MANCHESTER MUSLIM PREPARATORY SCHOOL

FAITH • LEARNING • LIFE

Online Safety and E-Safety Policy

Last reviewed on:	November 2026
Next review due by:	July 2027

This Policy takes effect from 1 September 2026 and reflects Keeping Children Safe in Education (KCSIE) 2026 and other statutory guidance applicable from that date.

Contents

1. Aims
2. Legislation and guidance
3. Roles and responsibilities
4. Educating pupils about online safety
5. Educating parents about online safety
6. Cyber-bullying
7. Acceptable use of ICT systems, internet and email
8. Use of mobile phones, smart technology and personal devices
8.1 Pupils
8.2 Staff
9. Staff using work devices outside school
10. How the school will respond to issues of misuse
11. Training
12. Monitoring arrangements
13. Links with other policies
Appendix 1A: EYFS Acceptable Use Agreement (Pupils and Parents/Carers)
Appendix 1B:KS1 Acceptable Use Agreement (Pupils and Parents/Carers)
Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)
Acceptable Use Agreement – Staff, trustees, volunteers and visitors: refer to ICT and Internet Acceptable Use Policy
Appendix 3: Online safety incident report log
Appendix 4: Online Safety Incident Response Procedure
Appendix 5: Artificial intelligence (AI): Safe use by staff and pupils

1. Aims

Our school aims to:

Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees

Identify and support groups of pupils that are potentially at greater risk of harm online than others

Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following four categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, **extreme sexual or physical violence**, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact** – being subjected to harmful online interaction with other users **or with generative AI applications that simulate interaction**, including peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention of grooming or exploiting them for sexual, criminal, financial or other purposes.
- **Conduct** – online behaviour that increases the likelihood of, or causes, harm, including making, sending or receiving explicit images, **including those generated using AI**, and online bullying.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and financial scams.

2. Legislation and guidance

This policy has been developed with regard to relevant legislation and statutory guidance, including:

- **Keeping Children Safe in Education 2026 (KCSIE)**;
- the **Education (Independent School Standards) Regulations 2014** and the DfE's **Independent School Standards Guidance**;
- **Working Together to Safeguard Children 2026**;
- the **Early Years Foundation Stage (EYFS) statutory framework for group and school-based providers**, where applicable;
- the DfE's statutory guidance on **Relationships Education, Relationships and Sex Education (RSE) and Health Education**, as applicable to the school;
- the DfE's statutory guidance **Mobile phones in schools**;
- the **Prevent Duty Guidance: England and Wales (2023)**;
- the **Equality Act 2010**; and
- relevant data protection legislation, including the **UK GDPR**, the **Data Protection Act 2018** and the **Data (Use and Access) Act 2025**.

This policy also takes account of relevant DfE and UK Council for Internet Safety (UKCIS) guidance and standards, including guidance on **teaching online safety, filtering and monitoring, digital**

and cyber security, searching, screening and confiscation, sharing nudes and semi-nudes, and the safe and appropriate use of generative artificial intelligence (AI) in education.

As an independent school, MMPS is not required to follow the National Curriculum. However, the school draws on the National Curriculum computing programmes of study, where appropriate, when planning age-appropriate online safety education.

3. Roles and responsibilities

3.1 The board of trustees

The trust board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The trust board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The trust board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The trust board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Trust Board will ensure that pupils are taught how to keep themselves and others safe, including online.

The trust board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Trust Board will ensure that the effectiveness of the school's filtering and monitoring arrangements is reviewed at least once every academic year. The review will be led by the senior member of the Senior Leadership Team (SLT) with responsibility for filtering and monitoring, supported by the DSL and ICT Manager/IT support. The review will include checks that filtering and monitoring arrangements are working appropriately across all internet-connected devices in all relevant locations, and a record will be kept of the checks undertaken, any findings and actions required.

All trustees will:

Ensure that they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (ICT & Internet Acceptable Use Policy)

Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures

Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

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

3.3 The designated safeguarding lead (DSL)

Details of the school's Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (DDSL) are set out in the Child Protection and Safeguarding Policy.

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

Ensuring that staff understand this policy and that it is being implemented consistently throughout the school

Working with the trustees to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly

Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

Providing trustees with assurance that filtering and monitoring systems are working effectively and reviewed regularly

Working with the ICT manager to make sure the appropriate systems and processes are in place

Working with the ICT manager and other staff, as necessary, to address any online safety issues or incidents

Managing all online safety issues and incidents in line with the school's child protection policy

Responding to safeguarding concerns identified by filtering and monitoring

Supporting the annual review of the effectiveness of the school's filtering and monitoring arrangements, including checks across internet-connected devices and relevant locations, and ensuring that identified safeguarding concerns or weaknesses are acted upon promptly.

Making sure that any online safety incidents are recorded and dealt with appropriately in line with this policy and the Child Protection and Safeguarding Policy (see Appendix 3).

Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

Updating and supporting the delivery of staff training and regular updates on online safety, including filtering and monitoring, emerging online risks and the safe use of artificial intelligence.

