

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.

Extra vigilance should be exercised when opening emails and files from unknown sources and advice sought from NCS if required.

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

Data protection

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

The Data Protection Policy can be found on the school website.

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 NCS and SLT.

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.

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 Headteacher.

Protection from Cyber Attacks

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 risks of using 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 (such as 360 degree safe) [insert frequency – at least 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 [insert frequency – this should be regularly and ideally at least once a day (it can be automatic)] 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 [insert frequency – this should be at least annually though ideally every 6 months] and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Maintained schools and academies, add: Work with our [LA/trust – delete as appropriate] 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

Internet Access

The school's wireless internet connection is secure. BroadBand 4 is utilised as a Filtering and Monitoring system. Filtering and Monitoring reports are reviewed regularly and specific sites and users are reported to NCS where appropriate. Staff understand that this falls within their safeguarding responsibility.

Pupils

Pupil only use school devices whilst on site and therefore no additional wifi access is required.

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.

Monitoring and Reviewing

The headteacher monitors 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 2 years, or as the need arises.

The governing board is responsible for reviewing/approving this policy.

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
- Mobile and Smart Technology

Appendix 1 - Early Years and KS1 Materials

I understand that the Mersham Primary School Acceptable Use Policy will help keep me safe and happy online.

- I only use the internet when an adult is with me
- I only click on links and buttons when I know what they do
- I keep my personal information and passwords safe online
- I only send messages online which are polite and friendly
- I know the school can see what I am doing online
- iPads/Tablets/Chromebooks should only be used with the permission of an adult
- I know that if I do not follow the rules then:
  - I will be moved down the traffic lights according to the behaviour policy
- I have read and talked about these rules with my parents/carers
- I always tell an adult/teacher if something online makes me feel unhappy or worried
- I can visit www.ceopeducation.co.uk to learn more about keeping safe online
- I have read and talked about these rules with my parents/carers.

Shortened EYFS and KS1 version (e.g. for use on posters)

- I only go online with a grown up.
- I am kind online.
- I keep information about me safe online.
- I tell a grown up if something online makes me unhappy or worried.

Early Years and KS1 Acceptable Use Poster


Be
SAFE
Online
1 I only go online with a grown up
2 I am kind online
3 I keep information about me safe
Address
Name
Age
4 I tell a grown up if something online makes me unhappy
???
eis Kent
Education iT Services
Kent County Council
kent.gov.uk
Published by EIS Kent • 0300 065 8800 • www.eiskent.co.uk

Appendix 2- KS2 Materials

I understand that the Mersham Primary School Acceptable Use Policy will help keep me safe and happy online at home and at school.

Safe

- I will behave online the same way as I behave in the classroom.
- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are safe and appropriate, and if I have permission.
- I only talk with and open messages from people I know.
- I will only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

Learning

- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use my school computers for school work unless I have permission otherwise.
- I will not print anything without the permission of an adult.
- I will only post pictures or videos on the Internet if they are appropriate and if I have permission.
- When using iPads/tablets, only the staff can put in the passcode and I will not access the 'Mail' icon.
- If I need to learn online at home, I will follow the Mersham Primary School remote learning AUP.

Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on other sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, images, or text I use.

Responsible

- I keep my personal information safe and private online.
- I will keep my passwords safe and not share them.
- I will log off when I have finished using the computer or device.
- I will not access or change other people's files or information.
- I will only change the settings on a device if a member of staff has allowed me to.

