



ONLINE SAFETY POLICY

Policy reviewed by: Deputy Head Teacher/ Lead DSL

Date reviewed: November 2025

Date of next review: November 2026

Contents

1. Policy Aims	3
2. Legislation and guidance	3
3. Managing online safety	7
4. Handling online safety concerns	8
5. Education and Engagement Approaches	9
6. Remote Learning including homework	11
7. Cyberbullying and AI.....	12
8. Child on Child sexual abuse and harassment.....	13
9. Online Hate.....	13
10. Grooming and exploitation.....	13
11. Child sexual exploitation (CSE) and child criminal exploitation (CCE).....	14
12. Mental health.....	14
13. Online hoaxes and harmful online challenges.....	15
14. Radicalisation and Extremism	16
15. Cyber-crime	17
16. Online Safety Training for Staff.....	17
17. Supporting pupils use of the Internet within the curriculum.....	18
18. Safer Use of Technology	18
19. Learner's use of social media	19
20. Acceptable use of Technology in school	20
21. Use of Smart Technology	21
22. Educating parents/carers.....	22
23. Use of Devices	22
24. Security and Management	24
25. Managing the Safety of the School's Website	25
26. Managing Email	25
27. Indecent Images of Children (IIOC).....	26
28. Monitoring Role and Review of Cyber Security	27
29. References.....	31

1. Policy Aims

New technologies have become integral to the lives of children and young people today, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone.

Mayfield School identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

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

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

2. Legislation and guidance

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Online Safety Act 2023 and Ofcom Codes of Practice
- UK Data Use and Access Act 2025 (DUAA) – including recognising legitimate interests and ADM safeguards
- DfE (2022, updated 2025) Meeting digital and technology standards in schools and colleges – Cyber security standards
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2025) 'Keeping children safe in education'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'

- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- DfE (2024) Prevent Duty Guidance
- DfE (2025) Early years foundation stage statutory framework for group and school-based providers
- DfE (2019) Guidance - Safeguarding children and protecting professionals in early years settings: online safety guidance for practitioners
- Equality Act 2010 (as clarified by UK Supreme Court ruling, 2025)
- EU Artificial Intelligence Act – risk assessment and transparency obligations
- DfE (2024) Filtering and Monitoring Standards for Schools
- DfE (2024) Cyber Security Standards
- National Cyber Security Centre guidance
- Accessibility Regulations 2018

This policy operates in conjunction with the following school policies:

- Mayfield Child Protection and Safeguarding Policy
- Mayfield Behaviour Policy
- Mayfield Attendance Policy
- Mayfield School children with health needs who cannot attend school
- Mayfield School Remote Learning Policy
- EIAT Acceptable Use Policy
- EIAT Staff Code of Conduct
- EIAT Disciplinary Policy
- EIAT Data Protection & Retention Policies
- EIAT Whistleblowing Policy

Roles and Responsibilities

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Executive Head Teacher, with the support of DSL and the Governing Body, aims to embed safe practices into the culture of the school.

The Local Governing Body (LGB)

The LGB has overall responsibility for monitoring this policy and holding the Executive Head Teacher to account for its implementation.

The LGB will nominate a governor to oversee safeguarding including online safety; our nominated governor is Jodie Duffin.

Responsibilities will include arranging regular meetings with appropriate staff to discuss online safety and monitor any incidents of misuse of IT.

All governors will ensure that they have read and understand this policy and will agree and adhere to the terms on acceptable use of the school's IT systems and the internet.

Executive Head Teacher / Senior Leaders

The Executive Head Teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

- The Executive Head Teacher is responsible for ensuring the safety (including online safety) of members of the school community. The day-to-day responsibility for online safety will be delegated to the Functional Skills Curriculum Lead/Designated Safeguarding Lead.
- The Executive Head Teacher is responsible for the implementation and effectiveness of this policy. He is also responsible for reporting to the Local Governing Body on the effectiveness of the policy and, if necessary, make any necessary recommendations re further improvement.
- The Executive Head Teacher / Senior Leaders are responsible for ensuring that the Functional Skills Curriculum Lead/ Designated Safeguarding Lead and other relevant staff receive suitable CPD to enable them to carry out their online safety roles.
- The Executive Head Teacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.
- The Executive Head Teacher and Lead DSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in the safeguarding policy.