Liaising with other agencies and/or external services if necessary

Undertaking annual risk assessments that consider and reflect the risks pupils face

Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

Providing regular information and assurance to the Trust Board on online safety matters, including significant incidents, emerging risks and the effectiveness of filtering and monitoring arrangements.

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

Putting in place and maintaining appropriate filtering and monitoring systems on school devices and networks, working with the DSL and Headteacher to ensure that these meet the school's safeguarding needs and the DfE filtering and monitoring standards. This includes supporting the annual review of effectiveness and considering the capability and limitations of systems in relation to real-time, dynamic, personalised and AI-generated content.

Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

Conducting regular security checks and monitoring of the school's ICT systems, with the frequency determined by risk and the school's technical and safeguarding requirements.

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Reporting online safety incidents, filtering or monitoring concerns and suspected system failures promptly to the DSL, and providing technical support to investigate and respond to incidents where required.

Supporting the preservation of relevant technical information or evidence where an online safety, cyber-bullying, safeguarding or data-security incident occurs.

3.5 All staff and volunteers

All staff, including supply and agency staff, contractors and volunteers, are responsible for:

Maintaining an understanding of this policy

Implementing this policy consistently

Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (ICT & Internet Acceptable Use Policy), and ensuring that pupils follow the school's terms on acceptable use (Appendices 1A, 1B and 2)

Reporting all online safety concerns or incidents promptly to the DSL/DDSL and ensuring that they are recorded and dealt with appropriately in accordance with this policy and the Child Protection and Safeguarding Policy (see Appendix 3).

Reporting incidents of cyber-bullying and other harmful online behaviour and responding in accordance with the school's Behaviour and Anti-Bullying Policies and, where there is a safeguarding concern, the Child Protection and Safeguarding Policy.

Responding appropriately to all reports and concerns about child-on-child abuse, including sexual violence and sexual harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

Reporting any concerns about the school's filtering and monitoring systems, including suspected failures, inappropriate content being accessible or attempts to circumvent the systems, promptly to the DSL and ICT Manager.

Using artificial intelligence (AI) tools only in accordance with this policy, the school's approved arrangements and any relevant data protection requirements, and reporting any safeguarding, privacy or security concerns arising from the use of AI.

3.6 Parents/carers

Parents/carers are expected to:

Raise any concerns about their child's online safety, online behaviour or use of technology promptly with the school.

Support their child to understand and follow the school's age-appropriate Acceptable Use Agreement (Appendices 1 and 2) and reinforce safe and responsible use of technology at home.

Support and reinforce the school's rules regarding pupils' mobile phones, smartwatches and other personal or smart technology.

The school will work in partnership with parents/carers to promote online safety and will communicate with them where concerns arise regarding a pupil's online safety or behaviour.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre

Help and advice for parents/carers – Childnet

Parents and carers resource sheet – Childnet

MMPS website, Parent e-safety advice tab: https://mmps.miet.uk/

3.7 Visitors and members of the community

Visitors and members of the community who are given access to the school's ICT systems, network or internet will be made aware of the relevant requirements of this policy and will be expected to comply with them. Where appropriate, they will be required to agree to the school's terms on acceptable use. Any online safety or safeguarding concern arising from their use of school systems, networks or devices must be reported promptly to the DSL/DDSL.

4. Educating pupils about online safety

Online safety is embedded throughout the school's curriculum and safeguarding provision. Teaching will be age-appropriate, progressive and responsive to emerging technologies and risks, and will include both how pupils can keep themselves safe online and how they should behave responsibly and respectfully when using technology.

4.1 Early Years Foundation Stage (EYFS)

In the EYFS, online safety and the safe use of technology will be introduced in an age-appropriate way through adult-led teaching, discussion and supervised use of technology.

Screen use will be limited, purposeful, carefully planned and clearly linked to identified learning and development aims. Where screens are used with children, an adult will co-engage with them and content will be checked in advance to ensure that it is safe and age-appropriate. Screen use will not replace high-quality adult interaction, physical activity, outdoor play, stories, practical learning or interaction with other children.

The school will have regard to the DfE's guidance on screen use in early years settings, including its recommendations regarding the amount and nature of screen use for children under five.

EYFS pupils will not use generative AI tools, AI chatbots or toys with built-in AI features as part of their learning, in accordance with Appendix 5.

Where screen-based assistive technology is required to support a child with SEND or communication needs, its use will be considered according to the individual needs and best interests of the child.

Children will be taught, at an appropriate level, to seek help from a trusted adult if they see or hear anything on a device that worries, frightens or upsets them.

