

# E-Safety Policy (Including Acceptable Use Policy for Pupils) 2021-2022

Author: D. Reid / M. Keeley Approved by the governing board: August 2021 Date of next review: July 2022

MORE HOUSE SCHOOL

# **Covid-19 Update to Policy**

The Covid-19 pandemic has precipitated the need for the provision of remote learning for individual pupils or during full or partial school closure. During this time, the guidance provided in this policy (and in the related polices listed below) remains in force and relevant and should be adhered to by all staff, parents and pupils. The school further acknowledges its responsibilities to undertake to provide a safe environment for online learning during school closure and takes a proactive approach to this task by:

- Having in place an Online Home Learning Responsible User Agreement that is signed by all pupils and staff (appendix 3). The agreement makes clear the school's expectations of those engaging in remote learning;
- Providing regular advice and guidance to pupils on staying safe online by way of the PSHE and RSE programme delivered during form time and in the curriculum through IT lessons.. This guidance sets out to make them aware of both the benefits and hazards of online learning, their own responsibilities whilst on online and how they can report concerns;
- Providing regular advice and guidance to staff on the provision of remote learning by way of training sessions, briefings and email updates;
- Providing regular advice and guidance to parents by way of safeguarding bulletins and email communications. Parents sign an Online Learning Consent Form in which they consent to online learning via Google Meets (appendix 3);
- Providing additional and tailored support for pupils who have been identified as vulnerable. Such support is coordinated by the SENCO, Director of Pastoral Care and Deputy DSL;
- Maintaining systems to monitor the use of school systems using filtering software;
- Having in place an updated policy for the use of visiting speakers;
   Having in place a

signed parental agreement covering the use of pupil images and identifying

information;

• Updating relevant policies and procedures to reflect the latest government guidance.

# **Policy Statement**

At More House, and in keeping with the KCSIE 2021 guidance, we believe it is essential that pupils are safeguarded from potentially harmful and inappropriate online material. We have a whole school approach to online safety which empowers us to protect and educate pupils and staff in their use of technology.

More House acknowledges that the internet and associated Bring Your Own Device (''BYOD'') initiative, such as, computers, laptops, tablets et al, will provide a creative and engaging platform from which pupils can learn and flourish and is an important aspect of everyday life.

More House believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing board, Senior Leadership Team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as "staff" in this policy) as well as pupils and parents.

This policy applies to all access to the internet and use of any form of technology within school, including personal devices/BYOD, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones.

A whole school approach to online safety is essential to safeguarding. Our e-safety measures include robust policies and procedures, effective training, education for staff, pupils and parents, robust technical solutions to allow pupils to access appropriate resources and ongoing review and evaluation of the systems in place. We consult with stakeholders (pupils, staff and parents) on the formation of policies and procedures. Online safety is evident in the curriculum through our RSE and PHSE programme, the Digital Skills SOW and assembly programme. It is also evident in the Digital Skills curriculum and modelled in assemblies and other aspects of School life. Furthermore, the Catholic ethos of the School enshrines our values of dignity, respect, equality, justice, love and tolerance which guides the behaviour of all, both on and offline.

# The purpose of this policy is to:

- Safeguard and protect all members of the School community online;
- Identify approaches to educate and raise awareness of e-Safety throughout the community;
- Ensure that the curriculum teaches the knowledge and behaviours necessary for our pupils to flourish online and rewards pupils who model the knowledge and behaviours appropriately.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology;
- Identify clear procedures to use when responding to e-Safety concerns
- The issues classified within e-Safety are considerable and vast, but can be broadly categorised into <u>four areas of risk (as outlined in the KCSIE 2021)</u>:
  - **Content**: being exposed to illegal, inappropriate or harmful content;
  - Contact: being subjected to harmful online interaction with other users
  - Conduct: personal online behaviour that increases the likelihood of, or causes, harm
  - **Commerce:** risks such as online gambling, financial scams etc.
- This policy aims to ensure that all members of the School community are aware of these risks and can take the appropriate measures to safeguard themselves and others online.

## **Related Policies**

Section C1 No. 1	Safeguarding and Child Protection Policy
Section C2 No.1	Policy on Behaviour and Discipline
Section C1 No. 3	Anti-bullying Strategy
Section A No.15	Privacy Notice
Section E	Employee Handbook Section C1 No. 2 Code of Conduct
Section E	Employee Handbook Section C1 No. 2 Code of Conduc

Curriculum Policies, such as: IT, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)

# Monitoring and Reviewing Online Safety

Technology, and risks and harms related to it evolve and change rapidly. As such, we will conduct an annual review of our approach to online safety, supported by an annual risk assessment that considers and reflects the risks our pupils' face. In addition, we use the 360safe online safety self-review tool to inform our policies and procedures.