The DSL takes lead responsibility for online safety in school in particular:

- Supporting the Executive Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
 - Working with the Executive Head Teacher, IT team and other staff, as necessary, to address any online safety issues or incidents
 - Ensuring that any online safety incidents are logged and dealt with appropriately
 - Updating and delivering staff training on online safety
 - Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Executive Head Teacher and if necessary, the Local Governing Body

The IT Team

The IT team is responsible for:

- Meeting regularly with the Lead DSL to ensure filtering and monitoring software is operating effectively and is up to date with local, regional and national updates relating to safeguarding including Prevent
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate

content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Helping to ensure that any online safety incidents are logged and dealt with appropriately
- Maintain records of staff AUP acceptance via online Forms electronic signature and wet signature where applicable
- Regular auditing, system and practice/policy updates which enable the DfE monitoring and filtering and the DfE cyber security standards to be upheld

Members of Staff will

- Take responsibility for the security of IT systems and electronic data they use or have access to
- Will sign/accept the EIAT AUP at staff induction and as required
- Model good online behaviours
- Maintain a professional level of conduct in their personal use of technology
- Have an awareness of online safety issues and GDPR legislation relating to practice relevant to their role
- Ensure they are familiar with, and understand, the indicators that pupils may be unsafe online
- Report concerns in line with the school's reporting procedure
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum

Parents

Parents are expected to:

- Be aware of the measures the school takes to ensure IT safety
- Follow Acceptable Use Agreement if their child has home use of any mobile technology provided by the school and sign an agreement regarding this.
- School will provide parents with information on online safety as part of the Relationships and Health Education curriculum, to support parents in keeping their children safe online. There is a section on the school website dedicated to this
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Executive Head Teacher and/or the DSL

Visitors including volunteers

- Visitors, such as training providers, who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

Pupils

- Are responsible for using the school IT systems in accordance with the Student / Pupil Acceptable Use Agreement, which they will be expected to agree to before being given access to school systems, where appropriate for age and ability
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, where appropriate for age and ability
- Will be expected to follow school rules relating to this policy e.g., safe use of cameras, cyber-bullying etc.
- Should understand that the school's online safety Policy covers their actions out of school, if related to their membership of the school, where appropriate for age and ability

Shared access at HML

The HML (Holte Mayfield Lozells) site is a shared site between 3 schools. The NHS Special School Nursing Team are also based at Mayfield School. Each organisation is responsible for their site online safety procedures. Wi-Fi access is provided and each site has its own password protected logins and administration rights protecting user access to the internet and school IT systems.

Vulnerable Pupils

- Mayfield School is a school for pupils with a range of special educational needs and is aware that some pupils are more vulnerable online due to a range of factors. This may include but is not limited to children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss. We recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation. The school will ensure that differentiated and appropriate online safety education, access, and support is provided to vulnerable pupils.
- Mayfield School is a split site provision. Pupils educated at the Heathfield Road site have complex and high functioning autism. Pupils at the Wheeler Street site have a range of special educational needs including severe and moderate learning difficulties. This means that the life experiences and the communication needs of our pupils and their families must be considered carefully when implementing the policy. We recognise that all pupils are vulnerable to exploitation and the impacts of using technology and therefore we differentiate accordingly to meet the individual needs of all learners.

3. 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 Lead DSL has overall responsibility for the school's approach to online safety, with support from deputies and the Executive Head Teacher where appropriate and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

The school leadership team has reviewed the school's online safety using the 360 safe online safety self-review tool which audit's the policies, informs practice and supports targeted CPD training for staff in a range of roles. The effectiveness of this tool is reviewed by the curriculum leads and senior leaders responsible for quality of education and safeguarding through curriculum and safeguarding audits.