4.2 Key Stages 1 and 2

- Pupils in **Key Stage 1** will be taught to
- Use technology safely and respectfully, keeping personal information private

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the **end of primary school**, and at an age-appropriate level pupils will know:

- That people should behave respectfully in online interactions and that the same principles of respect apply to online relationships as to face-to-face relationships, including where people are anonymous.
- The importance of not pressuring others to share information or images online, and strategies for resisting pressure from others.
- How to think critically about online relationships and sources of information, including understanding that people may pretend to be someone they are not, including pretending to be a child.
- How to recognise harmful or inappropriate online content and contact, and how and where to report concerns.
- That online services, apps and social media platforms have minimum age requirements, which vary between services, and why age restrictions exist to help protect children from inappropriate content and unsafe contact.
- The importance of being cautious about sharing personal information online and of using privacy and location settings appropriately.
- That information, photographs, videos and other material shared online may be copied or circulated and that, once shared, it may not be possible to remove it completely or control where it goes.
- That the internet contains content which may be inappropriate, upsetting or harmful to children and that they should seek help from a trusted adult if they are worried or concerned by anything they see or experience online.
- What appropriate boundaries look like in friendships and other relationships, including online.
- How to respond safely to adults they encounter online, including people they know and people they do not know.
- How to recognise when an online interaction or relationship may be unsafe or harmful, and how to ask for help for themselves or others and keep seeking help until they are heard.
- How information and data may be collected, shared and used online and why personal information should be protected.

Through Computing, PSHE and wider safeguarding education, pupils will also be taught, at an age-appropriate level, about healthy and balanced use of technology; age restrictions on online services, games and apps; online advertising and targeting; misinformation and disinformation; and the fact that digital content, images and information may be inaccurate, manipulated or generated using artificial intelligence (AI). Pupils will be encouraged to question the reliability of online information and to seek help from a trusted adult where content or an online interaction concerns them.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted to meet the needs of vulnerable pupils, pupils who have experienced abuse and pupils with SEND or other additional needs.

5. Educating parents/carers about online safety

The school will work in partnership with parents/carers to promote the safe and responsible use of technology. Online safety information and guidance will be provided through appropriate communications, parent induction, the MMPS website and other opportunities as appropriate.

Parents/carers will be made aware of:

- the school's approach to online safety, including the filtering and monitoring systems used to help protect pupils when using school devices and networks;
- the types of online activities, websites and digital services pupils may be asked to access as part of their learning and, where relevant, who pupils may interact with online;
- the school's expectations regarding mobile phones, smartwatches and other personal or smart technology;
- age-appropriate online risks, including social media, online communication, harmful or inappropriate content, misinformation and the use of artificial intelligence (AI); and
- where relevant, guidance relating to safe and developmentally appropriate screen use for children in the EYFS.

The school will communicate with parents/carers where concerns arise about a pupil's online safety or behaviour and may provide or signpost additional guidance where appropriate.

This policy will be made available to parents/carers.

Parents/carers who have concerns about online safety should raise these with the Headteacher/DSL or another appropriate member of staff.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.) Cyber-bullying may constitute child-on-child abuse and may occur whether the pupil is in or outside school.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff will also identify appropriate opportunities across the curriculum to reinforce learning about cyber-bullying, including through personal, social, health and economic (PSHE) education and other subjects where appropriate.

Staff, trustees and volunteers, where appropriate, will receive information and training on cyber-bullying, its impact and how to recognise, report and respond to concerns as part of the school's safeguarding training and updates (see Section 11).

In relation to a specific incident of cyber-bullying, the school will respond in accordance with the Behaviour and Anti-Bullying Policies. Where the incident raises a safeguarding concern, including concerns relating to child-on-child abuse, it will also be managed in accordance with the Child Protection and Safeguarding Policy and reported to the DSL/DDSL.

Where illegal, inappropriate or harmful content has been shared, the school will take reasonable steps to prevent further circulation and protect those affected. Staff will take care not to unnecessarily view, copy, download or forward potentially illegal material or interfere with evidence that may be required by the police or another agency.

Where there are reasonable grounds to believe that a criminal offence may have been committed, the DSL will consider referral to the police and/or other appropriate agencies, having regard to KCSIE and relevant statutory or national guidance.

6.3 Searching, confiscating and examining electronic devices

Any search of a pupil or their possessions, and any confiscation or examination of an electronic device, will be carried out in accordance with the school's Behaviour Policy and the latest DfE guidance on Searching, Screening and Confiscation.

Only the Headteacher or a member of staff authorised by the Headteacher may carry out a search. A search may be considered where there are reasonable grounds to suspect that a pupil is in possession of a prohibited item, or an item identified in the school rules as an item for which a search may be made, or where the pupil has agreed to the search.

Before carrying out a search, the authorised member of staff will consider the urgency of the situation and any safeguarding risks, explain to the pupil why and how the search will take place and seek the pupil's co-operation.

Where a pupil is searched, the search will normally be carried out by a member of staff of the same sex as the pupil and in the presence of another member of staff. The statutory exceptions relating to an immediate risk of serious harm will apply where relevant. School staff will not conduct a strip search.

An authorised member of staff may confiscate an electronic device or other item found during a search where there are reasonable grounds for suspecting that it:

- poses a risk to staff or pupils;
- is prohibited or is identified in the school rules as an item for which a search may be made; or
- constitutes evidence in relation to an offence.

