MAYVILLE HIGH SCHOOL
Founded in 1897

E-SAFETY POLICY

Introduction

It is the duty of Mayville High School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles;
- Mobile internet devices such as smart phones and tablets.

This policy, supported by the Acceptable Use Policy (Annex B) (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding (incl. child on child abuse)
- Staff Behaviour Management Policy;
- Health and Safety;
- Behaviour Management;
- Anti-Bullying;

- Prevent;
- Acceptable Use Policy;
- Data Protection;
- Bring Your Own Device; and
- PSHE

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact**: being subjected to harmful online interaction with other users; for example: child to child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 4G and 5G). This access means some children, whilst at school, could sexually harass other children via their mobile and smart technology, share indecent images: consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content. For this reason, mobile phones are not allowed to be accessed during the school day. All smart technology must be handed in to their tutor at the start of the school day and signed out prior to going home.

At Mayville High School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the Acceptable Use Policy (for all staff, visitors and pupils) cover both fixed and mobile internet devices provided by the school (such as Chromebooks, PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

Roles and responsibilities

1. The Trustee Board

The Trustee Board is responsible for the approval of this policy and for reviewing its effectiveness. The Board will review this policy at least annually.

The Trustee Board also have overall strategic responsibility for filtering and monitoring and ensuring the filtering and monitoring standards as set out by the Department for Education are met.

The E-Safety Trustee is Mrs T Riordan.

2. Headteacher and the Senior Management Team

The Headteacher is responsible for the safety of the members of the school community and this includes responsibility for e-safety. The Headteacher has delegated day-to-day responsibility to the Director of IT and the DSL.

The senior management team are responsible for making sure that all staff:

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

The Director of IT is responsible for:

- procuring filtering and monitoring systems
- ensuring this policy is upheld by all members of the school community, and works with IT staff to achieve this

The DSL is responsible for:

- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of the filtering and monitoring provision with regular checks (using a test pupil account and via testing software such as http://testfiltering.com/)
- overseeing and acting on filtering and monitoring reports
- safeguarding concerns

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL works closely with the Director of IT to ensure the system meets the needs of the school. Both will keep up to date on current e-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

The IT service provider (Matrix) and web filtering provider (Securely) has technical responsibility for:

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

4. IT staff

The school's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data. Training for staff is conducted by the Director and Assistant Director of IT. All use of the internet and emails is monitored and any inappropriate use is reported to the

Director of IT.

5. Teaching and support staff

All staff are required to sign the Staff Acceptable Use Policy before accessing the school's systems.

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

Staff have the responsibility to physically monitor pupils devices when being used in their classrooms and report any concerns to the Director of IT/ DSL.

All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

6. Pupils

Pupils are responsible for using the school IT systems in accordance with the Acceptable Use Policy, and for letting staff know if they see IT systems being misused.

7. Parents and carers

Mayville High School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. We also use parents' evening where we have a captive audience to promote online safety and give further advice. We also have videos that are sent to parents and carers on parental settings. There's also a page on the school's website where parents can log in to gain advice on how best to monitor social media platforms. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Parents and carers are responsible for endorsing the school's Pupil Acceptable Use Policy.

Filtering and monitoring

KCSIE 2024 obliges schools and colleges to "ensure appropriate filtering and monitoring systems are in place and regularly review their effectiveness". Pupils should not be able to access harmful or inappropriate content from the schools IT system. However, schools will need to be careful that over-blocking does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching practices and effective supervision.

1. The filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning

An effective filtering system needs to block internet access to harmful sites and inappropriate content. It

should not:

- unreasonably impact teaching and learning or school administration
- restrict students from learning how to assess and manage risk themselves

Our filtering provider (Securely) is:

- a member of Internet Watch Foundation (IWF)
- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- blocking access to illegal content including child sexual abuse material (CSAM)

Our filtering system is operational, up to date and applied to all users (including guest accounts); school owned devices; devices using the school broadband connection and personal devices owned by pupils who have signed up to BYOD (for which they must download Securely onto their device).

