

Mapledown School



Working and Learning Together

E- and Online Safety

Name of School	Mapledown School
This policy was reviewed on	2nd September 2021
This policy was reviewed on	September 2022 November 2023
The policy is to be reviewed in	November 2024

This policy should be read in conjunction with the following regulations and documents:

- (i) Data protection Act 2018
- (ii) The UK GDPR as amended and brought into UK law by the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc.)(EU Exit) Regulations 2019 and subsequent regulation.
- (iii) Computer Misuse Act 1990
- (iv) Freedom of Information Act 2000
- (v) The school's Safeguarding policy

Abbreviations: CEOP (Child Exploitation and Online Protection Center)

<http://ceop.police.uk/>

DfE (Department for Education)

ICT (Information Communications Technology)

SEN (Children with special educational needs)

GAFE (Google Apps for Education)

<u>Contents</u>
Development of this policy
Schedule for Monitoring & Review
Scope of this Policy
Preface
Legal Framework
What is Google Workspace for Education
Google Workspace for Education security
Introduction
Internet Use
Internet Use for Children and Young People with SEN
Roles and Responsibilities
Policy and Statements
Education – Policy
Technical -infrastructure/equipment, filtering and monitoring
Password security
Use of digital and video images
Data Protection
Communications
Social Media- Protecting Professional Identity
Unsuitable/ inappropriate activities
Published content on the school website
Mobile devices and hand-held computers
Online safety Audit - Mapledown school

Development of this Policy

This online safety policy has been developed by a working group made up of:

- IT lead
- Head teacher

Schedule for Monitoring & Review

This online safety policy was approved by the Health and safety Committee on:	
The implementation of this online safety policy will be monitored by the	Senior Leadership Team and Learning Zone Leads
Monitoring will take place at regular intervals:	Date for review: Annually
Should serious online safety incidents take place, the following external persons/agencies should be informed	LA safeguarding officer, police

Scope of this Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the school ICT systems, both in and out of the school.

Preface

At Mapledown School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives. We take Internet Safety very seriously and see it as our duty to keep our pupils safe whilst using technology not only in school but also at home.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to mitigate the risk of harm.

This Policy has been rewritten with the introduction of Google Workspace for Education at Mapledown School.

Google Workspace for Education was rolled out across Mapledown School during August 2021..

This policy has been further updated in line with the requirements of the new data protection regulations following Brexit, to include further information on consent, data security and the responsibilities of the data protection officer (DPO). The updated policy also includes reference to the 2023 version of Keeping Children Safe in Education (see appendix).

Legal framework:

- 1.1. This policy has due regard to all relevant legislation including, but not limited to:
 - The UK General Data Protection Regulation
 - The Data Protection Act 2018

- Freedom of Information Act 2000
- 1.2. This policy also has regard to the following statutory guidance:
- DfE (2023) 'Keeping children safe in education'
 - National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- 1.3. This policy will be used in conjunction with the following school policies and procedures:
- Cyber and Information Security Policy
 - Access Control Policy
 - Allegations of Abuse Against Staff Policy
 - Acceptable Use Policy
 - Data Protection and Security Incident Reporting Procedure

What is Google Workspace for Education?

Google Workspace for Education, formerly known as Google Suite for Education, is a core suite of productivity applications that Google offers to schools and educational institutions. These communication and collaboration apps include Gmail, Calendar, Drive, Docs and Sites, and a Google Workspace account that unlocks access to dozens of other collaborative tools supported by Google. All of these applications exist completely online (or in the cloud), meaning that all creations can be accessed from any device with an Internet connection. The School can administer all teacher and Pupil (if appropriate) accounts from an administrative dashboard. The school is less reliant on the infrastructure of servers as the majority of our everyday data is securely cloud-based.

Google Workspace for Education Security:

All teachers have been issued with Chromebooks. Staff are responsible for ensuring they log out and disconnect at the end of a session, and for the security of passwords and document sharing. No pupil specific information may be shared outside of Mapledown's domain without the express permission of the Headteacher.