In light of the responsibility to safeguard and promote the welfare of children and provide pupils with a safe environment in which to learn, the Governors will do all that they reasonably can, in keeping with their statutory duty, to limit our pupils' exposure to risks from the School's IT system. As part of this process, Governors will ensure that our filters and monitoring systems are appropriate.

In determining the appropriateness of our filters and monitoring system, this is informed in part, by the risk assessment required by the Prevent Duty. Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the Senior Leadership Team. The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective BYOD classroom management and regular education about safe and responsible use is essential.

More House currently uses Iboss to monitor the internet usage of pupils.

# 1. Roles and Responsibility

#### Headteacher's responsibility

- Oversee the update and review of the E-safety policy and manage allegations of misuse of ICT by staff
- The Headteacher will ensure that the School e-Safety practice (and as a significant safeguarding issue), is in keeping with legal requirements
- Ensure there are appropriate and up-to-date policies working in conjunction with the E safety policy such as the Safeguarding and Child Protection policy and Behaviour Policy
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks
- Ensure that e-Safety is embedded within the curriculum, which enables all pupils to develop an age-appropriate understanding of e-Safety
- Support the DSL and any deputy DSL by ensuring they have sufficient time and resources to fulfil their e-Safety responsibilities
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology
- Audit and evaluate e-Safety practice to identify strengths and areas for improvement

## The Designated Safeguarding Lead

- Have overall responsibility for the implementation of this policy, including the management of allegations of misuse of ICT systems by pupils and the promotion of e-safety to pupils, staff and parents.
- The DSL will evaluate the risks posed to More House pupils online and educate accordingly.

- Will act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside the Deputy Head Academics to ensure that e-Safety is embedded as part of the school's safeguarding responsibilities and that a whole school approach is implemented
- Work alongside the Senior Teacher Academics and Deputy Head Academics to ensure all members of staff receive regular and up-to-date e-Safety training
- Access regular and appropriate training and support to ensure they understand the unique risks associated with e-Safety and have the relevant knowledge and up to date required to keep pupils safe online whilst recognising the particular vulnerabilities of those pupils with SEN
- Maintain records of e-Safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms
- Report e-Safety concerns, as appropriate, to the SLT team and to Governors
- Meet annually with the Lead Governor with responsibility for safeguarding and online safety

#### **Staff Members**

It is the responsibility of all members of staff to:

- Read and adhere to the e-Safety policy and acceptable use policies take responsibility for the security of school systems and the data they use or have access to
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site
- Embed e-Safety education in curriculum delivery. By way of example, now that the BYOD initiative is being launched, classroom teachers must ensure pupils are using their devices appropriately and only for the activities authorised by the classroom teacher.
- To address any inappropriate BYOD issues that arise in their classroom by first sanctioning the pupil and/or escalating the inappropriate usage to the Head of Department. If the HOD feels that this is a serious infraction or an E-safety concern, it will be escalated to the DSL and/or Deputy DSL.
- Have an awareness of a range of e-Safety issues and how they may be experienced by the pupils in their care
- Identify e-Safety concerns and take appropriate action by following the school's safeguarding policies and procedures
- Know when and how to escalate e-Safety issues, including signposting to appropriate support, internally and externally
- Take personal responsibility for professional development in this area

## Staff managing the technical environment

- Provide technical support and perspective to the DSL and Senior Leadership Team, especially in the development and implementation of appropriate e-Safety policies and procedures
- Implement appropriate security measures such as password policies and encryption, to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing online learning opportunities to be maximised
- Ensure that the filtering and monitoring policies and procedures are applied on a daily basis.

## Senior Teacher Academic and Deputy Head Academic

• To ensure e-safety is evident across the curriculum and for providing training for staff (whether in-house or via external agencies)

## **Pupils**

It is the responsibility of pupils to:

- Follow the instructions of classroom teachers at all times and to use and access the online sites/materials and resources that teachers have authorised the pupils to access and use. Pupils agree to engage in age appropriate e-Safety education opportunities;
- read and adhere to the acceptable use policies;
- always be respectful, kind and considerate and to uphold each person's dignity both on and offline;
- take responsibility for keeping themselves and others safe online;
- contribute to the development of e-Safety policies by providing feedback through pupil questionnaires and School Council feedback;
- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of the School community are advised to take steps to protect their devices from loss, theft or damage; The School accepts no responsibility for the loss, theft or damage of such items on our premises.
- Years 7-11 pupils are **not allowed** to use their devices outside of lesions and are **not permitted** to use their devices at break and/or lunchtime. The only exception to this is if pupils are in the **library during break and/or lunchtime** to complete school work and under the supervision of a member of staff. Pupils must ensure their personal devices and/or School devices are either in lockers or in their Schoolbags during break and lunch.