Our filtering system:

- filter all internet feeds, including any backup connections
- age and ability appropriate for the users, and be suitable for educational settings
- handles multilingual web content, images, common misspellings and abbreviations
- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- provides alerts when any web content has been blocked

It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the senior leadership team or the designated safeguarding lead.

- device name or ID and the individual login/ user
- the time and date of attempted access
- the search term or content being blocked

As a school we have decided to use Safe Search on our web browser to provide an additional level of protection for our users on top of the filtering service. Our firewall is provided by Bitdefender which additionally protects against viruses, malware etc.

2. There are effective monitoring strategies that meet the safeguarding needs of our school

Monitoring user activity on school devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software.

Monitoring allows us to review user activity on school devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing us to take prompt action and record the outcome.

Our monitoring strategy is informed by the filtering and monitoring review (conducted by the Director of IT and DSL). A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software

- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

The Trustee Board supports the senior leadership team to make sure effective device monitoring is in place which meets this standard and the risk profile of the school or college.

The designated safeguarding lead (DSL) will take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.

The management of technical monitoring systems require the specialist knowledge of both safeguarding and IT staff to be effective. Training is provided to make sure their knowledge is current. We use training provided by Matrix and Securely for system specific training and support.

Device monitoring is managed by IT staff, who:

- make sure monitoring systems are working as expected
- provide reporting on pupil device activity
- receive safeguarding training including online safety
- record and report safeguarding concerns to the DSL

Make sure that:

- monitoring data is received in a format that your staff can understand
- users are identifiable to the school or college, so concerns can be traced back to an individual, including guest accounts

Technical monitoring systems do not stop unsafe activities on a device or online. Staff should:

- provide effective supervision
- take steps to maintain awareness of how devices are being used by pupils
- report any safeguarding concerns to the DSL

Schools and colleges that have a technical monitoring system will need to conduct their own data protection impact assessment (DPIA) and review the privacy notices of third party providers. A DPIA template is available from the ICO.

3. We review our filtering and monitoring provision at least annually

The review is conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider (staff technician or external service provider) and involve the responsible Trustee. The results of the online safety review are recorded for reference and made available to those entitled to inspect that information.

A review of filtering and monitoring is carried out to identify our current provision, any gaps, and the specific needs of our pupils and staff.

We understand:

- the risk profile of our pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what our filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines

- any relevant safeguarding reports
- the digital resilience of our pupils
- our PSHE curriculum
- the specific use of our chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies we have in place
- what checks are currently taking place and how resulting actions are handled

To make our filtering and monitoring provision effective, our review informs:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

The review is done as a minimum annually, or when:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced

Checks are undertaken from both a safeguarding and IT perspective. A log of checks is recorded so they can be reviewed. The log will record:

- when the checks took place
- who did the check
- what they tested or checked
- resulting actions

We make sure that:

- all staff know how to report and record concerns
- filtering and monitoring systems work on new devices and services before releasing them to staff and pupils
- blocklists are reviewed and they can be modified in line with changes to safeguarding risks

We use South West Grid for Learning's (SWGfL) testing tool to check that our filtering system is blocking access to:

- illegal child sexual abuse material
- unlawful terrorist content
- adult content

Education and training

1. Staff: awareness and training

New teaching staff receive information on Mayville's E-Safety and Acceptable Use policies as part of their induction.

All teaching staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. All supply staff receive information about e-Safety as part of their safeguarding briefing on arrival at school.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in school. When children use computers in school staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's DSL and Director of IT.

2. Pupils: e-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, and usually via PSHE, all pupils are taught about their e-safety responsibilities and to look after their own online safety. From Remove, pupils are formally taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL, the e-Safety Coordinator or any member of staff at the school.

From Remove, pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images through discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the Safeguarding Lead or School Counsellor or Director of IT as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

3. Parents (see number 7 above)

The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Policy Statements

1. Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them.

Staff are referred to the Staff and Visitors BYOD Policy for further guidance on the use of non-school owned electronic devices for work purposes.

Staff at Mayville are permitted to bring in personal devices for their own use.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents / carers and under no circumstances may staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system for school business.