The importance of online safety is integrated across all school operations in the following ways:

- Staff 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
- Personal Development Days

4. Handling online safety concerns

All staff must refer to the Mayfield Safeguarding and Child Protection Policy if they are concerned about a child's safety.

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.

Concerns regarding a staff member's misuse and or online behaviour are reported to the Executive Head Teacher, who decides on the best course of action in line with the relevant policies, e.g., the Staff Code of Conduct, whistleblowing policy and Disciplinary Policy and Procedures. If the concern is about the Executive Head Teacher, it is reported to the chair of governors. Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer)

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g., the Executive Head Teacher and IT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g., the Behavioural Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Executive Head Teacher contacts the police.

The school avoids unnecessarily criminalising pupils, eg. calling the police, where criminal behaviour is thought to be inadvertent and because of ignorance or normal developmental curiosity, eg a pupil has taken and distributed indecent imagery of themselves. The Executive Head Teacher and Lead DSL will seek support and guidance from the NPCC 'When to call the police; guidance for schools and colleges.'

All online safety incidents and the school's response are recorded by the DSL and:

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns

- The DSL will record these issues in line with the school's safeguarding and child protection policy
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Birmingham Children's Trust thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required

Procedures for Responding to Specific Online Incidents or Concerns

Youth Produced Sexual Imagery or "Sexting"

The school will follow the advice as set out in the non-statutory

- UKCCIS (The UK Council for Child Internet Safety guidance): 'Sexting in Schools and Colleges UKCCIS'
- Mayfield School will ensure that all members of the community are made aware of the potential social, psychological, and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery

Dealing with 'Sexting'

- If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will act in accordance with our Child protection and Safeguarding policies and the relevant DfE guidance.

5. Education and Engagement Approaches

Online safety and the curriculum

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

- Computing
- PSHE

Online safety teaching is always appropriate to pupils' ages and developmental stages. It teaches pupils responsible ethics and how to manage risks. Exposure to risk is therefore managed in a safe environment.

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 PSHE for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g., with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks pupils may face online are always considered when developing the curriculum.

The Functional Skills Curriculum Lead and Lead DSL is involved with the development of the 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.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g., designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

The 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 review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Executive Head Teacher and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the curriculum lead, class teacher and DSL 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 advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are 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 ensures 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.

ClassDojo

Mayfield School uses a digital platform called ClassDojo that connects teachers, pupils, and families all in one space. That can mean easy sharing of work but also better communication and monitoring all round. It allows the school to share with parents and pupils how to use social media safely. Information can be uploaded to a pupils own portfolio and comment on the class story; this is monitored by class staff and the ClassDojo champion an Associate Head of School and Deputy Designated safeguarding Lead. Moderation of portfolio content and class story comments allows the school to identify and address any individual reports, behaviours, comments that may indicate a need for an intervention.

Parents are informed that during the school day class teams will be engaged in teaching and learning and therefore we have allocated quiet times between 8am – 4pm.

6. Remote Learning including homework

The school will risk assess the technology use for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed and can establish secure connections.

During a period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online
- Ensure parents are aware of what their children are being asked to do, e.g., sites they have been asked to use and staff they will interact with

- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites
- Direct parents to useful resources to help them keep their children safe online

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g., anti-virus software, on devices not owned by the school.

During times when homework is provided staff will provide pre checked educational sites and or educational sites that require a login/password. Work set will avoid internet search engines. Parental knowledge and understanding of online safety will be provided during online safety workshops led by our CEOP ambassador and IT.

7. Cyberbullying and artificial intelligence

Cyberbullying can include the following:

- Threatening, intimidating, or upsetting text messages
- 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
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites, and social networking sites, e.g., Facebook

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 our behaviour policy.

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Mayfield School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Mayfield School will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school or Trust.