## Parents

It is the responsibility of parents to:

- read the acceptable use policies and to ensure that their children adhere to them;
- support the school's e-Safety approaches by discussing e-Safety issues with their children and reinforcing appropriate and safe online behaviours at home;
- Manage and oversee their daughter's online usage, behaviour, language and the apps that she uses and posts on;
- Consider operating a time restriction, beyond which, your daughter has no access to technology and can relax and unwind before bedtime e.g. for KS3 no technology after 8pm; KS4 no technology after 9pm.
- role model safe and appropriate use of technology and social media;
- identify changes in behaviour that could indicate that their daughter is at risk of harm online
- seek help and support from the school, or other appropriate agencies, if their daughter encounters risk or concerns online;
- take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

# 2. Communicating School Policy

This policy is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school and are reflected in our Safeguarding Child Protection Policy. E-safety is integrated into the curriculum in our whole school approach and duringDigital Skills lessons and form time where personal safety, responsibility, and/or development are being discussed through PSHE and RSE.

# 3. Making use of BYOD, ICT and the Internet in School

The BYOD to School and internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school. Some of the benefits of using ICT and the internet in schools are:

#### For students:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

#### For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.

#### For parents:

- Access to resources to support daughter's learning
- Access to the parent portal and information published on that platform such as reports and AP results
- Access to the school website
- Effective communication with school via email
- Receiving texts from the school
- Reporting absence to school

## **Classroom Use**

- In September 2021 the School initiates a BYOD to School initiative which will incorporate a wide range of technology. This includes School and personal access to:
  - Computers, laptops and other BYOD/digital devices
  - Internet which may include search engines and educational websites
  - Google Classroom
  - Email and School Gmail accounts
  - Games-based technologies
  - Digital cameras, webcams and video cameras

- All school owned devices and BYOD will be used in accordance with the acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and applications fully before use in the classroom or recommending for use at home.
- We will use age appropriate search tools to identify which tool best suits the needs of our community.
- We will ensure that the use of internet-derived materials, by staff and pupils complies with copyright law and acknowledge the source of information.
- Classroom teachers are responsible for the supervision of pupils' usage of the BYOD and will ensure that they are accessing information, websites, appropriate to their age and ability.
- More House School's IT Support Manager has ensured that the school has age and ability appropriate filtering and monitoring in place, to limit pupil exposure to online risks.
- The IT Support Manager is aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- As previously stated, all members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective BYOD classroom management and regular education about safe and responsible use is essential.
- Year 7-11 pupils are only allowed to use their BYOD during lessons and in the **library during break and/or lunchtime** for the completion of school work. This will be supervised by a break and lunchtime member of staff. Pupils must ensure their personal devices and/or School devices are either in lockers or in their Schoolbags during break and lunch.

# 4. Learning to evaluate online content

We will establish and embed an effective whole school approach to online safety to protect and educate pupils, and staff in their use of technology and establish mechanisms to identify, intervene and escalate concerns where appropriate. We will use the curriculum to raise awareness and promote safe and responsible online usage and provide pupils with the knowledge and behaviours necessary to evaluate online content by:

- providing e-Safety education and training as part of the BYOD initiative
- including e-Safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and ICT programmes of study
- reinforcing e-Safety messages regularly
- More House will support pupils to read and understand the acceptable use policies in a way which suits their age and ability by:
- displaying acceptable use posters in all rooms
- using support, such as external visitors, where appropriate, to complement and support our internal e-Safety education approaches

With so much information available online it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of the BYOD digital literacy across all subjects in the curriculum. Pupils will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online
- to acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

The new RSE curriculum which is delivered through the PSHE programme includes being taught what positive, healthy and respectful online relationships look like, the effects of online actions on others and knowing how to recognise and display respectful behaviour online.

Pupils with SEN have an increased vulnerability to risk online, especially those with language and communication needs, or social communication difficulties. The SENCO will make provision for pupils with SEN to be made aware of the specific risks associated with the use of ICT.

The School will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites, then the URL will be reported to the school DSL. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies.

Regular software and broadband checks will take place to ensure that filtering services are working effectively.

## 5. Managing information systems

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by the IT technician/ICT coordinator/network manager and virus protection software will be updated regularly.

Some safeguards that the school takes to secure our computer systems are:

- ensuring that all personal data sent over the internet or taken off site is encrypted
  making sure that unapproved software is not downloaded to any school computers.
- Alerts will be set up to warn users of this
- files held on the school network will be regularly checked for viruses
- the use of user logins and passwords to access the school network will be enforced
- portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team. For more information on data protection in school please refer to our data protection policy. More information on protecting personal data can be found in section 11 of this policy.

#### **Parents and Pupils**

Parents and Pupils should ensure that they have the requisite internet security and/or virus protection to ensure their daughters are safe online in and outside of School.

# 6. Emails

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies including (but not limited to) the: Policy on Behaviour and Discipline, Safeguarding and Child Protection Policy, Data Protection Policy.