An independent third party auditor issued Google Apps an unqualified SSAE 16 and ISAE 3402 Type II

http://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu_en_isae3402-ssae16_04072014.pdf) Organization and administration: Controls provide reasonable assured audit opinion. The independent third party auditor verified that Google Apps has the following controls and protocols in place:

Logical security: Built in Controls provide reasonable assurance that logical access to Google Apps production systems and data is restricted to authorized individuals

Privacy: Controls provide reasonable assurance that Google has implemented policies and procedures addressing the privacy of customer data related to Google Apps

Data center physical security: Controls provide reasonable assurance that data centers that house Google Apps data and corporate offices are protected

Incident management and availability: Controls provide reasonable assurance that Google Apps systems are redundant and incidents are properly reported, responded to, and recorded.

Change management: Controls provide reasonable assurance that development of and changes to Google Apps undergo testing and independent code review prior to release into production

Introduction

Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Downloading from the Internet
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Internet Use

The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.

When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including the following:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. content involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

Internet Use for Children and Young People with SEN

Mapledown School recognises that Children with SEN are potentially more vulnerable and more at risk than others when using ICT. At Mapledown School we understand the responsibility to educate our pupils in online safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Curriculum Committee receiving regular information about online safety incidents and monitoring reports.

A member of the Curriculum Committee has taken on the role of online safety Governor.

The role of the online safety Governor will include:

- *meetings with the online safety Coordinators (Daniel Green and Sandra Chaaya)*
- *regular monitoring of filtering/change control logs*
- *reporting to relevant Governors committee meetings*

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of

members of the school community.

- The Headteacher and Senior Leadership Team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents-included in a later section- “Responding to incidents of misuse” and relevant Local Authority HR disciplinary procedures). In the event that illegal material is found on the school’s network, or evidence suggests that illegal material has been accessed, the police will be contacted. If a child protection incident is suspected, the school’s child protection procedure will be followed , and social care/the police will be contacted.
- The Headteacher/Senior Leaders are responsible for ensuring they and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher/Senior Leaders share regular monitoring reports from the online safety coordinator.
- The Headteacher and Data Protection Officer (DPO) ensure there is a system in place which monitors and supports the Online safety Coordinator whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.
 - The headteacher will review and amend this policy with the e-safety officer and DPO, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
 - The headteacher is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

Online safety Coordinator (Daniel Green - technical, Sandra Chaaya - all other areas)

- takes day to day responsibility for online safety issues
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and will keep a log of all incidents reported
- provides training and advice for staff
- Liaises with Local Authority /relevant body
- attends online safety training
- monitors online safety issues and the provision of e-safety in school, as well as provide feedback to the headteacher
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with online safety governor to discuss current issues, review incident logs and filtering/change controls logs
- reports regularly to Senior Leadership Team.
- ensures the school’s technical infrastructure is secure and is not open to misuse or malicious attack
- ensure the school meets required online safety technical requirements through a properly enforced password protection policy
- ensures the filtering is applied and updated on a regular basis
 - ensures access is regularly monitored in order that any misuse/attempted misuse can be reported for investigation and action

- ensures software and systems are implemented and updated as agreed.
- attempts to find alternatives to monitoring staff use of social media, where possible, and will justify all instances of monitoring to ensure that it is necessary and outweighs the need for privacy. The member of staff who is being monitored will be consulted prior to any interception by the school.

Teaching and Support Staff

are responsible for ensuring that

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they report any suspected misuse or problem to the online safety coordinator for investigation
- all digital communication with students, pupils, parents, carers is at a professional level
- online safety issues are embedded in all aspects of the curriculum and other activities
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use; that processes are in place for dealing with any unsuitable material that is found in internet searches.
- they understand and adhere to our Acceptable Use Policy
- they will not view or forward any illegal materials, including images of a child. If they are made aware of such an image, they will contact a Designated Safeguarding Lead.

