Online Safety Policy

Date adopted by the MAT	July 2024
This policy is scheduled for review on	Annually

Contents

Statement of intent

Manor Multi Academy Trust understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the MAT/ School, therefore, there are a number of controls in place to ensure the safety of pupils and staff.

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

- Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- Contact: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our MAT has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for Schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2023) 'Keeping children safe in education 2023'
- DfE (2023) 'Teaching online safety in School'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following MAT/ School policies:

- Social Media Policy
- Acceptable Use Agreement
- Cyber-security Policy
- RPA Cyber Response and Recovery Plan
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- ICT and Electronic Devices Policy
- Prevent Duty Policy

Roles and responsibilities

The MAT & Directors will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant MAT/ School policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the MAT/ School's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.

- Organising engagement with parents to keep them up to date with current online safety issues and how the MAT/ School is keeping pupils safe.
- Working with the DSL and ICT Admin to conduct half-termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in School.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT Admin.
- Ensuring online safety is recognised as part of the MAT/ School's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the MAT/ School's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the MAT/ School community understand this procedure.
- Understanding the filtering and monitoring processes in place at the MAT/ School.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the MAT/ School.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the MAT/ School's provision and using this data to update the MAT/ School's procedures.
- Reporting to the Directors about online safety on a regular basis.
- Working with the Headteacher and ICT Admin to conduct termly light-touch reviews of this policy if required.
- Working with the Headteacher and Directors to update this policy on an annual basis.

ICT Admin will be responsible for:

- Providing technical support in the development and implementation of the MAT/ School's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Headteacher.
- Ensuring that the MAT/ School's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and Headteacher to conduct termly light-touch reviews of this policy if required.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the MAT/ School's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from MAT/ School staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.
The DSL has overall responsibility for the MAT/ School's approach to online safety, with support from deputies and the Headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all MAT/ School operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted termly on the topic of remaining safe online

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be

handled in line with the Child Protection and Safeguarding Policy. Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress. Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the Headteacher, it is reported to the CEO and /or chair of directors. Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Headteacher and ICT Admin, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.
Where there is a concern that illegal activity has taken place, the Headteacher contacts the police.

The MAT/ School avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy. All online safety incidents and the MAT/ School's response are recorded by the DSL.

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating, or upsetting text messages or using social media
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras

- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. WhatsApp, Facebook etc
- Abuse between young people in intimate relationships online i.e. relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The MAT/ School will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of MAT/ School, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a MAT/ School culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the

imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The MAT/ School will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The MAT/ School will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

The MAT/ School will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the MAT/ School premises or using MAT/ School-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion. Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the MAT/ School and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised. Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

Mental health

Staff will be aware that online activity both in and outside of the MAT/ School can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

Online hoaxes and harmful online challenges

For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, “harmful online challenges” refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.
Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the MAT/ School, they will report this to the DSL immediately.
The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the MAT/ School or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils’ age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL’s assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate. The DSL and headteacher will only implement a MAT/ School-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils’ exposure to the risk is considered and mitigated as far as possible.

Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- Cyber-enabled – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- Cyber-dependent – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The MAT/ School will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.
The DSL and Headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Relationships and health education
- PSHE
- Citizenship
- ICT

Online safety teaching is always appropriate to pupils' ages and developmental stages. Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support

- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in appendix A of this policy.

The DSL will be involved with the development of the MAT/ School's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The MAT/ School will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils. Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into the MAT/ School to help with the delivery of certain aspects of the online safety curriculum. The Headteacher and DSL will decide when it is appropriate to invite external groups into the MAT/ School and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions and are not worried about getting into trouble or being judged.
If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.
If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Laptops
- iPads
- Online subscriptions
- Office 365 / Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Use of smart technology

While The MAT/ School recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the MAT/ School will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the MAT/ School's Acceptable Use Agreement for Pupils.

Staff will use all smart technology and personal technology in line with the MAT/ School's Staff ICT and Electronic Devices Policy.

The MAT/ School recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the MAT/ School's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom. Where it is deemed necessary, The MAT/ School will ban pupils' use of personal technology whilst on the MAT/ School site.