8. 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 school and 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
- Up skirting, 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

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 school responds to all concerns regarding online peer-on-peer sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the DSL, who will investigate the matter in line with the Peer-on-peer Abuse Policy and the Child Protection and Safeguarding Policy.

9. Online Hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at Mayfield School and will be responded to in line with existing school policies, including the Behaviour and Safeguarding policy
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures
- The Police will be contacted if a criminal offence is suspected
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Birmingham Children's Trust and/or West Midlands Police
- Further information can be found at:
www.educateagainsthate.com/resources/prevent-duty-guidance-update-september-2023-a-briefing-note-for-schools-and-early-years-providers

10. 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, including the following:

- The pupil believes they are talking to another child, when they are talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- 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.
- Having an older boyfriend or girlfriend, usually one that does not attend the 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.

11. 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.

12. Mental health

The internet, particularly social media, can be the root cause of several mental health issues in pupils, e.g., low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of 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 school safeguarding and curriculum procedures including early help.

13. 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 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 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 Executive Head Teacher 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, e.g., it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, 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 even to individual children at risk where appropriate.

The DSL and Executive Head Teacher will only implement a 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.

14. Radicalisation and Extremism

To be read in conjunction with the Prevent duty guidance: for England and Wales- GOV.UK (www.gov.uk) and Keeping Children Safe in Education 2024.

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.

The first objective of Prevent has been changed to "tackle the ideological causes of terrorism". The ideological component of terrorism is what sets it apart from other acts of serious violence. The guidance recommends education settings consider ideology when delivering all aspects of Prevent. The guidance introduces a new theme - 'Reducing Permissive Environments' to tackle the ideological causes of terrorism. For schools and early years, this includes the existing considerations of building resilience through the curriculum and **having effective IT and visiting speaker policies to reduce exposure to radicalising influences.**

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.

- Mayfield School will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school; The firewalled boundary is monitored by CoConnect and onGuard by netsweeper and all devices filter terrorism content and offensive language. Monitoring also supports the school in identifying who is accessing this material and appropriate actions put in place as per the safeguarding policy
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately, and action will be taken in line with the Safeguarding and Child protection policy and the Prevent Duty Policy
- If the school is concerned that member of staff may be at risk of radicalisation online, the Executive Head Teacher will be informed immediately, and action will

be taken in line with the Safeguarding and Child Protection, Whistleblowing, Staff Code of Conduct and Prevent Duty policies

- The school will regularly update its prevent risk assessment and action plan and implement actions as required
- The school will provide updated annual training and on-going updates aligned to national and local guidance – refer to www.birmingham.gov.uk/downloads/download/773/the_prevent_duty

15. 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 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 regarding 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, curriculum Lead and Executive Head Teacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g., the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

As required the school will report cyber attacks to National Cyber Security Centre (NCSC), ICO if there has been a breach of personal data, Action Fraud, DfE.

16. Online Safety Training for Staff

The EIAT CEOP Ambassador is Ryan Perrens.

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online 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 Conduct and Commerce) as well as our professional practice expectations

- Make staff aware that school systems are monitored, and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school
- 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 online safety concerns affecting pupils, colleagues, or other members of the school community
- Information about the school's full responses to online safeguarding incidents can be found in Anti-Bullying Policy and Child Protection and Safeguarding Policy

17. Supporting pupils use of the Internet within the curriculum

The schools will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:

- Ensuring education regarding safe and responsible use precedes internet access
- Including online safety in the PSHE, RSE and Computing programmes of study, covering use both at home school and home. (e.g., Friendship/Respect week, Safer Internet Day, regular focus on online safety)
- Reinforcing online safety messages whenever technology or the internet is in use
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval, and evaluation
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

18. Safer Use of Technology

Classroom Use

Mayfield School uses a wide range of technology. This includes access to:

- Computers, laptops, tablets, and other digital devices
- Internet which may include search engines and educational websites
- School learning platform/intranet
- Email
- Games consoles and other games-based technologies
- Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the EIAT Acceptable Use Policy (AUP) and with appropriate safety and security measures in place. This will

be done through education of the children, filters that are in place and careful supervision whilst they are being used. This use must also be in class time only. It will be the responsibility of the member of staff who has planned for children to use devices, to ensure that the school guidelines are strictly followed

- Members of staff will always evaluate websites, tools, and apps fully before use in the classroom or recommending for use at home this will be reviewed as on going.
- The school will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information
- Supervision of pupils will be appropriate to their age and ability

Early Years Foundation Stage and Key Stage 1

- Pupils' access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils' age and ability

Key Stage 2 – Key Stage 5

- Pupils will use age-appropriate search engines and online tools.
- Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability

Staff should ensure that mobile technology is locked when left unattended to prevent unauthorised access. It should be locked away securely at the end of the session.

19. Learner's use of social media

Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach via age-appropriate sites and resources. We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for learners under the required age as outlined in the services terms and conditions

The school will support pupils to read and understand the EIAT AUP in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with internet access
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation
- Rewarding positive use of technology by pupils
- Implementing appropriate peer education approaches
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments
- Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation. Pupils contribute to rules around use of IT and how to keep safe on line via lessons
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are taught the importance of keeping information such as their password safe and secure
- Rules for the use of IT systems / internet will be made available for pupils to read
- Staff should act as good role models in their use of IT, the internet, and mobile devices
- Where Pupils are allowed to freely search the internet, e.g., using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g., racism, drugs, and discrimination) that would normally result in internet searches being blocked
- Using support, such as external visitors, where appropriate, to complement and support the school's internal online safety education approaches
- Report Remove is a tool that allows young people to report an image or video shared online, to see if it's possible to get it taken down. Provided by Childline and IWF, it keeps the young person informed at each stage of their report, and provides further support where necessary. <https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/report-remove/>

20. Acceptable use of Technology in school

All staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet. Parents will be expected to sign an agreement if their child is given any school mobile technology to use at home. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant as part of the electronic signing in system.

Our children only use IT under supervision, and do not bring personal mobile technology into school. A small number who travel independently may bring a phone in for safety – these are locked away during the school day by the class teacher.

School external visitors such as Speech & Language (SALT) can access the school Wi-Fi via a key code which provides access to the school web browser 'Garden Wall;' they will require a certificate to be uploaded to their devices which will then have the filtering controls as per a school user; the IT department will be responsible for installing this. Monitoring of external use will be completed by site associate heads of school and reported to the lead DSL. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

Staff will be allocated password protected access to the school IT system. They should ensure their password meets the complexity requirements. They should not tell anyone their password, write it down on paper or electronically, or share it with others. Multi-factor Authentication (MFA) applies when further security levels are required for example CPOMS (Child Protection Online Management System) used by the Designated Safeguarding Leads. Senior Leaders and administration staff and any staff who have access to sensitive personal information will require MFA access. They should not log on using anybody else's account and they must ensure that they log off or lock

the screen when leaving a computer. Others should not share use of the system using a single password. School provides all staff with devices.

We will monitor the websites visited by pupils, staff, volunteers, governors, and visitors (where relevant) to ensure they comply with the above.

Additional software must not be downloaded onto school devices without consent (discuss with the IT team if there is a piece of software you require related to your work).

Refer to the EIAT Acceptable Use Policy.

21. Use of Smart Technology

Mayfield School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff, and parents/carers, but technologies need to be used safely and appropriately within school.

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

Staff will ensure that all mobile phones are password protected even when securely locked away. Some staff in school (leadership, pastoral managers) have use of a mobile phone as part of their duties therefore pupil access is possible. All phones will be locked with use of a password to gain access. Due to advances in digital technology, the use of mobile phones and cameras has been extended to include other electronic devices with imaging and sharing capabilities.

Smart watches (such as apple watches) must be on flight mode at all times when pupils are in school as staff should not be distracted by personal messages and alerts when supervising pupils. Smart watches must not be worn in early years areas of the school.