Designated Safeguarding Leads

are aware of online safety issues and are aware of the potential for serious child protection and safeguarding issues to arise from

- sharing of personal data of any individual at the school
- access to illegal materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Students

Where appropriate, pupils should:

- understand the importance of reporting abuse, misuse or access to inappropriate materials and be taught how to do this.
- know and understand safe practice on the use of mobile devices and digital cameras. They should also be taught to understand how to stay safe around taking/use of images and regarding cyber-bullying

Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' meetings, newsletters, and through our website. Parents and families will be encouraged to support the school in promoting good

online safety practice and follow guidelines on the appropriate use of:

- digital and video images taken as school events
- their children's personal devices in the school

Policy and Statements

Education - students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus across the curriculum and staff should reinforce online safety messages.

- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Students should be taught how to safely use technology both inside and outside the school if appropriate
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites that young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that normally result in internet searches being blocked. In such a situation, staff can request the online safety coordinator can temporarily remove those sites from the filtered list for a period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education - parents

Some parents and carers may have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviour. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website
- Parents/carers sessions

Technical - infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure is as safe and secure as reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school systems
- Wireless systems and cabling must be securely located and physical access restricted
- The administrator passwords for the school ICT system must also be available to the Headteacher and kept securely.
- The IT coordinator is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider. Content lists are regularly updated and Internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- IT coordinator regularly monitors and records activity of users on the school technical systems
- Users are aware of the need to report any actual or potential technical incident or security breach to the IT coordinator
 - Appropriate security measures are in place to protect the learning platform, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
 - An agreed process is in place for the provision of temporary access of “guests” onto the school systems.
 - The school uses secure broadband connectivity through the London Grid for Learning.
 - The school uses the LGfL webscreen filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved ‘web filtering management’ status
 - The School uses LGfLmail and Google Workspace email to send personal data over the Internet and uses secure remote access where staff need to access personal level data off-site
 - The School provides staff with an email account for their professional use, and makes clear personal email should be through a separate account
 - Works in partnership with Google to ensure any concerns about the system are communicated so that systems remain robust and protect students
 - Ensures the Systems Administrator / network manager is up-to-date with Google services and policies Managing emerging technologies
 - Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
 - The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material.
 - The sending of abusive or inappropriate text messages or emails is forbidden.
 - Staff will use a school phone where contact with families is required.

Password Security

- Adult users are provided with an individual Google Workspace username and password, email address and password, which they are encouraged to change periodically, with a 2 step verification process through the use of the Authenticator App
- All members of staff are aware of their individual responsibilities to protect the security and confidentiality of the school network systems.
- Use of USB memory sticks must be approved by the school and encrypted for sensitive data.

Use of digital and video images

Staff, parents/carers and students are made aware of the risks associated with publishing digital images on the Internet. Such images may provide avenues for cyber-bullying to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff should recognise the risks attached to publishing their own images on the Internet e.g. social networking sites.
- Parents and families are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and, in some cases, protection, these images should not be published or made publicly available on social networking, nor should parents and families comment on any activities involving other students in the digital/ video images.
- Staff, students and volunteers are allowed to take digital / video images to support educational aims, but must follow school policy concerning the sharing, distribution and publication of those images, in line with GDPR
- Care should be taken when taking digital /video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students' full names will not be used anywhere on a website.
- Parents and carers must give permission before a student's photographs are published on the school website.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the data protection regulations which include the following principles (adapted from UK GDPR Article 5) stating that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary
- Processed in a manner that ensures appropriate security

The school must ensure that

:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for;
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay;
- Has a Data Protection Policy
- Data subjects have their rights respected

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse;
- use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged off” at the end of any session in which they are using personal data;
- Transfer data using encryption and secure password protected devices.
- Keep personal devices safe. Staff who receive work emails on personal devices are responsible for the data security. These devices must be protected by passwords
- Staff must report any breach to security to the online safety officer (Daniel Green) who will report to Headteacher (Sandra Chaaya)
- It is a legal requirement to record all breaches. The LEA performs this on our behalf, and provides a Data Protection Officer who should be consulted immediately on any breach so that the legal obligation to report serious breaches to the ICO within 72 hours can be managed. The DPO is available at weekends and outside term time.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus protection
- the data must be securely deleted from the device

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. User should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems. School email accounts must not be used for personal purposes.
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers (email, etc) must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media

must not be used for these communications. The use of personal email accounts to send and receive information or personal data is prohibited

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Social Media- Protecting Professional Identity

Staff should ensure that:

- No reference should be made in social media to students, parents/cares or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- They do not communicate with pupils over social networking sites and are reminded to alter their privacy settings

The school's use of social media for professional purposes will be checked regularly by the online safety committee to ensure compliance.