Pupils

If pupils bring in mobiles (e.g. for use during the journey to and from school), they must be handed in to their form tutors at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

The school has introduced the use of pupil owned tablets as a teaching and learning tool and pupils are required to adhere to the Pupil BYOD Policy when using tablets for school work. In particular, the Pupil BYOD Policy requires pupils to ensure that their use of tablets for school work complies with this policy and the Pupil Acceptable Use Policy and prohibits pupils from using tablets for non-school related activities during the school day.

School mobile technologies available for pupil use including laptops, tablets, cameras, etc are stored in the IT office. Access is available via the IT Manager. Members of staff should sign devices out and in before and after each use by a pupil.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the Director of Studies to agree how the school can appropriately support such use. The Director of Studies will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

2. Use of internet and email

Staff

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with school work or business whilst teaching. Such access may only be made outside of the classroom.

When accessed from staff members' own devices, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.

Staff must immediately report to the Director of Studies 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. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Director of IT.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring the School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should school pupils or parents be added as social network 'friends' or contacted through social media for school business.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email address for school business. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

All pupils are issued with their own personal school email addresses for use on our network. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work assignments / research / projects. Pupils should be aware that email communications through the school network and school email addresses are monitored.

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, pupils should contact the IT Manager for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to the Director of IT.

The school expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the Director of IT. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Management Policy. Pupils should be aware that all internet usage via the school's systems and its wifi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should contact the IT Manager for assistance.

3. Data storage and processing

The school takes its compliance with the Data Protection Act 2018 seriously. Please refer to the Data Protection Policy and the Acceptable Use Policy for further details.

Staff and pupils are expected to save all data relating to their work to their school laptop/ PC or to the school's central server / Google Drive Account in accordance with the IT Policy.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending unless coursework for exam purposes.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by school.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Director of IT.

4. Password security

Pupils and staff have individual school network logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every 6 months;
- not write passwords down; and
- not share passwords with other pupils or staff.

5. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming 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.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents / carers are welcome to take videos and digital images of their own children at school events for their own personal use.

Staff are allowed to take digital / video images to support educational aims, but must follow this policy and the Acceptable Use Policy / IT Policy / EYFS Mobile Phone Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of each other.

Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website.

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

6. Misuse

Mayville High School will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the LSCB. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP. Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures (in particular the Safeguarding Policy.)

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

7. Remote learning

Where children are being asked to learn online at home the Department has provided advice to support schools and colleges do so safely: safeguarding in schools colleges and other providers and safeguarding and remote education. The NSPCC and PSHE Association also provide helpful advice:

- NSPCC Learning - Undertaking remote teaching safely during school closures
- PSHE - PSHE Association coronavirus hub

Complaints

As with all issues of safety at Mayville High School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the Director of IT in the first instance, who will liaise with the Headteacher and undertake an investigation, where appropriate. Please see the Complaints Policy for further information.

Incidents of or concerns around e-safety will be recorded using a Record of Concern form and reported to the school's Director of IT, the Headteacher and the Designated Safeguarding Lead, in accordance with the school's Safeguarding Policy.

Annex A

Information and support

There is a wealth of information available to support schools, colleges and parents/carers to keep children safe online.

Advice for governing bodies/proprietors and senior leaders

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- UK Council for Internet Safety have provided advice on, and an Online Safety Audit Tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring
- Department for Digital, Culture, Media & Sport (DCMS) Online safety guidance if you own or manage an online platform provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk.
- Department for Digital, Culture, Media & Sport (DCMS) A business guide for protecting children on your online platform provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

Remote education, virtual lessons and live streaming

- Case studies on remote education practice are available for schools to learn from each other
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing
- National cyber security centre guidance on how to set up and use video conferencing
- UK Safer Internet Centre guidance on safe remote learning

Support for children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Parental support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

Annex B

Mayville High School

Staff Acceptable Use Agreement

I understand that I should use the school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure pupils receive opportunities to gain from use of digital technology. I will, where possible, educate the young people in my care the safe use of digital technology and embed online safety in my work with young people.