The School uses email internally for staff and pupils, and externally for contacting pupils and parents, and is an essential part of school communication. It is also used to enhance the curriculum by:

- initiating contact and projects with other schools nationally and internationally
- providing immediate feedback on work, and requests for support where it is needed.

Staff and pupils should be aware that school email accounts should only be used for school-related matters, i.e for staff to contact parents, pupils, other members of staff and other professionals for work purposes. This is important for confidentiality. The School has the right to monitor emails and their contents but will only do so if it feels there is reason to.

## School email accounts and appropriate use

All pupils and staff are assigned an individual gmail account when they join the school. Only these accounts, which are managed and approved by the school, may be used.

Staff should be aware of the following when using email in school:

- Staff should only use official school-provided email accounts to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in school.
- Staff should only use the pupil initials in email subject titles.

Pupils should be aware of the following when using email in school, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- in school, pupils should only use their school email address;
- Pupils will make use of acceptable email etiquette when emailing their teachers. This includes an appropriate salutation, use of correct grammar, appropriate register and a suitable sign off.
- excessive social emailing will be restricted
- pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- pupils must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge. Pupils will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

## **Passwords and Password Security**

Passwords for school gmail accounts are strictly controlled and managed by the IT department. Should a password be inadvertently shared or forgotten, the pupil or staff member should contact the IT department who will reset the password.

# 7. Published content and the school website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects. The website is in the public domain, and can be viewed by anybody online. We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the: Policy on Behaviour and Discipline, Safeguarding and Child Protection Policy and Data Protection Policy. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the school will be for the school office only. For information on the school policy on children's photographs on the school website please refer to section 7.2 of this policy.

The Communications Officer is responsible for publishing and maintaining the content on the school website.

#### Policy and guidance of safe use of children's photographs and work

Colour photographs and pupils' work bring our school to life, showcase our student's talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material. The school will only use photographs in accordance with its Privacy Notice. On admission to the school parents/carers will be asked to sign a photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to.

Parents will be contacted annually for consent.

#### Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place. It is important that published images do not identify students or put them at risk of being identified. The school is careful to ensure that images published on the school website cannot be reused or manipulated through watermarking and browser restrictions.

Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children:

- Parental consent must be obtained. Consent will cover the use of images in:
  - all school publications
  - on the school website or in newspapers as allowed by the school
  - in videos made by the school or in class for school projects.
- We will store photographs and videos of children securely, in accordance with our safeguarding policy and data protection law. We will keep hard copies of images in a locked drawer and electronic images in a protected folder with restricted access.

- Images will be stored for a period of 10 years. We will never store images of children on unencrypted portable equipment such as laptops, memory sticks and mobile phones. More House does not permit staff and volunteers to use any personal equipment to take photos and recordings of children. Only cameras or devices belonging to the School should be used.
- Names of stored photographic files will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (ie a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only.
- Parents will be asked for photos taken during school events not to be shared on social media, recommending that people check the privacy settings of their social media account to understand who else will be able to view any images they share.
- Pupils are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers who are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils. For more information on safeguarding in school please refer to our school child protection and safeguarding policy.

## Complaints of misuse of photographs or video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our complaints policy for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the schools child protection and safeguarding policy and behaviour policy.

## Social networking, social media and personal publishing

The expectations regarding safe and responsible use of social media applies to all members of the More House School community. The term social media may include, but is not limited to, blogs, tiktok, snapchat, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. SEND pupils are particularly vulnerable to cyber bullying and online grooming and Form Tutors and the Director of Pastoral Care in consultation with the SENCO will ensure that these pupils fully understand the risks they face online through one to one sessions and information given in form time. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. There are various restrictions on the use of these sites in school that apply to both students and staff.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHE and RSE programmes about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place.

The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites/resources that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction and training sessions.

## **Pupil Work**

All work is securely stored in Google Classroom.

# 8. Mobile phones and Smart devices including smart watches

Because Year 7-11 pupils will now use their own device in many lessons pupils are NOT permitted to have their mobile phones and/or smart devices such as apple watches in lessons (unless the classroom teacher has provided permission and in this instance, the classroom teacher is responsible for taking the phone box from the office and crucially in returning it to the office at the end of the lesson to ensure all pupils have returned their mobile phone and/or smart watch). This is for a number of reasons:

- they can make pupils and staff more vulnerable to cyberbullying
- they can be used to access inappropriate internet material
- they can be a distraction in the classroom
- they are valuable items that could be stolen, damaged, or lost
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school will not tolerate cyberbullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message, either in school or off site, of such content will be disciplined. For more information on the school's disciplinary sanctions read the school Behaviour Policy.