Unsuitable/ inappropriate activities

School devices and school network must not be used for any illegal activities. All staff have a responsibility to report any misuse of school devices and network to the Headteacher who will report incidents to the Local Authority Designated Officer and the police.

Published content on the school website:

- The headteacher will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.
- Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully and will not be posted until and unless authorisation from parents has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take pictures, though they must do so in accordance with our data protection policy. Staff will not take pictures using their personal equipment.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

Mobile devices and hand-held computers

- Staff are permitted to use hand-held computers (such as tablets or iPads) which have been provided by the school, though internet access will be monitored for any inappropriate use by the Online safety Coordinator where it is justifiable to do so and the justification outweighs the need for privacy.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Personal mobile devices will not be used to take images or videos of pupils or staff.
- No mobile device or hand-held computer owned by the school will be used to access public Wi-Fi networks.
- The DPO will, in collaboration with the Online safety Coordinator, ensure all school-owned devices are password protected to ensure their security.

- Mobile devices and hand-held computers will be fitted with tracking software to ensure they can be retrieved if lost or stolen.
- To protect, retrieve and erase personal data, mobile devices and hand-held computers will be fitted with software to ensure they can be remotely accessed.
- The Online safety coordinator will review and authorise any apps and/or computer programmes before they are downloaded – no apps or programmes will be downloaded without express permission
- Apps will only be downloaded from manufacturer approved stores, e.g. Google Play and the Apple App Store.

Online safety Audit

This self-audit has been completed by the members of the Senior Leadership Team (SLT) responsible for the online safety policy, the IT Manager, the DPO and the Headteacher.

Has the school an online safety Policy that complies with Local Authority guidance?	Yes
Date of latest update (at least annual):	November 2023
The policy is available for staff at:	Google Drive policies
The policy is available for parents/carers at:	school website
The responsible member of the SLT is:	Sandra Chaaya
The responsible member of the Governing Body:	Sue O'Halloran
The Designated Child Protection Coordinator is:	Sandra Chaaya / Sue Hart
The online safety Coordinator is:	Daniel Green
Has online safety training been provided for both pupils and staff?	Yes
Is there a clear procedure for a response to an incident of concern?	Yes
Have online safety materials from CEOP been obtained?	Yes
Do all staff sign a Code of Conduct for ICT on appointment?	Yes
Are all pupils aware of the Schools online safety Rules?	Pupils require staff support and supervision
Are online safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Yes
Do parents/carers sign and return an agreement that their child will comply with the School online safety Rules?	Student Admission form requires parental response re: home supervision & parental control
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Yes

Has an ICT security audit been initiated by SLT?	Yes
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Yes
Has the school-level filtering been designed to reflect educational objectives and approved by SLT	Yes

APPENDIX 1

Acceptable Use Agreement 2023-24

Whilst our school promotes the use of technology or devices, and understands the positive effects they can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology and devices appropriately. Any misuse of technology and devices will not be taken lightly and will be reported to the headteacher in order for any necessary further action to be taken.

This agreement outlines staff members' responsibilities when using technology and devices, both school-owned and personal, and applies to all staff, volunteers, contractors and visitors.

Please read this agreement carefully, and sign at the bottom to show you agree to the terms outlined.

Data protection and cyber-security

I will:

- Use technology and devices, including the use and storage of personal data, in line with data protection legislation, including the Data Protection Act 2018 and UK GDPR.
- Follow the school's E-Safety Policy and Data Protection Policy and any other relevant school policies and procedures.
- Report immediately any accidental loss of personal or sensitive school data so that appropriate action can be taken.