I confirm that I have read and will adhere to the following:

- Any content I post online (including outside school time) or send in a message will be professional and responsible and maintain the reputation of the school.
- To protect my own privacy I will use a school email address and school telephone numbers as contact details for pupils and their parents.
- If I use any form of electronic communication for contacting pupils or parents I will use the school's system, never a personal account.
- in silent mode except in emergency situations with prior agreement with my line manager.
- I will never use my personal mobile phone or other personal electronic equipment to photograph or video pupils.
- I will use the school mobile devices for school trips.
- I will only use agreed social media platforms set up specifically for school trips by our Marketing Director for communication with parents via the school mobile phone.
- Taking photographs and videos will only be done with the permission of pupils and/or their parents for agreed school activities and only on school devices not personal devices.
- I will 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.
- I will take all reasonable steps to ensure that all personal laptops and memory devices are fully virus protected and that protection is kept up to date.
- I will report any accidental access to material which might be considered unacceptable immediately to my line manager and ensure it is recorded.

I will follow school policy on compliance with the General Data Protection Regulations (GDPR). In particular:

- I understand that I have the same obligation to protect school data when working on a computer outside school.
- I will report immediately any accidental loss of personal or sensitive information so that appropriate action can be taken.
- I understand that the school may monitor or check my use of IT equipment and electronic communications.
- I understand that the school has the right to examine or delete any files that may be held on its computer system, to monitor any internet sites visited and emails exchanged and, if necessary to report anything which may constitute a criminal offence.

For staff who are also parents at the school

- Digital communication with other parents will remain professional at all times and no discussions of specific pupils or staff relating to school will be communicated to parents.

I understand that by not following these rules I may be subject to the school's disciplinary procedures.

Name.....

Signed.....

Date.....

Acceptable Use Policy for Senior Pupils

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. They may also pose greater and more subtle risks to young people.

We understand the responsibility to educate our pupils on online safety issues, to teach them the appropriate behaviours and critical-thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.

Further details on measures taken by the School to try and ensure our pupils stay safe in the online environment are set out in the School's Online Safety Policy.

This Acceptable Use Policy is intended to ensure:

- that all MHS pupils will be responsible users and stay safe while using
- the internet and other communications technologies for educational, personal and recreational use
- that School ICT systems and users are protected from accidental or
- deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Policy Agreement

I understand that I must use School ICT systems and my own devices insofar as they are allowed in School, in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the School ICT systems and other users.

I must also follow the School's Bring Your Own Device (BYOD) Policy when using my own device at School and logging on to School facilities.

For my own personal safety:

- I understand that the School will monitor my use of the ICT systems, email and other digital communications.
- I understand that I have an email account issued to me by the School. I must use this email account when emailing staff at School.
- I will not reveal my username and password to anybody else, nor will I try to use any other person's username and password.

And whatever device I am using:

- I understand that it is in the best interest of my safety to ensure that any social media profiles I have are set to the highest privacy setting and that I only communicate with people I know offline.
- I will be aware of "stranger danger" when I am communicating on-line and, if in doubt, I will seek the advice of a member of staff or parent/guardian.
- I will not disclose or share personal information or images of or about myself or others on-line.
- If I arrange to meet people off-line that I have communicated with on- line, I will do so in a public place and take an adult with me.
- I will immediately report any material or communications I receive online that make me feel uncomfortable or which are offensive, discriminatory, threatening or bullying. I will not respond to any such communications.

I understand that everyone at School has equal rights to use technology as a resource and:

- I understand that the School ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the School's internet systems for inappropriate activities such as on-line gaming, on-line gambling, internet shopping or file sharing or sending and/or sharing inappropriate images.
- I will act as I expect others to act toward me, and whatever device I am using
- I will respect others' work and property and will not access, copy, share, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will adopt appropriate etiquette when sending emails to staff and other pupils, ensuring those emails are polite and formatted correctly.
- I will be polite and responsible when I communicate with others online, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take, use, share, publish or distribute images of anyone without their permission, even if I consider the image to be harmless.
- I will not share other peoples' contact details or other information about them without their permission.
- I will not refer to the School, its staff or pupils on websites or other areas of social media without the School's consent.
- I will not build, use or host any website (eg blogs, YouTube) outside of the School network which contains any material relating to MHS or members of the School community.
- I understand that the School will monitor the use of social networking sites by pupils.