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

The 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 school's acceptable use of IT 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 school will ban pupil's use of personal technology whilst on school site. Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behavioural Policy.

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

The school will consider the 4C's (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

22. Educating parents/carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

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

- Providing information and guidance on online safety in a variety of formats and languages. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, parental workshops
- Drawing their attention to the Mayfield online safety policy and expectations in newsletters, letters, our prospectus and on our website
- Requesting that they read online safety information as part of joining our school, for example, within our home school agreement
- Requiring them to read the EIAT Acceptable Use Policy (AUP) and discuss its implications with their children
- Engage with information on Class Dojo

23. Use of Devices

Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Safeguarding and Child protection, Data security and Acceptable use.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place during lesson time
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
- Not use personal devices during teaching periods, unless written permission has been given by the Executive Head Teacher /LT, such as in emergency circumstances
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers. The 3CX app allows staff to call families which displays the school contact number or staff can block their number in such cases during a lockdown and remote learning is required
- Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead

Staff will not use personal devices, such as: mobile phones, tablets, or cameras:

- To take photos or videos of pupils and will only use work-provided equipment for this purpose
- Directly with pupils, and will only use work-provided equipment during lessons/educational activities
- If a member of staff breaches the school policy, action will be taken in line with the Staff Code of Conduct
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted

Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences
- Mayfield School expects pupil's personal devices and mobile phones to be kept in a secure place designated by the school and switched off
- Mobile phones or personal devices will not be used by pupils at any time during the school day
- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Bullying policy, or could contain youth produced sexual imagery (sexting)
- Searches of mobile phone or personal devices will only be carried out in accordance with the DFE's Searching, Screening, Confiscation Guidance
- Pupils' mobile phones or devices may be searched by a member of the leadership team, with the consent of a parent/ carer following the DFE's Searching, Screening, Confiscation Guidance
- Mobile phones and devices that have been confiscated will be released to parents or carers.

- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation

Visitors' Use of Personal Devices and Mobile Phones

(Refer to page 21 above)

- Parents, carers, and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the EIAT's AUP as per the electronic visitor management system. Due to advances in digital technology, the use of mobile phones and cameras has been extended to include other electronic devices with imaging and sharing capabilities.
- The school will ensure appropriate signage and information is provided to inform parents, carers, and visitors of expectations of use
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy

Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with pupils or parents/ carers is required
- School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff
- School mobile phones and devices will always be used in accordance with the Acceptable Use Policy and other relevant policies

24. Security and Management

Information Systems

The school take appropriate steps to ensure the security of our information systems including:

- Virus protection being updated regularly. Sophos Antivirus with Intercept X is enabled and active on computers across the school. iOS device's applications are controlled and limited through our mobile device mechanisms MDM (Jamf).
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems
- Any use of a portable storage device would be appropriately encrypted (currently not applicable)
- Not downloading unapproved software to work devices or opening unfamiliar email attachments
- Regularly checking files held on the schools' networks
- The appropriate use of user logins and passwords to access the school networks
- All users are expected to log off or lock their screens/devices if systems are unattended

Mobile technology

- Staff school laptops should not be left in cars. If this is unavoidable, it should be temporarily locked out of sight in the boot

- Staff should only use the laptop which is allocated to them
- Mobile technology devices for pupil use are stored in a locked cupboard. Access is available via classroom staff
- Mobile Technology assigned to a member of staff as part of their role and responsibility must have a passcode or device lock so unauthorised people cannot access the content
- When they are not using a device staff should ensure that it is locked to prevent unauthorised access
- No personal devices belonging to staff or children are to be used during lessons at school. In the event of an emergency staff may need to use their own devices such as mobile phones, these are to be used during staff break times only, in rooms where no pupils have access and kept on silent in locked cupboards as per staff code of conduct.

25. Managing the Safety of the School's Website

The schools will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).