I will not:

- Attempt to bypass any filtering, monitoring and security systems.
- Attempt to upload school data onto any unauthorised platforms.
- Share school-related passwords with staff, parents or others unless permission has been given for me to do so.

Using technology in school

I will:

- Only use ICT systems which I have been permitted to use.

- Ensure I obtain permission prior to accessing materials from unapproved sources.
- Only use the internet for personal use during out-of-school hours, including break and lunch time.
- Report any accidental access to material which might be considered unacceptable immediately to the ICT technician and ensure it is recorded.
- Only use removable media approved by the school and keep this securely stored.

I will not:

- Install any software onto school ICT systems unless instructed to do so by the ICT technician.
- Search for, view, download, upload or transmit any inappropriate material when using the internet.

Emails

I will:

- Only use the approved school email accounts that have been provided to me when sending communications regarding school business.
- Ensure any personal information that is being sent via email is only sent to the relevant people and is appropriately protected.
- Ensure that sensitive data is sent only via approved secure file transfer systems such as Egress and USO-FX.

I will not:

- Use personal emails to send and/or receive school-related personal data or information, including sensitive information.
- Use personal email accounts to contact pupils or parents.

School-owned devices

I will:

- Only use school-owned or approved devices for the purpose of carrying out my school responsibilities.
- Only access websites and apps that have been approved by the school.
- Understand that the usage of my school-owned devices may be monitored.
- Keep my school-owned devices with me or within my sight at all times.
- Transport school-owned devices safely.
- Provide suitable care for my school-owned devices at all times.
- Only communicate with pupils and parents on school-owned devices using appropriate channels.
- Ensure I install and update security software on school-owned devices as directed by the ICT technician.
- Use only a school-owned device to take and store photographs or videos of pupils, parents, staff and visitors.

- Immediately report any damage or loss of my school-owned devices to the ICT technician.
- Immediately report any security issues, such as downloading a virus, to the ICT technician.
- Understand that I am expected to pay an excess for any repair or replacements costs where the device was damaged or lost as a result of my own negligence.
- Make arrangements to return school-owned devices to the ICT technician upon the end of my employment at the school.

I will not:

- Permit any other individual to use my school-owned devices without my supervision, unless otherwise agreed by the headteacher or ICT technician.
- Install any software onto school-owned devices unless instructed to do so by the ICT technician.
- Use school-owned devices to send inappropriate messages, images, videos or other content.
- Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content.
- Use school-owned devices to access personal social media accounts.

Personal devices

I will:

- Only use personal devices during out-of-school hours and non-teaching time, including break and lunch times.
- Only use personal devices onsite within the designated areas permitted for staff: school office, staffroom and resources room, unless prior permission has been granted by the headteacher for the purpose of receiving an urgent phone call.
- Ensure personal devices are either switched off or set to silent mode during school hours.
- Store personal devices appropriately during school hours, e.g. a lockable cupboard in the classroom.
- Understand that I am liable for any loss, theft or damage to my personal devices.

I will not:

- Use personal devices to communicate with pupils or parents. The **only** exception is an **emergency** situation when no other option is available, such as accompanying a student to hospital. In this instance, I will **inform the headteacher** about my use of a personal device.
- Use personal devices to take photographs or videos of pupils, even in an emergency. There is **no exception** to this rule. Any recordings of pupils are **only permitted on school devices**.
- Use personal devices to take photographs or videos of staff **during working hours**.
- Access the school's Wi-Fi using a personal device unless permission to do so has been granted by the ICT technician.
- Store any school-related information on personal devices unless permission to do so has been given by the headteacher.

Social media and online professionalism

I will:

- Understand that I am representing the school and behave appropriately when posting on school social media accounts.
- Ensure I apply necessary privacy settings to social media accounts.