Where an electronic device has been lawfully confiscated following a search, authorised staff may examine data or files on the device where there is a good reason to do so. A good reason may exist where there are reasonable grounds to suspect that the data or files have been, or could be, used to cause harm, undermine the safe environment of the school, disrupt teaching or commit an offence.

If data or files may constitute evidence relating to a suspected offence, they will not be deleted and the device will be handled in accordance with DfE guidance and, where appropriate, passed to the police. Where the material is not suspected to be evidence of an offence, deletion will only be considered in accordance with the DfE guidance.

Where a search or examination reveals a safeguarding concern, the DSL/DDSL will be informed without delay and the matter will be managed in accordance with the Child Protection and Safeguarding Policy.

Nudes and semi-nudes, including AI-generated images

If a member of staff suspects that a device may contain a nude or semi-nude image of a child, including an image that has been digitally altered or wholly generated using AI, such as a deepfake or 'deep nude', they must:

- not intentionally view the image;
- never copy, print, share, store or save the image;
- confiscate the device where appropriate and avoid further examination of it; and
- report the concern immediately to the DSL/DDSL.

The DSL/DDSL will determine the appropriate safeguarding response in accordance with KCSIE, the school's Child Protection and Safeguarding Policy and the UKCIS guidance on sharing nudes and semi-nudes.

In exceptional circumstances, where the DSL determines that there is a good and clear safeguarding reason why imagery must be viewed, this will only take place in accordance with UKCIS guidance and will be appropriately recorded.

Where there are reasonable grounds to suspect that material constitutes evidence of an offence, staff will preserve the evidence and seek appropriate advice rather than deleting, forwarding or otherwise interfering with it.

6.4 Artificial intelligence (AI)

MMPS recognises that artificial intelligence (AI), including generative AI, may provide educational and administrative benefits but also presents safeguarding, data protection, privacy, accuracy, bias, intellectual property and online safety risks. The safety and wellbeing of pupils will remain the school's priority when considering any use of AI.

AI tools or AI-enabled systems will only be adopted for school use where their intended use has been appropriately considered and approved. The school will take account of the educational purpose and benefit, age appropriateness, safeguarding implications, data protection and privacy, cyber security, filtering and monitoring, accuracy and reliability, equality and accessibility, and the safety features of the product. A record of AI tools approved for school use will be maintained.

Pupils are not permitted to use AI tools in school. This applies to all year groups, including EYFS. Staff must not give pupils access to staff AI accounts or ask pupils to use AI to complete school activities. Pupils may learn about AI through age-appropriate discussion and pre-checked examples, without accessing AI tools themselves. Any future proposal to introduce pupil use requires a separate risk assessment, approval and amendment of this policy before use begins.

Staff must use AI responsibly and only in accordance with school-approved arrangements. Staff remain professionally responsible for any material created or assisted by AI and must check its accuracy, appropriateness, bias and suitability before it is used or shared. AI must not replace professional judgement or meaningful human oversight.

Staff may enter only public, generic or completely anonymised, non-confidential information into approved AI tools. Personal, identifiable, sensitive or confidential school information must not be entered into any AI tool, whether free or paid. Approval of a tool does not authorise the input of such information. The detailed restrictions in Appendix 5 apply.

AI must not replace the school's safeguarding processes or reporting routes. Pupils will be taught not to rely on AI for advice about safeguarding, health, wellbeing or other personal concerns and to seek help from a trusted adult instead. Any concerning disclosure, content or interaction involving AI must be reported to the DSL/DDSL in the same way as any other safeguarding concern.

The creation or use of AI-generated or manipulated content to bully, harass, deceive, impersonate or harm another person is prohibited. This includes the creation or sharing of deepfakes, 'deep nudes', sexualised images, fabricated audio or video and other harmful or misleading content. Such

incidents will be addressed under the school's Child Protection and Safeguarding, Behaviour, Anti-Bullying and Data Protection Policies, as appropriate.

Further requirements are set out in Appendix 5: Artificial intelligence (AI): Safe use by staff and pupils.

7. Acceptable use of ICT systems, internet and email

Pupils and parents/carers are expected to read and agree to the school's age-appropriate Acceptable Use Agreements (Appendices 1A, 1B and 2). Staff, trustees, volunteers and other adults using the school's ICT systems must comply with the school's ICT & Internet Acceptable Use Policy and any other relevant school policies. Visitors will be required to comply with the school's acceptable-use requirements where relevant.

Use of the school's ICT systems, network and internet must be for educational purposes or for the legitimate purposes of an individual's role, except for any limited personal use expressly permitted by the school.

The school uses appropriate filtering and monitoring systems to help safeguard users and may monitor use of school ICT systems, networks and internet access in accordance with this policy, the ICT & Internet Acceptable Use Policy and applicable data protection requirements.