- The schools will ensure that our website complies with guidelines for publications including accessibility; data protection; respect for intellectual property rights; privacy policies and copyright
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email, and telephone number
- The administrator account for each school's website will be secured with an appropriately strong password

26. Managing Email

Access to schools' email systems will always take place in accordance with EIAT Data protection policy and in line the EIAT AUPs and EIAT Code of conduct.

- Staff should take care when forwarding any chain messages/emails that sensitive/confidential information is not inadvertently sent to an unauthorised individual.
- Spam or junk mail will be blocked and reported to the email provider
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email
- School email addresses and other official contact details will not be used for setting up personal social media accounts
- Email access on personal devices should be through the Outlook App and should require pin code/password
- Members of the school community will immediately tell the DSL Team if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked in school

Staff

All members of staff are provided with a specific school email address, to use for all official communication. The use of personal email addresses by staff for any official school business is not permitted. Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and parents.

Pupils

Pupils will use school provided email accounts for educational purposes. Parents will be asked to provide consent should there be an educational requirement. Pupils will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.

27. Indecent Images of Children (IIOC)

Mayfield School will ensure that all members of the school are made aware of the possible consequences of accessing Indecent Images of Children (IIOC):

- The school will act regarding IIOC on school equipment and/or personal equipment, even if access took place off site
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls, and anti-spam software

If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through West Midlands Police and/or the Birmingham Children's Trust

If made aware of IIOC, the school will:

- Act in accordance with the schools safeguarding and child protection and the relevant Birmingham Children's Trust procedures
- Immediately notify the school Designated Safeguard Lead.
- Store any devices involved securely
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), West Midlands police or the LADO team

If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:

- Ensure that the Designated Safeguard Lead is informed
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
- Ensure that any copies that exist of the image, for example in emails, are deleted
- Report concerns, as appropriate to parents and carers

If made aware that indecent images of children have been found on the school devices, the school will:

- Ensure that the Designated Safeguard Lead is informed
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk

- Ensure that any copies that exist of the image, for example in emails, are deleted
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate)
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only
- Report concerns, as appropriate to parents and carers

If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:

- Ensure that the Executive Head Teacher is informed
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy
- Quarantine any devices until police advice has been sought

28. Monitoring Role and Review of Cyber Security

Monitoring will take place by the following:

Executive Head Teacher – Victoria Miller

Curriculum Leaders:

- Update curriculum plans
- Support the training of staff
- Educate and inform parents
- Working with DSLs, leaders and the wider teaching team to ensure the implementation of curriculum delivery and the delivery of online safety training to a range of stakeholders

Designated Safeguarding Lead - Caroline Mace will:

Online Safety

Be responsible for monitoring and filtering of online safety as outlined in Keeping Children Safe in Education and the filtering and monitoring standards for schools, working with the IT, LT and curriculum lead team.

MAT Compliance/ Data Protection Officer will carry out:

Data protection impact assessments

Are routinely carried out by our DPO for any repositories for personal data that we opt to use within the trust.

Trust and School IT Teams will:

Monitor Application Security

The installation of new applications is controlled by IT staff through policies that limit user installation. IT staff check new applications for security vulnerabilities before installation. Further, our Antivirus software instantly flags and quarantines applications that present malware or viruses.

Be responsible for accounts

High level accounts are all secured with complex long passwords and MFA. There are always 2 top level accounts to ensure continuity of access. User account creation and removal is part of existing joining and leaving protocols.

IT user accounts are set up according to job role and access level required to carry out tasks. Staff accounts are similarly limited to provide access to only what is required for the job role. Student accounts are further limited, especially where simpler passwords are used to meet the students need's. The network is appropriately segmented for additional security.

Monitoring Licencing and Patching

All software and operating systems used are licenced and automatically patched where possible. Where not, periodic checks are carried out and manual updates pushed/carried out. We employ a network management solution Netsupport DNA that provides an inventory of all computer hardware, software and licencing. This is used for monitoring and identifying areas for replacement or upgrade.