I will not:

- Communicate with pupils or parents over personal social media accounts.
- Accept 'friend' or 'follow' requests from any pupils or parents over personal social media accounts.
- Post any comments or posts about the school on any social media platforms or other online platforms which may affect the school's reputability.
- Post any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- Post or upload any images and videos of pupils, staff or parents on any online website without consent from the individuals in the images or videos.
- Give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

Working from home or off-site

I will:

- Access school data on my personal or school device only via my mobile data, home Wi-Fi or trusted Wi-Fi network.
- Ensure I obtain permission from the headteacher or ICT technician before any school data is made accessible on a personal device.
- Ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- Ensure my personal device has been assessed for security by the ICT technician before it is used for home.
- Ensure that my access to confidential school information, pupil information or data is via a device which is encrypted or protected with a strong password.
- Take all reasonable steps to ensure the safety and security of school IT equipment which I take off-site and will remove anything of a personal nature before it is returned to school.
- Take all reasonable steps to ensure that personal devices are fully virus-protected and that protection is kept up to date.
- Ensure no unauthorised persons, such as family members or friends, access my personal device while I am working from home.
- Ensure that my computer has a password-protected screensaver and that any devices used for school work (including Chromebooks) are fully logged off, shut down or screen-locked before being left unattended.

I will not:

- Access school data on my personal or school device over public Wi-Fi, e.g. shopping centres, coffee shops, airports, trains, hotels and internet cafes.

Training

I will:

- Participate in any relevant training offered to me, including cyber-security and online safety.
- Allow the school to undertake audits to identify any areas of need I may have in relation to training.
- Employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.

Reporting misuse

I will:

- Report any misuse by staff members or pupils breaching the procedures outlined in this agreement to the headteacher.
- Understand that my use of the internet may be monitored by the ICT technician and recognise the consequences if I breach the terms of this agreement.
- Understand that the headteacher may decide to take disciplinary action against me if I breach this agreement.

Agreement

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Name	
Signature	
Date	

Appendix 2

KCSIE & DfE 2023 Updates

[Keeping children safe in education 2023 \(publishing.service.gov.uk\)](https://publishing.service.gov.uk)

14 - New text added to raise awareness of the existing expectation for relevant staff to understand filtering and monitoring.

103 - Added reference to filtering and monitoring.

124 - New text added to make clear staff training should include understanding roles and responsibilities in relation to filtering and monitoring.

138 - Reference to child protection policies and appropriate filtering and monitoring on school devices and school networks.

142 - Added new section referencing the new published filtering and monitoring standards. The standards are to support schools to meet their duty to have appropriate/effective filtering and monitoring systems in place.

144 - Reference to cyber security standards.

221 (Footnote) - Clarification that it is good practice for schools to inform shortlisted candidates that online searches will be carried out.

The senior leadership team are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Senior leaders will work closely with governors, the designated safeguarding lead (DSL) and ICT Support in all aspects of filtering and monitoring.

The DSL works closely with ICT Support to meet the needs of our setting. The DSL takes lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

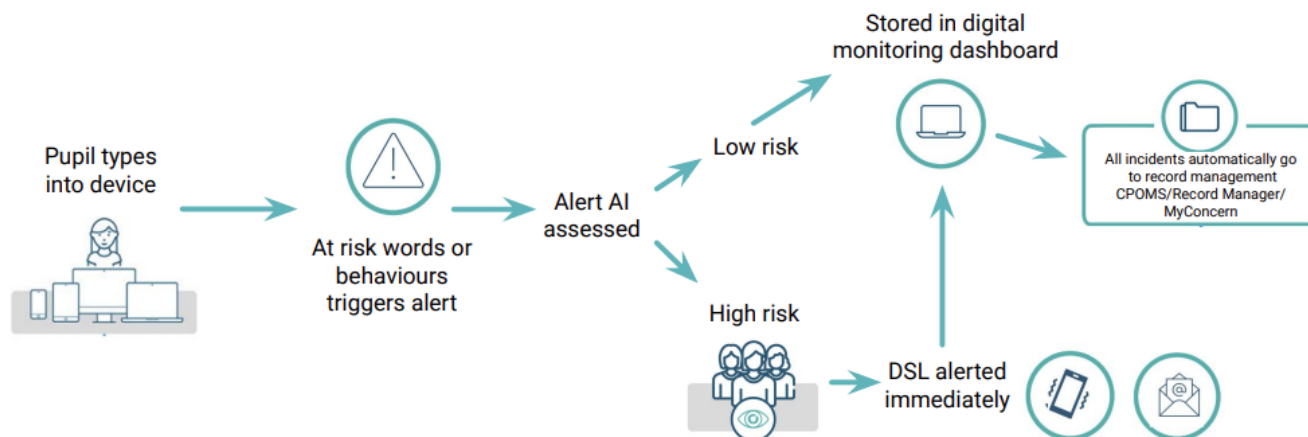
ICT Support has technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