I recognise that the School has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the School:

- My mobile phone must be handed in to my tutor in the morning and switched off.
- I understand that use of cameras or other recording equipment, including on mobile phones and other devices, is forbidden during normal school hours, unless under direction of a member of staff. It is always forbidden in toilet, washing and changing areas.

- I will not upload, download, send, print, or access any materials which are illegal, obscene or inappropriate or may cause harm or distress to others, nor will I use any programs or software that might allow me, or otherwise attempt to bypass the filtering / security systems in place to prevent access to such materials. I will immediately report to staff any accidental access to inappropriate materials.
- I will treat School ICT equipment with respect and care, and will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails unless I know and trust the person / organisation who sent the email. This is because of the risk of the attachment containing viruses or other harmful programs.
- I will not install or attempt to install programs of any type on School hardware nor will I try to alter computer settings.
- I will not use a memory stick or external hard drive on any School ICT equipment.
- I will use School email responsibly and I will not send inappropriate emails or distribute mass emails (eg distribution lists) without good reason.
- I understand that, with the exception of portable computers, School IT equipment should not be moved, relocated or adjusted without the permission of a member of staff.
- I understand that display screens and signs in classrooms and other areas of the School should not be touched without a member of staff present in the classroom in order to supervise.
- I understand that I have my own user area to store private files and folders for school work only. This area should not be used to store personal photographs, music or documents. If my work is particularly important, it is good practice to save additional copies elsewhere as the School cannot guarantee against possible hardware failure.
- I understand that any deliberate attempt to damage or 'hack' into the School's ICT infrastructure will result in serious disciplinary action.

When using the internet for research or recreation, and whatever device I am using, I recognise that:

- I must think carefully before I post any information online or repost or endorse content created by other people
- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that MHS also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information, hurtful or derogatory comments on chat rooms, instant messaging, text messaging, social networking sites or similar websites).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement (and the Bring Your Own Device Policy, where applicable), I will be subject to disciplinary action.

Please click on I Accept below to show that you have read, understood and agree to the rules included in

the Acceptable Use Agreement (and the Bring Your Own Device Policy, where applicable). If you do not accept, access will not be granted to School ICT systems and you will not be allowed to bring your own device into School and log on to the School's facilities.

I confirm that I have read and understood this policy.

Pupil name.....

Pupil signature.....

I confirm that I have read and understood this policy.

Acceptable Use Policy for Key Stage 2 Pupils

- I will take care when using the school IT equipment and use it responsibly.
- I will keep my passwords private unless I need to share them with a trusted adult.
- I will inform an adult if I see or receive any unpleasant text, images or messages.
- I will not interfere with anyone else's passwords, settings or files on the computer.
- I will be careful when downloading material from the internet or using material I have brought into school because I understand the risks from virus infections.
- Any work I upload to Google Classroom will be my own.
- I know I need permission to take someone's photograph or to video them.
- Any messages I post online or send in an email will be polite and responsible.
- I will not send or forward messages or create material which is deliberately intended to upset other people.
- I know I must take care about giving away my personal information and making contact with people I do not know when using the internet.
- I will only bring my personal devices such as smart watches and mobile phones into school with the consent of my teacher. I will follow the school rules on storage of my devices during the school day.
- I understand that the school may check my use of IT and contact my parent/carer if they are concerned about my online safety.
- I will follow guidance on age appropriate social media platforms and apps.
- I understand that if I do not follow these rules I may not be allowed to use the school computers or access the internet for a period of time and that this may happen even if the activity was done outside school.

Pupil name.....

Pupil signature.....

I confirm that I have read and understood this policy.

Signed.....

Relationship to child.....