The school's filtering systems prohibit the access of social media sites in school. Such sites are only accessible in special circumstances and under staff supervision. These circumstances may, for example, include:

- Use of social media sites for research purposes (ie as a tool for learning rather than for personal use)
- The access and use of departmental blogs

The school takes certain measures to ensure that mobile phones are used responsibly in school. Some of these are outlined below:

- Pupils in years 7, 8 & 9 are required to hand in their mobile phone on arrival at school and place them into the respective form mobile phone box. Phones are returned to the pupils at the end of the school day.
- Pupils in years 10 & 11 are required to hand in their mobile phone during morning registration. Phones are returned to them at the end of the school day.
- Year 7-11 pupils are required to seek permission from their Form Tutor or the School Office if they wish to use their mobile phone during the school day. This should only occur infrequently in the knowledge and understanding that if pupils need to contact parents as an emergency during the School day, this can be done via the School Office main phone and thus does not require the pupils' having access to their personal phones and/or smart watches.
- Members of the Sixth Form are required to restrict their use of mobiles phones to the Sixth form area on the 4<sup>th</sup> floor ONLY
- This means that phones and/or smart watches are not allowed to be visible in lessons, assemblies or whilst transiting around the School (*the exception to this is if the teacher has given the pupils permission to use the mobile phones in lessons*)..
- Mobile phones and/or smart watches can be confiscated by a member of staff, and the device can be searched by a member of the senior leadership team if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
- Mobile phones must be switched off during school lessons or any other formal school activities.
- Any pupil who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.
- Images or files should not be sent between mobile phones in school.

Instances of alleged misuse of mobile phones or personal devices should be reported to the Director of Pastoral Care

#### Laptops and other BYOD/personal devices

The use of BYOD devices is governed by the same rules and guidelines as mobile phones with the following exceptions:

All pupils are required to bring a laptop to school from September 2021.

#### Mobile phone, smart devices or other BYOD/personal device misuses

#### Pupils

- Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's Behaviour Policy and Anti-bullying Strategy. Their mobile phone and/or smart watch and/or BYOD may be confiscated.
- Pupils are under no circumstances allowed to bring mobile phones, smart watches or personal devices into examination rooms with them. If a pupil is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the pupil being prohibited from taking that exam.

#### Staff

- Staff are to follow the Staff Code of Conduct at all times.
- Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of school time.

- Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.
- The school expects staff to lead by example. Use of personal mobile phones should be limited to the staff room or offices or other designated areas during school hours.
- Any breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in the child protection and safeguarding policy, or in the staff contract of employment.
- Use of personal devices is included in the Employee Handbook under Computers and Electronic Communications.

## Webcams and Video Conferencing

Webcams and video conferencing may be used on occasions to support learning but only under the direct supervision of a member of staff. Misuse of these technologies should be reported to the Director of Pastoral Care and sanctions may be applied according to the Behaviour Policy.

# 9. Responding to E-safety incidents and concerns

- All members of the More House community will be made aware of the reporting procedure for online safety concerns, including but not limited to:
- breaches of filtering, youth produced sexual imagery (sexting), cyberbullying, peer on peer abuse, prejudice, discriminatory behaviour, and illegal content.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
- Pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the DSL will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL will seek advice from the relevant external agencies.
- Where there is suspicion that illegal activity has taken place, the DSL will contact the relevant external agencies and/or the Police if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local schools are involved or the public may be at risk), the DSL will speak with the Police.

## Concerns about Pupils' Welfare

- The DSL will be informed of any online safety incidents involving Safeguarding or Child Protection concerns. The DSL will keep the Head informed and the Head will be involved in addressing any serious concerns/matter pertaining to this.
- Staff will make a record of the concern:. All concerns will contain the following:
  - a clear and comprehensive summary of the concern;
  - details of how the concern was followed up and resolved;
  - a note of any action taken, decisions reached and the outcome.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the KCSIE and the School Safeguarding and Child Protection policy.
- The DSL and/or Deputy DSL will inform parents of online safety incidents or concerns involving their child, as and when required.

## Staff Misuse

- Any complaint and/or allegation about staff misuse will be referred to and investigated by the Headteacher.
- Appropriate action/sanctions will be taken by the Headteacher in accordance with our Child Protection Policy for Managing Allegations against Staff, Behaviour, Safeguarding policies.

#### Cyber Bullying/Peer on Peer Abuse

More House School operates under the culture that 'this (online/cyber bullying and/or peer on peer abuse) can happen anywhere' and thus we treat any issues, concerns, allegations, reports pertaining to online/cyber bullying very seriously and in line with the procedures noted below. All our approaches are underpinned by the principle that there is a zero-tolerance approach to bullying and peer on peer abuse and that bullying is never acceptable and will not be tolerated. We act with 'the best interests of the child' as the guiding principle.

Cyberbullying, prejudice based bullying, discriminatory bullying, peer on peer abuse, online bullying, sexual harassment and sexual bullying and online bullying, is taken very seriously by the school. This policy should be read in conjunction with the Anti-Bullying Strategy, the Sexual Violence and Sexual Harrassment policy and the Behaviour policy.