- Where a school email account is provided, it must be used for school business and work-related communications.
- School business must be conducted through school-approved email accounts and communication systems.
- Staff must not use personal email accounts to send or receive school-related information or materials and must not share personal email addresses with pupils or parents/carers for professional purposes.
- All electronic communication with pupils and parents/carers must remain professional in tone, content and purpose and must use school-approved communication channels.
- Users must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email and other electronic communications may need to be disclosed in legal proceedings or in response to information rights requests, including Subject Access Requests. Users should therefore understand that work-related electronic communications may be retrievable and should always communicate professionally and appropriately.
- Staff must take particular care when sending personal, sensitive or confidential information electronically. Such information must only be shared with authorised recipients using school-approved secure methods and must be encrypted or otherwise protected where required by the school's data protection and information-security procedures.
- Any actual or suspected loss, unauthorised disclosure or accidental transmission of personal data must be reported immediately in accordance with the school's Data Protection Policy and data breach procedure.
- Any permitted personal use of the internet must be reasonable, take place during authorised break times or other permitted periods and must not interfere with school duties. School devices must not be used for personal social networking unless expressly authorised for a school purpose.
- If a user encounters harmful, inappropriate or concerning online content, or becomes aware that filtering or monitoring controls may have failed, they must not deliberately continue to access the content and must report the matter promptly to the DSL and/or ICT Manager, as appropriate.

Unacceptable use of the ICT systems and the internet

It is unacceptable to:

- access, create, download, store, transmit or share illegal, offensive, obscene, indecent, abusive, discriminatory, extremist, violent or otherwise harmful content;
- use technology to bully, harass, threaten, impersonate, discriminate against or cause harm to another person;
- use school systems or online communications in a way that may bring the school into disrepute;
- breach confidentiality, privacy or data protection requirements, including through unauthorised access to, alteration, deletion or disclosure of information;
- infringe copyright or other intellectual property rights;
- access gambling, inappropriate commercial or other prohibited websites or services;
- attempt to bypass, disable or interfere with the school's filtering, monitoring, security or access-control systems;
- introduce or distribute malware, malicious software or other material intended to damage or disrupt school systems or data;
- use AI tools contrary to section 6.4 or Appendix 5, including entering personal, identifiable, safeguarding, confidential or other restricted school information into any AI tool;
- use another person's account, password or credentials, or share personal login credentials with another person;
- use school ICT systems in a way that deliberately disrupts the work of others or wastes school resources; or
- upload a personal photograph to a school email or user profile unless expressly authorised by the school.

This list is not exhaustive. The Headteacher may determine that other conduct constitutes unacceptable use where it is inconsistent with this policy, the ICT & Internet Acceptable Use Policy or other school policies. Staff misuse may result in disciplinary action in accordance with the school's procedures. Pupil misuse will be dealt with in accordance with the Behaviour Policy and other relevant school policies.

8. Use of mobile phones, smart technology and personal devices

8.1 Pupils

Pupils are not permitted to bring mobile phones into school. MMPS is a mobile-phone-free school and pupils must not have access to or use a mobile phone at any point during the school day.

This prohibition also applies to personal smart technology with similar communication, messaging, internet-access, audio/video recording or notification functions, including smartwatches, unless expressly authorised by the school.

If a pupil brings a mobile phone or prohibited smart device into school without authorisation, it will be confiscated and stored securely in accordance with the school's Behaviour Policy and arrangements for confiscated items. Parents/carers may be contacted and required to collect the device.

Pupils must not use personal devices to photograph, film or record another person, access the internet, send or receive messages or communicate with others while on school premises or participating in school activities.

The school recognises that an exception may exceptionally be necessary for an individual pupil, for example for a medical reason or as a reasonable adjustment relating to SEND or disability. Any

such arrangement must be agreed in advance by the Headteacher and will be considered on an individual basis.

Any breach of these requirements will be dealt with in accordance with the school's Behaviour Policy.

8.2 Staff

Staff must use personal mobile phones, smartwatches and similar wearable devices in accordance with the School's Mobile Phone Policy, Staff Code of Conduct and ICT & Internet Acceptable Use Policy.

Personally owned laptops or computers must not be brought in or used for School work, or connected to School systems or the School network. Personal mobile phones, smartwatches and similar wearable devices must be switched off or on silent, stored securely and kept out of sight while staff are working with or supervising pupils. They must not be used in areas where pupils are present, except where permitted under the Mobile Phone Policy for an emergency or other exceptional circumstance.

Staff must never use a personal device to photograph, film or make an audio recording of a pupil. Images, videos or recordings of pupils must only be created using school-owned or school-approved equipment and in accordance with the school's safeguarding, data protection and images policies. This requirement applies particularly to the EYFS.

Staff must not use personal telephone numbers, personal email accounts, social media accounts or other personal communication platforms to communicate professionally with pupils or their families.