Tell

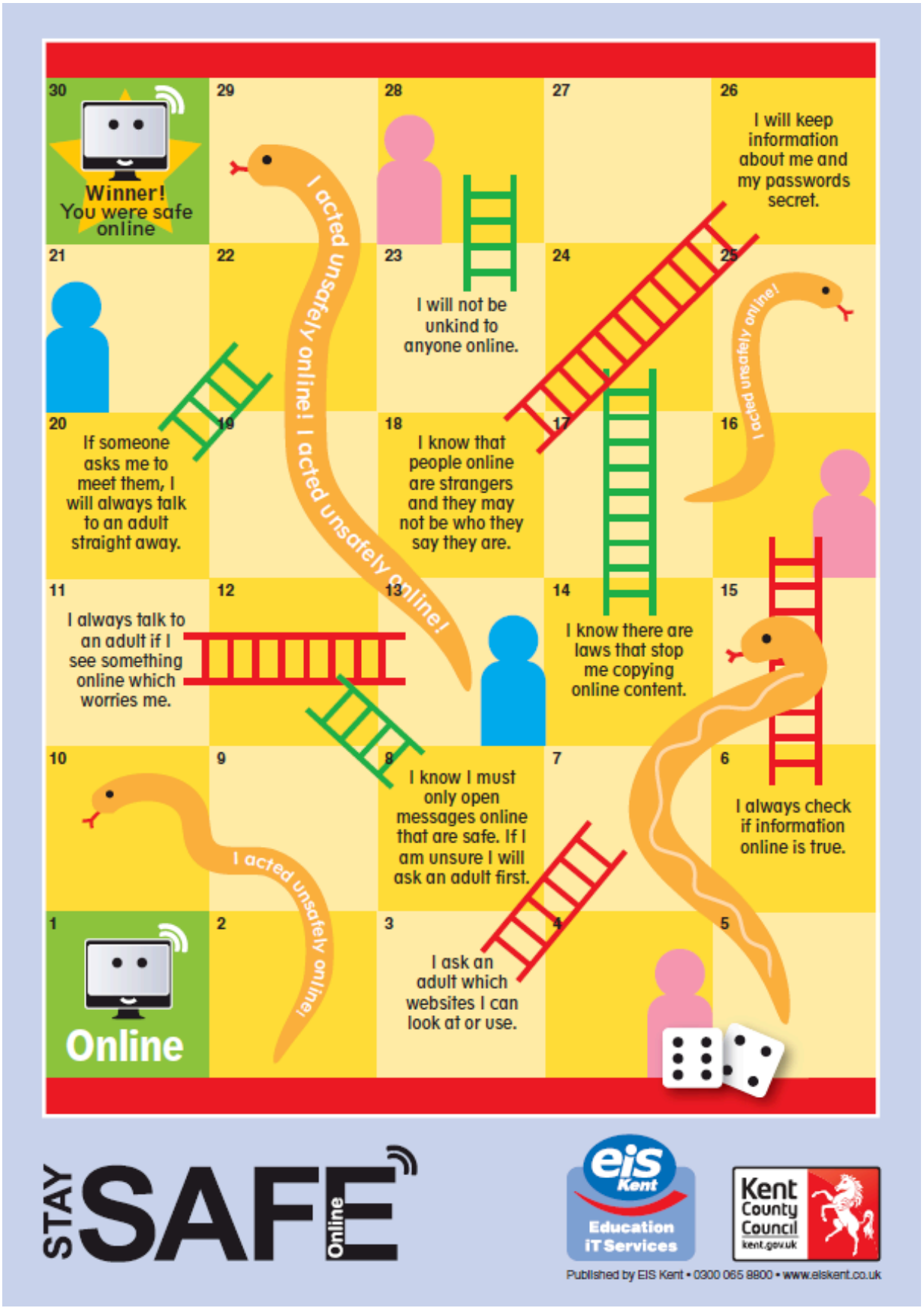
- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page/lock the screen and tell an adult straight away.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher.
- I know it is not my fault if I see or someone sends me something bad online.
- I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.

Understand

- I understand that the Mersham Primary School internet filter is there to protect me, and I will not try to bypass it.
- I know that all Mersham Primary School devices and systems are monitored to help keep me safe, including when I use them at home. This means someone at the school/setting may be able to see and/or check my online activity when I use school devices/accounts and/or networks if they are concerned about my or anyone else's safety or behaviour.