Acceptable Use Policy for Early Years/ Pre-Prep Pupils

- I will take care when using the school IT equipment and use it properly.
- I will only share my username or password with trusted adults.
- I will tell an adult if I see anything which upsets me.
- I will use a safe name and not my real name on the internet.
- I will only take a photograph or video of someone if they say it is alright.
- Any messages I send will be polite.
- I will not deliberately write anything which upsets other people.
- I understand that the school may talk to my parent or carer if they are worried about my use of school IT equipment.
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a while, even if it was done outside school.

Pupil name.....

I confirm that I have read and understood this policy.

Signed.....

Relationship to child.....

Acceptable Use Policy - Teaching lessons remotely and online

Safeguarding

- All the rules for safe, professional behaviour that apply at school still apply online
- All teachers have been given advice about delivering remote lessons safely
- All our teachers have been safely recruited, have up-to-date training, have undergone enhanced DBS checks and are experienced professionals
- All lesson invitations will go to parent/carer email addresses so that you will log in for your child/ren
- Parents will be asked by teachers to confirm that they have read this guide when they receive their first lesson invitation – you must reply to confirm that you have read this and give permission to proceed
    - other children should not be present if possible
- Teachers can mute participants and end the lesson at any time and have been instructed to end immediately if anything happens that they feel uncomfortable about
- If anything happens that you as a parent feel uncomfortable about you should report it to n.ramsey@mayvillehighschool.net

Setting up the system

- Google Classroom is a safe system and all teachers will be using their school email addresses
- In the unlikely event of an unknown third party infiltrating the lesson, you must end the meeting immediately – this will be reported by the teacher when the session has ended

- If you have problems with video, or feel that you would prefer not to use it, then teachers can deliver the lesson using audio only
- If you have technical difficulties with accessing the lesson, ask your teacher for advice and they will do their best to help you

Lesson Preparation

- Select a suitable room where your child will not be disturbed – **avoid using their bedroom unless there is no alternative**
- Try to ensure that external noise will not affect the lesson
- Some areas of your house may be better than others in terms of the Wi-fi connection
- Pupils must be dressed appropriately in daytime clothing – teachers will not deliver the lesson if a child is not appropriately dressed
- Remind your child/ren that this is a lesson situation and not a social media interaction and they should speak and behave appropriately as they would in a school lesson

Acceptable Use Policy for Temporary or Supply Staff and Visitors to School

As a visitor to the school I recognise that it is my responsibility to follow school procedures and that I have a responsibility to ask for advice if I am not sure of a procedure.

I confirm that I will use all electronic communication equipment provided by the school, and any personal devices which I bring into in school, in a responsible manner and in accordance with the following guidelines:

- I will only use the school network for the purpose I have been given access, related to the work I am completing in the school.
- I will not use a personal computer I have brought into school for any activity which might be considered inappropriate in the school.
- I will not use my personal mobile phone or other electronic equipment to photograph or video pupils.
- I will not publish photographs or videos of pupils without the knowledge and agreement of the school or the pupils concerned.
- I will not give my personal contact details such as email address, mobile phone number, or social media details to any pupil or parent in the school. Contact will always be through a school approved route. I will not arrange to communicate online or use a web camera with pupils unless specific permission is given.
- I will take all reasonable steps to ensure the safety and security of school IT equipment, including ensuring that any personal devices or memory devices I use are fully virus protected and that protection is kept up to date.
- I will report any accidental access to material which might be considered unacceptable immediately to a senior member of staff and ensure it is recorded.
- I will report immediately any accidental loss of personal or sensitive information to a senior member of staff so that appropriate action can be taken.
- I understand that I have a duty of care to ensure that students in school use all forms of electronic equipment and devices safely and should report any inappropriate usage to a senior member of staff.

- I will not publish or share any information I have obtained whilst working in the school on any personal website, blog, social networking site or through any other means, unless I have permission from the School.
- I understand that the school has the right to examine or delete any files that may be held on its computer system, to monitor any internet sites visited and emails exchanged and, if necessary to report anything which may constitute a criminal offence.
- I understand that by not following these rules I may be subject to disciplinary procedures

Name.....

Signed.....

Date.....

August 2023, RP.