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. peer on peer abuse)

· Staff Behaviour Management Policy;

· Health and Safety;

· Behaviour Management;

· Anti-Bullying;

· 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: peer to peer 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. 3G, 4G and 5G). This access means some children, whilst at school, could sexually harass their peers 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 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 E-Safety Trustee is Mrs J Scoins.

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 Communications.

In particular, the role of the Headteacher and the Senior Management Team is to ensure that:

· staff, in particular the Director of IT are adequately trained about e-safety; and

· staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

3. Director of IT

The School's Director of IT is responsible to the Headteacher for the day to day issues relating to e-safety. The Director of IT, has responsibility for ensuring this policy is upheld by all members of the school community, and works with IT staff to achieve this. They 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.

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 and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage 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.

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. The Director of IT posts messages every Sunday “Safety Sunday” on the school’s facebook account giving parents advice on how to keep their child safe online. We also use parents’ evening where we have a captive audience to promote online safety and give further advice. 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.

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 school computers, 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, pupils are taught about their e-safety responsibilities and to look after their own online safety. From year 7, 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 year 7, 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.

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 IT Manager.

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.

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. 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.

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 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 on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.

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

MAYVILLE HIGH SCHOOL
Founded in 1897

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

1. I will only use the school's email/Internet/Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Headteacher.

2. I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

3. I will ensure that all electronic communications with pupils, parents and staff are compatible with my professional role and via the school email systems in place ie: schoolbase/parent portal, Gmail.

4. I will not give out my own personal details, such as mobile phone number, personal. email address, personal Twitter account, or any other social media link, to pupils or parents. [Exceptions: In the case of school trips or expeditions, eg. D of E, it may be necessary to use a personal mobile number for emergency contact with parents.]

5. I will not give out any confidential information about the school via my own social media accounts.

6. I will only use the approved, secure email system(s) for any school business.

7. I will ensure that personal data (such as data held on Schoolbase) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.

8. If I leave a PC unattended I will either lock the screen or log off to prevent unauthorised access to data.

9. I will not install any hardware or software without permission of the IT Director or Network Support Manager.

10. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

11. I will not take photographs of pupils on any personal digital device. *[Exception: Discretion to be used here – school cameras should be available but if in exceptional cases a personal device is used to take photographs these must be deleted from the device as soon as they are transferred onto the school network which should be at the first opportunity.]

12. A) Images of pupils will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent..

13. B) Images of staff will only be taken, stored and used for professional purposes in line with school policy and with verbal consent of the staff member.

14. Images will not be distributed outside the school network without the permission of the parent, member of staff or Headteacher.

15. I understand that my use of the Internet and school system can be monitored and logged.

16. I will respect copyright and intellectual property rights.

17. I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

18. I will support and promote the school's E-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

19. I will not use a mobile phone in classrooms when pupils are present; additionally my mobile phone should be on 'silent' and out of sight. [Exception:a) Staff who are 'on call' who do not have a phone in the classroom or DYC. b) In exceptional circumstances staff may be expecting an urgent call and discretion should be used in dealing with this.c) In event of Lock Down emergency signal phones to be used]

I understand this forms part of the terms and conditions of my employment

MAYVILLE HIGH SCHOOL

Founded in 1897

Acceptable Use Agreement: Pupils - Secondary

- I will only use ICT systems in school, including the internet, email, digital video, and mobile technologies for school purposes.
- I will not download or install software on school devices.
- I will only log on to the school network, email and hub with my own user name and password.
- I will follow the school's ICT security system and not reveal my passwords to anyone; I will change them if I am concerned that they are known by others.
- I will only use my school email address within school or to communicate with teachers regarding school matters from home.
- I will make sure that all digital communication with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will follow online safety guidelines given within PSHE/ICT sessions and will not give out any personal information such as name, phone number or address. I will not arrange to meet anyone that I have made contact with online.
- I am aware that if/when I take images of fellow pupils and/or staff, that I must only store and use these for school purposes, in line with school policy and must never distribute these outside the school network without the permission of all parties involved.
- I will ensure that my online activity, both in school and outside school, will not cause the school, the staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I will not sign up to online services until I am old enough to do so.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/guardian may be contacted.

I understand that any misuse of ICT or the Internet will be investigated and

MAYVILLE HIGH SCHOOL

Founded in 1897

may mean that my access may be withdrawn or limited for a period of time.

Acceptable Use Agreement: Pupils - Junior

- I agree that my child will only use ICT systems in school, including the internet, email, digital video, and mobile technologies for school purposes.
- I agree that my child will not download or install software on school devices.
- I agree that my child will only log on to the school network, email and classroom with their own user name and password.
- I agree that my child will follow the school's ICT security system and not reveal my passwords to anyone; I will change them if I am concerned that they are known by others and let the classteacher know.
- I agree that my child (UII-U3) will only use my school email address within school or to communicate with teachers regarding school matters from home.
- I agree that my child will ensure that that all digital communication with pupils, teachers or others is responsible and sensible.
- I agree that my child will be responsible for their behaviour when using the Internet. This includes resources I access and the language used.
- I agree that my child will not browse, download, upload or forward material that could be considered offensive or illegal. If they accidentally come across any such material this will need to be reported immediately to the teacher.
- I agree that my child will follow online safety guidelines given within PSHE/ICT sessions and will not give out any personal information such as name, phone number or address.
- I agree that my child will not take any images of other pupils at school.
- I agree that my child will ensure that their online activity, both in school and outside school, will not cause the school, the staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts.
- I agree that my child will respect the privacy and ownership of others' work on-line at all times.
- I agree that my child will not attempt to bypass the internet filtering system.
- I agree that my child understand that all use of the Internet and other related technologies can be monitored and logged at school and can be made available to my teachers.
- I agree that my child will not sign up to online services.

MAYVILLE HIGH SCHOOL

Founded in 1897

- I agree that my child understand that these rules are designed to keep them safe and that if they are not followed, school sanctions will be applied and their parent/guardian may be contacted.

I understand that any misuse of ICT or the Internet will be investigated and may mean that my child's access may be withdrawn or limited for a period of time.

RHKP 21/07/22