- If, for any reason, I need to bring a personal device, for example a smart/mobile phone and/or other wearable technology into school then I will leave it securely at the school office and collect it at the end of the day.
- I know that I am not allowed on personal email, social networking sites or instant messaging in school.
- If I bring in memory sticks from outside of school, I will always give them to my teacher so they can be checked for viruses and content before opening them.
- I will protect myself by not telling anyone I meet online my address, my telephone number, my school/setting name or by sending a picture of myself without permission from a teacher or other adult.
- I will not arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- If I get unpleasant, rude, or bullying emails or messages, I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.
- I will always check before I download software or data from the internet. I know that information on the internet may not be reliable, and it sometimes needs checking.
- I have read and talked about these rules with my parents/carers.
- I can visit www.ceopeducation.co.uk and www.childline.org.uk to learn more about being safe online.
- I know that if I do not follow the Mersham Primary School rules then:
- I will be moved on the traffic lights according to the behaviour policy
- Shortened KS2 version (for use on posters)
- I ask a teacher about which websites I can use.
- I will not assume information online is true.
- I know there are laws that stop me copying online content.
- I know I must only open online messages that are safe. If I am unsure, I will not open it without speaking to an adult first.
- I know that people online are strangers and they may not always be who they say they are.
- If someone online suggests meeting up, I will always talk to an adult straight away.
- I will not use technology to be unkind to people.
- I will keep information about me and my passwords private.
- I always talk to an adult if I see something which makes me feel worried or uncomfortable.

KS2 Acceptable Use Poster



Appendix 3 - Parent/Carers Acceptable Use Policy

1. I have read and discussed the Acceptable Use Policy (attached) with my child.
2. I understand that the AUP applies to my child's use of Mersham Primary School devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another child, could have repercussions for the orderly running of the school, if a child is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.
3. I understand that any use of school devices and systems are appropriately filtered; this includes weekly filtering and monitoring reports of blocked content and searches. Monitoring approaches are in place to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
4. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use school devices and systems, on and offsite. I however understand that the school cannot ultimately be held responsible for filtering breaches that occur due to the dynamic nature of materials accessed online.
5. I am aware that the school mobile and smart technology policy states that my child cannot use personal devices, including mobile and smart technology on site.
6. I understand that my child needs a safe and appropriate place to access remote/online learning, for example, if the school is closed. I will ensure my child's access to remote/online learning is appropriately supervised and any use is in accordance with the school's remote learning AUP.
7. I, and my child are aware of the importance of safe online behaviour and will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the school community, or content that could adversely affect the reputation of the school.
8. I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety online.
9. I will inform the school/setting (for example speaking to a member of staff and/or the Designated Safeguarding Lead) or other relevant organisations if I have concerns over my child's or other members of the school community's safety online.
10. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.
11. I understand my role and responsibility in supporting the school's online safety approaches and safeguarding my child online. I will use parental controls, supervise access and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.
12. I am aware that the Mersham Primary School mobile technology policy states that my child cannot use personal devices and mobile technology on site. The school takes no responsibility for any mobile devices brought on site. *Any mobile device brought into school must be left in the school office.*
13. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Child's Name..... Child's Signature ..... (***if appropriate***)

Class..... Date.....

Parents Name.....

Parents Signature..... Date.....

Appendix 4 - Acceptable Use of Technology for Staff, Visitors and Volunteers

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Mersham Primary School IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for learners, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand Mersham Primary School expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that Mersham Primary School systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy Scope

I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Mersham Primary School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies.

I understand that Mersham Primary School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the Mersham Primary School staff code of conduct and remote learning AUP (see below)

I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the Mersham Primary School ethos, Mersham Primary School code of conduct and safeguarding policies, national and local education and child protection guidance, and the law.