The school recognises that the online world is constantly changing; therefore, the DSL, IT technicians and the Executive Head Teacher conduct half-termly light-touch reviews of this policy to evaluate its effectiveness

The governing board, Executive Head Teacher and DSL review this policy in full on an annual basis and following any online safety incidents

The next scheduled review date for this policy is November 2026

Any changes made to this policy are communicated to all members of the school community.

Filtering and Monitoring Online Activity

Monitoring

The Executive Head Teacher /Deputy Head Teacher / Lead DSL or other authorised members of staff may inspect or monitor any IT equipment owned or leased by the school at any time without prior notice.

Monitoring includes intercept, access, inspect, record, and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, e-mail, texts, or image) involving employees without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards, and procedures, to ensure the effective operation of School IT, for quality control or training purposes, to comply with a Subject Access Request under the GDPR, or to prevent or detect crime.

- Mayfield School governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks

- The governors and leaders are aware of the need to prevent “over blocking”, as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding
- The school's decision regarding filtering and monitoring has been informed by a risk assessment, considering our school's specific needs and circumstances
- 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 leadership team; all changes to the filtering policy are logged and recorded
- The 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 classroom management and regular education about safe and responsible use is essential

The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:

- Physical monitoring and supervision of the children using the devices
- Monitoring internet and web access through the technology monitoring services provided by: CoConnect and onGuard by Netsweeper
- The school has a clear procedure for responding to concerns identified via monitoring approaches. Issues should be raised and will be responded to, by following the Safeguarding and Child Protection procedures that are already in place
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights, and privacy legislation

The following members of staff will be responsible for the supervision and monitoring of CoConnect and onGuard by Netsweeper:

- Executive Head Teacher - Vicky Miller - v.miller@mayfield.eiat.org.uk
- Deputy Head Teacher & Lead DSL - Caroline Mace c.mace@mayfield.eiat.org.uk
- Deputy Head Teacher - Hayley Tinsley - h.tinsley@mayfield.eiat.org.uk
- Associate Head of School – Wheeler Street - Bianca Jackson
b.jackson@mayfield.eiat.org.uk
- Associate Head of School – Heathfield Road – Christa Haddleton –
c.haddleton@mayfield.eiat.org.uk

Filtering

The schools use educational broadband connectivity through: CoConnect

- The school's filtering systems are provided by onGuard by NetSweeper which blocks all sites on the Internet Watch Foundation (IWF) list, which can be categories as: pornography, racial hatred, extremism, gaming, and sites of an illegal nature.

- The school works alongside their respective providers to ensure that our filtering policy is continually reviewed and is in line with UK Safer Internet Centre and KCSIE 2025.

Breaches of Practice

A referral to the police will be made if criminal activity is detected. Any policy breaches will be investigated. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate. This could, if necessary, include disciplinary or safeguarding processes. Such breaches may also lead to criminal or civil proceedings.

The school reserves the right to monitor staff internet usage and behaviour relating to use of social media. The school considers that valid reasons for this include concerns that social media/internet sites have been accessed in breach of this Policy.

29. References

Useful Links and Resources

For Educational Settings

- Birmingham City Council Education Safeguarding Team: Children's Advice and Support Service (CASS): Telephone: 0121 303 1888
- Keeping Children Safe in Education (September 2025)

West Midlands Police

- In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact West Midlands Police via 101

National Links and Resources

[Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/keeping-children-safe-in-education-2025)

Action Counters Terrorism: <https://act.campaign.gov.uk/>

Action Fraud: www.actionfraud.police.uk

CEOP: www.thinkuknow.co.uk www.ceop.police.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

ChildLine: www.childline.org.uk

Net Aware: www.net-aware.org.uk

UK Safer Internet Centre: www.saferinternet.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

360 Safe Self-Review tool for schools: www.360safe.org.uk

EducateAgainstHate :[Prevent duty guidance Educate Against Hate](https://www.educateagainsthate.org.uk/prevent-duty-guidance)