9. Staff using work devices outside school

Staff who use school-issued devices outside school must take appropriate steps to maintain the security of the device and any school information accessed through it. This includes:

- keeping the device protected by a strong password, PIN or other approved authentication method and using multi-factor authentication where required;
- ensuring that encryption and other security controls installed or required by the school remain enabled;
- ensuring that the device locks automatically when left inactive and locking it whenever it is left unattended;
- not allowing family members, friends or other unauthorised individuals to use the device;
- keeping the device physically secure and taking reasonable precautions against loss, theft or unauthorised access;
- keeping operating systems, applications, anti-virus and other security software up to date and not disabling school-installed security, filtering or monitoring controls;
- using school-approved accounts, systems and storage for school information and not transferring school data to unauthorised personal accounts, devices, storage services or applications;
- taking particular care when accessing school systems away from the school network and avoiding the use of unsecured networks where this could put school information at risk;
- not entering personal, identifiable, safeguarding, confidential or other restricted school information into any AI tool; and
- complying at all times with the school's ICT & Internet Acceptable Use Policy, Data Protection Policy and other relevant policies.

School-issued work devices must be used for authorised work activities.

Any loss or theft of a school device, suspected unauthorised access, malware, security breach or other compromise must be reported immediately to the ICT Manager and, where personal data may be affected, in accordance with the school's data breach procedure.

10. How the school will respond to issues of misuse

Any suspected misuse of the school's ICT systems, internet access, devices, online services or artificial intelligence (AI) will be considered according to the nature, seriousness and circumstances of the incident. The school's response will be proportionate and will take account of any safeguarding, behavioural, disciplinary, data protection or security implications.

Where a pupil misuses technology, including through inappropriate online behaviour, attempting to circumvent filtering or monitoring controls, misuse of AI or misuse of a personal or school device, the matter will be dealt with in accordance with the school's Behaviour Policy, ICT & Internet Acceptable Use Policy and, where appropriate, the Anti-Bullying Policy.

Where misuse by a pupil raises a safeguarding concern, including child-on-child abuse, sexual harassment, harmful or illegal content, AI-generated or manipulated imagery, grooming, radicalisation or exploitation, the concern must be reported immediately to the DSL/DDSL and managed in accordance with the Child Protection and Safeguarding Policy.

Where a member of staff misuses the school's ICT systems, internet, AI tools or a school or personal device in a manner which may constitute misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct, Staff Handbook and applicable disciplinary procedures. Any safeguarding concern relating to an adult working with children will also be managed in accordance with the Child Protection and Safeguarding Policy.

Any actual or suspected loss, unauthorised disclosure or misuse of personal data will be reported and managed in accordance with the school's Data Protection Policy and data breach procedure.

The school will consider referral to the police, local authority or other relevant external agencies where an incident may involve illegal activity, presents a safeguarding risk or is otherwise sufficiently serious to require external involvement.

11. Training

11.1 Staff, trustees and volunteers

All staff will receive safeguarding and child protection training, including online safety, as part of their induction. This will include an understanding of the school's expectations and the applicable roles and responsibilities in relation to filtering and monitoring. Training will be regularly updated.

All staff will also receive safeguarding and child protection updates, including online safety, as required and at least annually, for example through training, staff meetings, emails and the school's weekly safeguarding questions.

In accordance with KCSIE 2026, all staff, including those who do not work directly with children, will read Part One of KCSIE. The DfE Part One overview may be used as a complementary quick-reference resource but does not replace Part One.

Online safety training and updates will be appropriate to staff roles and emerging risks and will include, where relevant:

- the four areas of online risk: content, contact, conduct and commerce;
- cyber-bullying and other forms of child-on-child abuse which may occur online, including abusive, threatening, harassing or misogynistic behaviour;

- online sexual harassment and sexual violence and the sharing of nudes and semi-nudes, including digitally altered or AI-generated images, deepfakes and ‘deep nudes’;
- online grooming, exploitation, radicalisation and exposure to extremist or other harmful content;
- how and when online safety concerns must be reported to the DSL/DDSL, including the need not to unnecessarily view, copy or share potentially illegal material;
- the school’s filtering and monitoring arrangements, including their limitations, staff responsibilities and how to report suspected failures, inappropriate content or attempts to circumvent controls;
- the safe and responsible use of artificial intelligence (AI), including safeguarding, data protection and confidentiality, accuracy and bias, age restrictions and the need for human oversight;
- relevant cyber-security, phishing and data-security risks and how to report a suspected breach or compromise; and
- the School’s requirements concerning mobile phones, personal devices and School-issued devices, including the specific safeguards applying within the EYFS.

Online safety training will form part of the school’s wider safeguarding approach and will be reviewed and adapted in response to changes in technology, emerging risks, incidents and identified training needs.

The DSL and DDSL will undertake appropriate safeguarding and child protection training, including online safety, at least every two years. Their knowledge and skills will also be refreshed at regular intervals and at least annually.

Trustees will receive appropriate safeguarding and child protection training, including online safeguarding, at induction and this will be updated regularly so that they are able to provide appropriate strategic challenge and assurance.

Supply and agency staff, contractors and volunteers will receive appropriate safeguarding and online safety information, training or briefing according to their role and level of access to pupils, school systems and information.