ICT Support works with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews and checks

Digital monitoring - how it works



Appendix 3

Web Monitoring

Online monitoring is about observing and tracking our school community's digital activities, including web browsing, social media interactions and chat conversations. It aims to identify potential risks and rule violations and raise alerts that can be acted on. Systems will also help in monitoring device usage by staff and students. When combined, filtering and monitoring can help you to take a comprehensive approach to online safeguarding.

- The DSL assumes primary responsibility for safeguarding and online safety, which includes overseeing and responding to:
- Filtering and monitoring reports
- Safeguarding concerns
- Checks on filtering and monitoring systems on different devices around the school and different users

The IT Manager holds technical responsibility for:

- Maintaining filtering and monitoring systems
- Providing filtering and monitoring reports
- Taking appropriate actions following concerns or system checks

Filtering and Monitoring at Mapledown School - Information for staff

Mapledown subscribes to Classroom Cloud, a monitoring service that helps enhance our school's safeguarding policy.

The service is being rolled out across a range of school devices, including PCs, Chromebooks and iPads. This is in keeping with the requirements concerning filtering and monitoring as outlined in the KCSIE 2023 guidance for schools.

Filtering is about protecting us from the outside world – a network defence that safeguards us by filtering out the dangers of the internet.

Monitoring is about protecting us from within – a service that inspects our usage of school devices to ensure that staff and students are acting safely, appropriately and in accordance with our E-Safety and Acceptable Use Policies.

In our school, the most effective **student** monitoring is performed by staff members who work with students in class on a daily basis. Classroom staff have a responsibility to monitor students' activity on the internet at all times, especially those who are able to navigate around sites such as YouTube on an iPad.

Classroom Cloud provides further monitoring support by keeping a check on our device activity.

Using a database of pre-supplied safeguarding keywords and phrases (in a range of languages) covering a range of topics from self-harm, bullying and racism through to risks of radicalisation and gambling, Classroom Cloud is our eyes and ears, monitoring the school network.

We can monitor, review and respond to the words and phrases typed/searched by staff and students on school devices that match with the keyword libraries in Classroom Cloud.

Classroom Cloud may provide a log, screenshot or screen recording of triggered words and searches. These results enable us to see the context behind the words that we type. For instance, if you search for 'relaxation music' on YouTube, and the page contains the term 'stress relief', then the word 'stress' may be flagged up as a possible sign of emotional distress. However, we can identify the many false alarms we receive by looking at the results of the logs and screenshots taken.

So, to be clear, school devices are filtered and monitored. For your own privacy, you may wish to avoid accessing your private email or online services on a school device in case it flags up a concern to us. Use your mobile to access your personal data.

Personal devices are not monitored by the school! Although staff are *still* subject to the Acceptable Use Policy concerning personal devices within school, your activity remains private to you.

For those who are using the school Wi-Fi in the staff room, your personal devices will be subject to filtering on the school network, but not monitoring. The filtering service may block your device from accessing particular content online or social media platforms. If you wish to avoid the restrictions of school filtering over Wi-Fi, please use your own mobile data instead.

The bottom line is this – If you are following our Acceptable Use Policy, which we must all sign and abide by, you have nothing to worry about. And if you stick to accessing your personal data on your personal device, your data remains private to you. These systems are about safeguarding our students and our staff, and as with all discussions related to safeguarding, it is the most important thing that we do.

If you have any questions or concerns please speak with Sue Hart and Daniel Green