Where there is a significant problem with the misuse of smart technology among pupils, the MAT/ School will discipline those involved in line with the MAT/ School's Behaviour Policy. The MAT/ School will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner. The MAT/ School will seek to

ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

Educating parents

The MAT/ School will work in partnership with parents to ensure pupils stay safe online at the MAT/ School and at home. Parents will be provided with information about the MAT/ School's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.
Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Twilight training sessions
- Newsletters
- Online resources

Internet access

Pupils, staff and other members of the MAT/ School community will only be granted access to the MAT/ School's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access in the MAT/ School office.
All members of the MAT/ School community will be encouraged to use the MAT/ School's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

Filtering and monitoring online activity

The governing board will ensure he MAT/ School's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for the MAT/ Schools and colleges'. The Directors will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the MAT/ School's safeguarding needs.

The filtering and monitoring systems the MAT/ School implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT Admin will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the Headteacher. Prior to making any changes to the filtering system, ICT Admin and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT Admin. Reports of inappropriate websites or materials will be made to an ICT Admin immediately, who will investigate the matter and makes any necessary changes. Deliberate breaches of the filtering system will be reported to the DSL and ICT Admin, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The MAT/ School's network and MAT/ School-owned devices will be appropriately monitored. All users of the network and MAT/ School-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT Admin. Firewalls will be switched on at all times. ICT Admin will review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates. Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to ICT Admin.

All members of staff will have their own unique usernames and private passwords to access the MAT/ School's systems. Pupils will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords will not expire, users will be allowed to change them.

Users will inform ICT Admin if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use. Full details of the MAT/ School's network security measures can be found in the Cyber-security Policy.

Emails

Access to and the use of emails will be managed in line with the Data Protection Policy and Acceptable Use Agreement.

Staff and pupils will be given approved MAT/ School email accounts and will only be able to use these accounts at MAT/ School and when doing MAT/ School-related work outside of MAT/ School hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the MAT/ School site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail, and report the matter to ICT Admin. The MAT/ School's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. ICT Admin will organise an annual assembly where they explain what a phishing email and other malicious emails might look like – this assembly will include information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

Generative artificial intelligence (AI)

The MAT/ School will take steps alongside it's MAT AI Policy to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The MAT/ School will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The MAT/ School will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The MAT/ School will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The MAT/ School will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

Social networking

The use of social media by staff and pupils will be managed in line with the MAT/ School's Social Media Policy.

The MAT / School website

The Headteacher will be responsible for the overall content of the MAT/ School website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website will be managed in line with the MAT/ School Website Policy.

Use of devices

Staff members and pupils will be issued with MAT/ School-owned devices to assist with their work, where necessary.
The use of personal devices on the MAT/ School premises and for the purposes of MAT/ School work will be managed in line with the Electronic Devices Policy.

Remote learning

All remote learning will be delivered in line with the MAT/ School's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

Virtual Meetings

Virtual Attendance at Face-to-Face Meetings

Where pupil parents / adults / PCAF Representatives or Directors / Trustees wish to attend a meeting by either telephone or video link the chair and governance professional must be notified at least 72 hours in advance of the meeting to ensure that appropriate arrangements can be made where possible. The people will be asked their reasons for not attending the meeting and the reason for this will be minuted and the relevant persons informed immediately.

Persons attending the meeting either by telephone or video conference will be entitled to vote on any issue providing they have been 'present' for the whole agenda item which the vote relates to. Where a secret ballot is required this will be facilitated where possible (e.g. by taking a telephone call off speaker phone and the governor sharing their vote verbally with the clerk). Where this is not possible the person(s) will be required either to vote publicly or abstain.

Persons attending the meeting virtually will contribute to the quorum for the meeting. If the technological link is lost, they will cease to contribute to the quorum, but this will not prevent the meeting continuing in their absence unless it has become inquorate.

Under normal circumstances, the meeting will be chaired by a person who is present at the meeting, however in extenuating circumstances, when the entire meeting is having to be held virtually, the meeting will be chaired by a person with relevant authority who themselves is attending remotely.

If, after all reasonable efforts, it does not prove possible for a person to participate by telephone or video conference the meeting may still proceed with its business provided it is otherwise quorate.

Ideally full meetings and scheduled committee meetings will be face-to-face meetings. However additional and extraordinary meetings can take place via telephone or video conference call as long as the usual qualifying quorum is 'present' on the call. If restrictions are imposed or recommended regarding face-to-face contact, the directors may vote to hold all regular meetings virtually until such time as it is practical to resume normal procedures.