Further information about safeguarding training is set out in the Child Protection and Safeguarding Policy.

11.2 Pupils

All pupils will receive online safety and cyber-security education appropriate to their age, developmental stage, needs and level of understanding. This will reinforce the teaching set out in Section 4 and the expectations contained in the school’s Acceptable Use Agreements.

Pupils will be taught, as appropriate, to:

- use school devices, accounts and online services safely and responsibly;
- protect personal information and understand the importance of passwords and secure logins;
- recognise potentially harmful, inappropriate, misleading or suspicious online content, communications and activity;
- understand that people and information online may not always be genuine or accurate, including content generated or manipulated using AI;

- recognise cyber-bullying and other harmful online behaviour and know how to seek help;
- understand the importance of not attempting to bypass the school's filtering, monitoring or security controls;
- report anything online that worries, frightens or upsets them, or anything that appears unsafe or unusual, to a trusted adult; and
- understand, at an age-appropriate level, the school's rules concerning AI, mobile devices and online communication.

For older pupils, particularly in Key Stage 2, teaching may also include age-appropriate awareness of phishing and social engineering, password security, multi-factor authentication, removable storage devices, cyber-security incidents and the loss or unauthorised disclosure of personal information.

Pupils will be reminded that they are not expected to investigate or resolve online safety or cyber-security concerns themselves. They should stop, seek help and report the concern to a member of staff.

12. Monitoring arrangements

The DSL will ensure that safeguarding and behaviour concerns relating to online safety are appropriately recorded and monitored. An online safety incident record is provided at Appendix 3. Significant incidents, emerging patterns and identified risks will inform safeguarding action, staff training, pupil education and future review of this policy.

The effectiveness of the school's filtering and monitoring arrangements will be formally reviewed at least once every academic year. The review will be led by the member of the Senior Leadership Team with responsibility for filtering and monitoring, supported by the DSL and ICT Manager/IT support.

The review will include checks that filtering and monitoring arrangements are working appropriately across all internet-connected devices and in all relevant locations. A record will be kept of the checks undertaken, including when they took place, who carried them out, what was checked, any issues identified and action taken.

Filtering and monitoring arrangements will also be reviewed where necessary following a significant safeguarding concern, a change in working practices, the introduction of new technology or AI-enabled tools, significant software or system updates, or changes to network or device configurations. The frequency of operational checks between formal reviews will be informed by the school's safeguarding and technical risk profile.

This policy will be reviewed at least annually by the Headteacher and shared with the Trust Board.

The review will be supported by an annual online safety risk assessment which considers the nature and extent of the risks faced by pupils, including their age and developmental stage, pupils who may be at greater risk of harm, SEND and other vulnerabilities, how pupils access technology and relevant risks identified through the Prevent Risk Assessment.

The findings of the annual review will be recorded in the school's separate MMPS Online Safety Risk Assessment and Filtering & Monitoring Review, together with any identified actions, responsible persons and completion dates.

The policy and associated risk assessments will also be reviewed sooner where there are significant changes to legislation or statutory guidance, technology, school systems or practice, or where an incident or emerging risk indicates that an earlier review is required.

13. Links with other policies

This Online and E-Safety Policy should be read in conjunction with the school's:

- Child Protection and Safeguarding Policy

- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- ICT & Internet Acceptable Use Policy
- Mobile Phone Policy
- Staff Handbook
- Data Protection Policy and Privacy Notices
- Social Media Policy
- Relationships Education / RSE and PSHE Policy
- Prevent Risk Assessment
- Complaints Policy
- AI tool risk assessment
- Approved AI tools and permitted uses register

Appendix 1A: EYFS Acceptable Use Agreement

(Pupils and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
At MMPS, technology in the EYFS is used carefully, purposefully and with appropriate adult supervision. Screen use will be limited and planned so that it supports learning and development and does not replace play, physical activity, conversation, reading, creative activity or interaction with adults and other children. When I use a computer, tablet or other technology in school, I will: • only use it when a teacher or other adult says I may; • use only the websites, apps, games or activities that an adult has chosen for me; • use technology with an adult nearby and follow their instructions; • be kind when I use technology with other children; • look after school equipment; • ask an adult before taking a photograph, video or recording; and • tell an adult straight away if I see or hear something that worries, frightens or upsets me. EYFS children will not independently access the internet. Generative AI tools, AI chatbots and AI-enabled toys will not be used by EYFS children. Screen-based assistive technology required to support a child with SEND may be used according to the child's individual needs.	
Parent/carer acknowledgement I understand how MMPS approaches the use of screens, online technology and digital devices within the EYFS and will support the school in helping my child develop safe and healthy habits when using technology.	
Signed (parent/carer):	**Date:**