All members of the School community know what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

Instances of alleged misconduct / inappropriate online behaviour / bullying should be reported to the Director of Pastoral Care immediately.

Staff will make a record of what has been reported to them. All cases of bullying (whether in School or online) will contain the following:

- a clear and comprehensive summary of the concern;
- details of how the concern was followed up and resolved;
- a note of any action taken, decisions reached and the outcome.

If an allegation of bullying does occur, the school will:

- take it seriously
- act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- record and report the incident, as outlined above
- provide support and reassurance to the victim
- make it clear to the 'bully' that this behaviour will not be tolerated. If there is a
  group of people involved, they will be spoken to individually and as a whole group.
  It is important that children who have harmed another, either physically or
  emotionally, redress their actions and the school will make sure that they
  understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provide may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in school.

Repeated bullying may result in a fixed-term exclusion issued by the Headteacher.

#### Online Sexual Violence and Sexual Harassment Between Children

The Department for Education guidance on 'Sexual violence and sexual harassment between children in school and colleges 2021' has been used to revise our Policy on Sexual violence and Sexual harassment and thus the E-safety policy should be read in conjunction with this policy. More House School, as an all girls' school, operates under the culture that 'this can happen anywhere' and thus we treat any issues, concerns, allegations, reports very seriously and in line with the procedures noted below. All our approaches are underpinned by the principle that there is a zero-tolerance approach to sexual violence and sexual harassment and it is never acceptable and will not be tolerated.

The school recognises that sexual violence and sexual harassment between children can take place online. Examples may include but are not limited to; consensual and non-consensual sharing of nudes and semi-nudes, sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation. Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Policy for Sexual Violence and Sexual Harrassment, Behaviour policy, Safeguarding and Child Protection and Anti-bullying Policies.

As per Part One of Keeping Children Safe in Education, if More House staff have any concerns about a pupil's welfare, they will act on them immediately and report it to the DSL.

Where the report includes an online element, we are aware of searching screening and confiscation advice and the UKCIS Sharing nudes and semi nudes: advice for education settings working with children and young people. The key consideration is for More House staff not to view or forward illegal images of a child. Please note that there may be occasions where viewing an image is unavoidable. In such cases, it may be more appropriate to confiscate any devices to preserve evidence and hand them to the police for inspection.

#### Online Sexual Abuse and Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE)

Both CSE and CCE are forms of abuse that occur where an individual or group takes advantage of an imbalance in power to coerce, manipulate or deceive a child into taking part in sexual or criminal activity, in exchange for something the victim needs or wants, and/or for the financial advantage or increased status of the perpetrator or facilitator and/or through violence or the threat of violence. CSE and CCE can affect pupils, and can include children who have been moved (commonly referred to as trafficking) for the purpose of exploitation.

The school will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns. The school recognises online child sexual abuse and exploitation (including child criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL in conjunction with the Headteacher. Please refer to the Sexual Violence and Harassment policy for further guidance.

External agencies and/or the police will be contacted where necessary.

#### Indecent Images of Children (IIOC)

The school will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC). We will act in accordance with the Safeguarding and Child Protection policy always.

We will respond to concerns regarding IIOC School equipment and/or BYOD equipment, even if access took place off site.

If we are unclear if a criminal offence has been committed the DSL, in conjunction with the Headteacher, will obtain advice immediately from the Police.

#### **Online Hate**

Online hate content, directed towards or posted by, specific members of the community will not be tolerated and will be responded to in line with existing policies, including Antibullying and Behaviour and Discipline.

The Police will be contacted if a criminal offence is suspected.

If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the relevant external agencies and/or police.

#### **Online Radicalisation and Extremism**

We will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site.

If we are concerned that a child may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our Child Protection and Safeguarding Policies.

If we are concerned that a member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately.

Relevant external agencies will be contacted where necessary.

# 10. Managing emerging technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

# 11. Staff Training

#### More House will:

- provide up-to-date and appropriate e-Safety training for all staff on a regular basis, with at least annual updates this will cover the potential risks posed to pupils (Content, Contact and Conduct and Commerce) as well as our professional practice expectations
- recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape e-Safety policies and procedures
- make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices
- make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation
- highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils

• ensure all members of staff are aware of the procedures to follow regarding an Esafety concern pertaining to a pupil, colleague or any other member of the School community.

# Appendix 1: Acceptable use of BYOD, Internet, Emails and Computers and all Devices in School

At More House School we understand the importance and benefits of emerging technologies for children's learning and personal development. However, we also recognise that safeguards need to be in place to ensure children are kept safe at all times.

Please could parents read and discuss this policy with their child and then sign and return to the school office.