Use of Mersham Primary School Devices and Systems

1. I will only use the equipment and internet services provided to me by Mersham Primary School for example laptops, tablets, mobile phones, and internet access, when working with children or completing training assigned to me as part of my role.
2. I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff. Personal use of setting IT systems and/or devices by staff is not allowed unless previously agreed by the headteacher.
3. Where I deliver or support remote learning, I will comply with the Mersham Primary School remote learning AUP. (see below)

Data and System Security

4. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
    a. I will use a 'strong' password to access Mersham Primary School systems. A strong password has numbers, letters and symbols, with 8 or more characters.
    b. I will protect the devices in my care from unapproved access or theft. For example not leaving devices visible or unsupervised in public places.
5. I will respect Mersham Primary School system security and will not disclose my password or security information to others.
6. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT technician.
7. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the Headteacher/IT technician.

8. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the Mersham Primary School information security policies.

a. All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.

b. Any data being removed from the Mersham Primary School site, such as via email or on memory sticks, will be suitably protected. This may include data being encrypted by a method approved by the school. i.e. password protected.

c. Any data being shared online, such as via cloud systems or artificial intelligence tools (AI), will be suitably risk assessed and approved by the school Data Protection Officer and leadership team prior to use to ensure it is safe and legal.

9. I will not keep documents which contain Mersham Primary School related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the Mersham Primary School learning platform to upload any work documents and files in a password protected environment.
10. I will not store any personal information on the Mersham Primary School IT system, including Mersham Primary School laptops or similar devices issued to members of staff that are unrelated to Mersham Primary School activities, such as personal photographs, files or financial information.
11. I will ensure that Mersham Primary School owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
12. I will not attempt to bypass any filtering and/or security systems put in place by the school.
13. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the IT Technician (NCS) as soon as possible.
14. If I have lost any Mersham Primary School related documents or files, I will report this to the IT Technician (NCS) and the Headteacher (to report to the Mersham Primary School Data Protection Officer) as soon as possible.
15. Any images or videos of learners will only be used as stated in the Mersham Primary School camera and image use policy.
    a. I understand images of learners must always be appropriate and should only be taken with Mersham Primary School provided equipment and taken/published where learners and their parent/carer have given explicit consent.

Classroom Practice

16. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by Mersham Primary School as detailed in the child protection, social media and online safety policy, and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.
17. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL), in line with the school's child protection and online safety policy.
18. I have read and understood the Mersham Primary School mobile technology and social media policies.
19. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in the child protection, online safety and remote learning AUP.
20. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I also recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material. Additionally, its use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that the use of AI as part of our education/curriculum approaches is permitted by staff only.
    a. A risk assessment will be undertaken, and approval will be sought from the senior leadership team prior to any use of AI tools (for example if used in the classroom, or to support lesson planning or assessments).

b. Any misuse of AI will be responded to in line with relevant school policies, including but not limited to, anti-bullying, staff and pupil behaviour and child protection.

21. I will promote online safety with the learners in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    a. Exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
    b. Creating a safe environment where learners feel comfortable to say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    c. Involving the Designated Safeguarding Lead (DSL) (Cheryl Chalkley) or a deputy (Leah Benjamin, Lindsay Wheeler) as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
    d. Make informed decisions to ensure any online safety resources used with learners is appropriate.
22. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the Mersham Primary School child protection policies.
23. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

Mobile Devices and Smart Technology

24. I have read and understood the Mersham Primary School Mobile Technology and Social Media Policy which covers expectations regarding staff and pupil use of mobile technology and social media.
25. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff behaviour policy/code of conduct and the school mobile technology policy and the law.