This does not include panel meetings related to the policies of the MAT/ School such as HR, Complaints, Exclusions and Admissions.

In circumstances where all the attendees are meeting virtually the meeting will be chaired following the normal protocols that would apply as for a physical meeting.

Where a meeting is taking place virtually every effort will be made to enable all persons to access the meeting.

Where a meeting is taking place virtually the usual statutory notice arrangements will apply and all papers to be considered will be circulated at least seven days in advance of the meeting, except where the chair has exercised his/her right to waive the usual notice in an emergency.

Virtual meetings will be minuted in the same way as other meetings, as required.

Virtual meetings should not be recorded, or audio recorded by any person or the clerk without the approval of the chair and for a specified purpose.
The protocol to be followed by an individual or full meeting when a virtual meeting is being held is given below.

Virtual Meeting Protocol

This protocol should be followed when individuals are using alternative arrangements to participate and vote in meetings. We have been advised that Microsoft Teams (accessed via Office 365) is a secure platform to use for virtual meetings so this will be used unless advised otherwise.

People who wish to use these alternative arrangements should:

- restrict themselves to using the arrangements
- inform the clerk to the governing board that it is their intention to make use of this arrangement as soon as possible but no later than 72 hours before the meeting is due to take place once normal notice of the meeting has been given. (Only applies to individuals wishing to make use of the facility, it does not apply when the Board /Committee has decided to operate in this way due to guidance from Government or due to extenuating circumstances agreed by the Chair of Directors)
- communicate and co-operate with the clerk as necessary to ensure that the alternative arrangements can be put in place and work well for all concerned, and abide by the normal rules, procedures and code of conduct adopted by the governing board and give particular regard to the duty to maintain confidentiality.

The following will apply for meetings being held using the virtual meetings policy:

- The usual (statutory) notice and arrangements for issuing papers will apply except where the chair has exercised their right to waive the usual notice;
- The chair may decide that only urgent items are to be considered and the agenda and meeting papers will reflect this;
- All participants to receive clear instructions regarding how to access the meeting including where they can access support if they experience difficulty;
- The governing board will abide by their normal rules, procedures and code of conduct adopted by the governing board and give particular regard to the duty to maintain confidentiality;
- Governors will contribute towards a safe and secure environment for the meeting by giving due regard to the MAT/ School's policies relating to data protection, GDPR, and the appropriate use of ICT. The minutes of the meeting will be taken by the clerk to the governing board and the meeting should not be recorded by any governor or the clerk without the approval of the governing board and for a specified purpose.

Please follow the guidelines below as best you can

- Confirm attendance when asked to do so
- Check your own equipment, settings, including lighting and sound etc in advance of the meeting. (Make sure you will be clearly visible to others on the screen for the meeting)
- Please review all documents made available before the meeting and send questions by email in advance to the person responsible for that item giving as much notice as possible.
- Join the meeting on time
- Use the mute button. The Chair, Headteacher and Clerk should keep their microphones activated.
- Ensure confidentiality of the meeting, i.e. no one else is present in the room from which you are using your device.
- Use the chat facility to ask questions
- Say your name before starting to speak and remember to mute once finished
- If anyone must leave during the meeting, please make this clear at the end of an agenda item when it is your turn to speak and ensure it is acknowledged so the clerk can record it in the minutes.
- Where questions have been submitted in advance, answers will be given in the presentation and the presenter will identify that a question was asked in advance. Doing this will make the process more efficient so you are encouraged to provide questions in advance.
- At the end of the meeting all governors will be asked to confirm they are content.
- Be present i.e. the chair needs to ensure that there is active listening and that when people are not on camera they are not multitasking beyond taking their own notes
- Voting will be undertaken through the use of the chat/thumbs up facility. When voting is by secret ballot then the Forms app in Teams will be used.

Virtual Meeting Etiquette

- ✓ With so many people dialling in there can be lots of background noise so can everyone put their device on mute when they are not speaking?
- ✓ It will not be possible to easily interject with questions as information is being presented, so please note anything down as it occurs to you. You will be given the opportunity to ask it at the end of the agenda item.
- ✓ Please be patient - not everything will run perfectly smoothly!
- ✓ The chair will sum up the actions or conclusion after each item.