- I will only use ICT systems in school, including the BYOD, internet, email, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school equipment. Equally I will not download or use any apps or software in lessons that the classroom teacher has not provided permission for.
- I will only log on to the school network/ learning platform with **my own** username and password. I understand that I am responsible for keeping this information secure.
- I will follow the school's ICT security system and not reveal my passwords to any other person. I will change my passwords regularly.
- I will only use my school email address
- I will only use Google Chrome as my web browser in school and I will ensure that I am logged into Google Chrome with my school email address at all times.
- I will make sure that all ICT communications with pupils, teachers or others is responsible, sensible, polite and courteous and such that upholds the dignity of each and every individual.
- I will be responsible for my behaviour when using the BYOD in lessons and accessing the Internet. This includes resources I access and the language I use.
- I will not deliberately 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 not give out any personal information such as name, phone number or address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- I understand that images of pupils will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without parental permission.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring them into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community or any other individual.
- I will respect the privacy and ownership of others' work online at all times. I realise that plagiarism of others' work is a serious disciplinary matter. Plagiarism is presenting someone else's work or ideas as your own, with or without their consent, by incorporating it into your work without full acknowledgement.

Plagiarism may be intentional or reckless, or unintentional. Under the regulations for examinations, intentional or reckless plagiarism is a disciplinary offence.

- 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 understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parents may be contacted.

We have discussed this policy and name) agrees to support the safe use of ICT at More House School.	(child's
Parent/Carer's Signature:	-
Child's Signature:	-
Date:	-

#### Appendix 2

# Acceptable use of a laptop or the school's ICT facilities and internet: agreement for pupils and parents/carers

#### Name of pupil:

When using my personal laptop or the school's ICT facilities and accessing the internet in school, I will not:

- Use it for a non-educational purpose
- Use it without a teacher being present, or without a teacher's permission
- Use it to break school rules
- Access any inappropriate websites
- Access social networking sites or online streaming services (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Bully other people
- Copy and paste information directly from any source
- Use any ideas I have gathered through research without referencing the source
- I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly and in accordance with all school policies and publications, including the E-Safety Policy and Acceptable Use of the Internet, Emails and Computers in School guidance.

#### Signed (pupil):

**Parent/carer agreement:** I agree that my child can use their own laptop and the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

#### Signed (parent/carer):

#### Appendix 3

Dear Parents,

For pupils in Year 11 and 6<sup>th</sup> Form we will be offering virtual lessons conducted **via Google Meet**. We must receive parental permission before your daughter is able to take part in the virtual lessons. Alongside our usual ICT acceptable use policy all staff and pupils have agreed to *More House School Online Home Learning Responsible User Agreement* (attached to this email). The document outlines the parameters by which all students are expected to adhere to, in order to engage safely in virtual lessons.

Students are expected to read and discuss the Responsible User Agreement with you, and then to follow the rules and guidelines. If your daughter usually receives 1:1 lessons at school these will continue as normal, but another teacher will also be present in the virtual lesson to eliminate any safeguarding concerns.

Any concerns or queries can be discussed with the Director of Pastoral Care.

To facilitate video conferencing during school hours, parents should support by:

- Providing students with a workplace that is quiet, safe and free from distractions.
- Parents should inform the school if their child is unwell by emailing absent@morehousemail.org.uk
- Making sure that your child is dressed appropriately (No pyjamas or revealing clothing)
- Ensuring that face-face communication is only between teachers and students. Any parent to teacher communication should be in the usual manner, via email.
- Parents may not record, share or comment on public forums about individual teachers.

By completing this google form, you give permission for your daughter to attend virtual lessons with More House staff.

#### Online Learning Consent Form

Your daughter will not be able to attend virtual lessons until confirmation is received so please complete the form as soon as possible.

Many thanks for your continued support, Sally Brown Online Learning Consent Form Parental permission for students to take part in virtual lessons.

Your	answer	

Daughter's name \*

I Your answer

Do you agree to your daughter taking part in lessons via Google Meet? \* Yes

No

I understand that I need to inform the office if my daughter is unwell and will not be attending lessons.  $\ensuremath{^*}$ 

Yes

Other:

#### ocher.

#### Submit

#### <u>l agree that:</u>

- During lessons conducted via Google Meet I will only use technology for school purposes as directed by my teacher.
- I will be responsible for my behaviour and actions when using technology, this includes the resources that I access and the language that I use.
- I will make sure that all my communication with students, teachers or others using technology is responsible and sensible.
- I will not record or take photos of my classmates or teachers during a face to face session.
- I agree to only use my school email address to interact with my teachers.
- I understand that when using my school email address my use can be monitored.
- I understand that these rules are designed to help keep me safe and that if they are not followed school sanctions will be applied and my parent may be contacted.