Online Communication, including use of Social Media

26. I will ensure that my online reputation and use of mobile devices, smart technology, IT and information systems are compatible with my professional role and in line with the staff code of conduct, when using Mersham Primary School and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.
    a. I will take appropriate steps to protect myself online when using social media as outlined in the online safety policy
    b. I am aware of the Mersham Primary School expectations with regards to use of personal devices and mobile technology, including mobile phones as outlined in the mobile technology policy.
    c. I will not discuss or share data or information relating to learners, staff, Mersham Primary School business or parents/carers on social media.
    d. I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the Mersham Primary School code of conduct and the law.
27. My electronic communications with current and past learners and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
    a. I will ensure that all electronic communications take place in a professional manner via Mersham Primary School approved and/or provided communication channels and systems, such as a Mersham Primary School email address, user account or telephone number.
    b. I will not share any personal contact information or details with learners, such as my personal email address or phone number.
    c. I will not add or accept friend requests or communications on personal social media with current or past learners and/or parents/carers.
    d. If I am approached online by a learner or parents/carer, I will not respond and will report the communication to the Headteacher/Designated Safeguarding Lead (Cheryl Chalkley).
    e. Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the Headteacher.

Policy Concerns

28. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.
29. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.
30. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the Mersham Primary School into disrepute.
31. I will report and record any concerns about the welfare, safety or behaviour of pupils or parents/carers online to the DSL in line with the school child protection policy.
32. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with school child protection policy and/or the allegations against staff policy.

Policy Compliance and Breaches

33. If I have any queries or questions regarding safe and professional practice online, either in school or off site, I will raise them with the DSL.
34. I understand that the school may exercise its right to monitor the use of its devices' information systems to monitor policy compliance and to ensure the safety of pupils and staff. This includes monitoring all school provided devices and school systems and networks including school provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
35. I understand that if the school believes that unauthorised and/or inappropriate use of school devices, systems or networks is taking place, the school may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.
36. I understand that if the school believes that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.
37. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with Mersham Primary School's Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member: .....

Signed: .....

Date: .....

Appendix 5 - Visitor and Volunteer Acceptable Use of Technology Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy. This is not an exhaustive list and visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

Policy Scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school or accessed by me as part of my role within Mersham Primary School, professionally and personally. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email. data and data storage, remote learning systems and communication technologies.
2. I understand that Mersham Primary School's AUP should be read and followed in line with the school staff behaviour policy/code of conduct and the Visitor/Volunteer Induction Booklet.
3. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.
4. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.
5. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.
6. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

Data and Image Use

7. I understand that I am not allowed to take images or videos of pupils.

Classroom Practice

8. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of pupils.
9. I will support and reinforce safe behaviour whenever technology is used on site, and I will promote online safety with the pupils in my care.
10. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the school community, I will report this to the DSL/Headteacher in line with the school child protection/online safety policy.
11. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

Use of Mobile Devices and Smart Technology

12. In line with the school mobile and smart technology policy, I understand that mobile phones and devices are not permitted in classrooms when children are present.

Online Communication, including the use of Social Media

13. I will ensure that my online reputation and use of technology is compatible with my role within the school. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
    a. I will take appropriate steps to protect myself online as outlined in the child protection/online safety/social media policy.
    b. I will not discuss or share data or information relating to children/pupils/students, staff, school business or parents/carers on social media.

c. I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the school code of conduct/behaviour policy and the law.

14. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    a. All communication will take place via school approved communication channels such as via a school provided email address, account or telephone number.
    b. Communication will not take place via social networking accounts or mobile phone numbers.
    c. Any pre-existing relationships or situations that may compromise my ability to comply with this will be discussed with the DSL (Cheryl Chalkley - Headteacher)

Policy Compliance, Breaches or Concerns

15. If I have any queries or questions regarding safe and professional practice online either in school or off site, I will raise them with the Designated Safeguarding Lead (Cheryl Chalkley) and/or the headteacher.
16. I will report and record concerns about the welfare, safety or behaviour of pupils or parents/carers online to the Designated Safeguarding Lead (Cheryl Chalkey) in line with the school child protection policy.
17. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with the allegations against staff policy.
18. I understand that if the school believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.
19. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with Mersham Primary School's visitor/volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer: .....

Signed: .....

Date: .....