#### **Guidelines**

When using Google Meet, remember that this is an extension of the classroom and you should conduct yourself as you would in the classroom. This includes:

- Video conferencing from an environment that is quiet, safe and free from distractions (*ideally this should not be your bedroom*)
- Be on time for your interactive session
- Make sure you have all the required resources ready, check Google Classroom / emails regularly for these.
- Be dressed appropriately for learning (no pyjamas or revealing clothing)
- Remain attentive during sessions
- Interact patiently and respectfully with your teachers and peers
- You MUST NOT record each other's online interactions
- Make sure you end the session as soon as the teacher indicates to do so.
- Provide feedback to teachers via email, if you have struggled with an aspect of the lesson or have not been able to access information.

Signed:

Date:

Year 7 - 10

More House School Online Home Learning Responsible User Agreement Name:

#### l agree that:

- I will be responsible for my behaviour and actions when using technology, this includes the resources that I access and the language that I use.
- I will make sure that all my communication with students, teachers or others using technology is responsible and sensible.
- I agree to only use my school email address to interact with my teachers.
- I understand that when using my school email address my use can be monitored.
- I understand that these rules are designed to help keep me safe and that if they are not followed school sanctions will be applied and my parent may be contacted.
- I will submit homework on time and understand that I will receive a debit if I fail to do so.

#### **Guidelines**

Whilst studying at home we request that you adhere to the following guidelines.

- Establish a quiet place to work where you will not get distracted.
- Try to ensure that you are practising conscious screen time. This means avoiding using your computer or phone during times when you are not studying. Make sure you have a purpose when you are online.

- Make sure you have all the required resources ready, check Google Classroom regularly for these.
- Interact patiently and respectfully with your teachers and peers
- Provide feedback to teachers via email, if you have struggled with an aspect of the lesson or have not been able to access information.

Signed:

Date:

Staff

#### More House School Staff Online Home Learning Responsible User Agreement Name:

#### l agree that:

- During lessons conducted via Google Meet I will only use technology for school purposes.
- I will be responsible for my behaviour and actions when using technology, this includes the resources that I access and the language that I use.
- I will make sure that all my communication with students is responsible and sensible and avoid having any family members in the background.
- I will not record or take photos of students during a face to face session.
- I agree to only use my school email address to interact with my pupils on an individual basis.
- I understand that when using my school email address my use can be monitored.
- I will not teach pupils 1:1 via Google Meet. I will include a member of SLT in these lessons.
- Make sure that you only end the session when all of the pupils have left the Google Meet. You should be the last one present in the meeting.

#### **Guidelines**

When using Google Meet, remember that this is an extension of the classroom and you should conduct yourself as you would in the classroom. This includes:

- Video conferencing from an environment that is quiet, safe and free from distractions. This should not be your bedroom and preferably there should be a neutral background.
- Be on time for your interactive session
- Make sure you have all the required resources ready and send these in advance when possible.
- Be dressed appropriately for learning (no pyjamas or revealing clothing)

Signed: Date:

# Appendix 4: Remote Learning, Partial or Full Closure of School

## Version control and dissemination

This is version 2.0 of this appendix. It will be reviewed by our designated safeguarding lead (DSL) or deputy DSL on a weekly basis as circumstances continue to evolve or following updated Department for Education advice or guidance. It is available on the school website (<u>https://www.morehouse.org.uk/88/school-policies</u>) and is made available to staff in the Staff Handbook.

## **E-safety Policy**

While the school continues to provide aspects of the curriculum online such as homework and research tasks, this E safety policy and the principles contained remain in full force and effect, including the policy statement, safeguarding information and responsibilities. As stated above, we will continue to update relevant policies and procedures to reflect the updated Department for Education advice or guidance.

#### **Online User Agreement**

All pupils, parents and staff have signed an online user agreement which remains in force during School reopening in September 2020. Please do refer to the Online User Agreement for the terms of agreement which makes clear the school's expectations of pupils engaging in remote learning;

#### Updates and advice - Pupils

We will continue to provide regular advice and guidance to pupils on staying safe online by way of the PSHE programme delivered during form time. This guidance raises awareness of both the benefits and hazards of online learning, pupils' responsibilities whilst online and how the pupils can report concerns. Additionally, we will continue to provide additional support for pupils who have been identified as vulnerable. Such support is coordinated by the SENCO, Director of Pastoral Care and Deputy DSL;

#### Updates and advice - Staff

We will continue to provide regular advice and guidance to staff on the provision of remote learning by way of training sessions, briefings and email updates.

#### **Updates and advice - Parents**

We will continue to provide regular advice and guidance to parents by way of safeguarding bulletins and email communications.

## ICT Tracking and monitoring

We will continue to maintain systems to monitor the use of school systems using filtering software.

#### Visiting Speakers - online

We have an updated policy for the use of visiting speakers which ensures the safeguarding of pupils whilst visiting speakers deliver talks.