Appendix 1B: KS1 Acceptable Use Agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the school's computers, tablets, ICT systems or internet, I will: • ask a teacher or other adult before using them; • only use websites, apps and online activities that a teacher or adult has told me I may use; • use school technology for learning and authorised school activities; • keep my username and password private and only use the account I have been given; • keep personal information such as my address, telephone number and passwords private; • be kind and respectful to other people when using technology; • look after school equipment and tell an adult if something is broken or not working properly; • ask an adult before taking or sharing a photograph, video or recording; • tell an adult immediately if I receive a message from someone I do not know or see anything online that worries, frightens or upsets me; • tell an adult if I accidentally access something I should not have accessed; • follow the school's rules about mobile phones, smartwatches and other personal devices; and • log off or shut down equipment appropriately when I have finished using it. I understand that the school uses filtering and monitoring systems to help keep me safe online and that there may be consequences if I deliberately do not follow these rules.	
Signed (pupil):	**Date:**
Parent/carer acknowledgement I agree that my child may use the school's ICT systems and internet when appropriately supervised by school staff. I have discussed the above rules with my child and will support the school in promoting safe and responsible use of technology.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2 Acceptable Use Agreement

(Pupils and Parents/Carers)

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the school's computers, tablets, ICT systems or internet, I will: • use them responsibly, for learning and only with permission; • keep my username, password and personal information private; • be kind and respectful and never use technology to bully, threaten, embarrass or upset others; • respect other people's privacy, work, photographs and information; • tell a member of staff immediately if I see or receive anything worrying, harmful, inappropriate or suspicious, or if someone I do not know contacts me; • look after school equipment and report anything that is damaged or not working properly; • only access websites, apps and online services permitted by the school; • never create, view, request, save or share nude, semi-nude, sexualised, violent or otherwise harmful material; • never create or share fake, manipulated or AI-generated images, video or audio intended to harm, embarrass or impersonate another person; • never use another person's account or attempt to bypass the school's filtering, monitoring or security controls; and • follow the school's rules about mobile phones, smartwatches and other personal devices. **I understand that pupils are not permitted to bring mobile phones into MMPS.** **Artificial Intelligence (AI)** I understand that pupils are not permitted to use AI tools in school. I will not access AI tools or use a member of staff's AI account. I may learn about AI through discussions and examples chosen by my teacher. I understand that AI can produce incorrect or harmful information. If anything worries me, I will tell a trusted adult. **I understand that the school uses filtering and monitoring systems to help keep pupils safe and that there may be consequences if I deliberately break these rules, including for serious online behaviour outside school that affects the school community.**	
Signed (pupil):	**Date:**
Parent/carer acknowledgement I have discussed these rules with my child and agree that they may use the school's ICT systems and internet when appropriately supervised by school staff.	
Signed (parent/carer):	**Date:**

Acceptable Use Agreement – Staff, trustees, volunteers and visitors
The Acceptable Use Agreement for staff, trustees, volunteers and visitors is contained in the school's ICT & Internet Acceptable Use Policy.

Appendix 3: Online Safety Incident Report Log

Safeguarding concerns must be reported to the DSL/DDSL and recorded in accordance with the school's safeguarding procedures. This log does not replace safeguarding, behaviour, data-breach or other records required under the school's policies.

ONLINE SAFETY INCIDENT LOG				
Date / time	**Pupil(s) / person(s) involved and year group, where applicable**	**Incident, location and device / platform involved**	**Category / concern** *e.g. Safeguarding; cyber-bullying; inappropriate content; AI/deepfake; filtering/monitoring; data/security; misuse*	**Immediate action, referrals and follow-up and recorded by**

Appendix 4: Online Safety Incident Response Procedure

Immediate response

Make the situation safe and report the concern promptly. Where there is any safeguarding element, report immediately to the **DSL/DDSL**. Technical, filtering or monitoring concerns should also be reported to the **ICT Manager/IT support**.

Do not unnecessarily view, copy, download, save, forward or share potentially illegal, sexual or otherwise harmful material. Preserve relevant evidence where appropriate.

Record the incident through the appropriate school procedure. Safeguarding concerns must be recorded in accordance with the **Child Protection and Safeguarding Policy**. The **Online Safety Incident Log (Appendix 3)** may be used where appropriate.

Response according to the type of concern

Safeguarding concern – including child-on-child abuse, grooming, exploitation, harmful content, radicalisation, AI-generated harmful content or deepfakes:
Report to the **DSL/DDSL**, who will follow safeguarding procedures and refer to external agencies where required.

Nude/semi-nude or suspected child sexual abuse material – including AI-generated or manipulated imagery:
Do not intentionally view, copy, save or share it. Report immediately to the **DSL/DDSL** and secure the device or material as appropriate.

Concern about an adult working with children:
Report to the **Headteacher** and follow the safeguarding allegations or low-level concerns procedures, including **LADO referral where the threshold is met**. Concerns about the Headteacher must be reported to the **Trust Chair**.

Suspected illegal or criminal activity:
The DSL/Headteacher will consider referral to the **police or other appropriate agency**.

Data protection or confidentiality breach:
Report immediately in accordance with the school's **data-breach procedure**.

Filtering, monitoring, cyber-security or technical failure:
Report to the **ICT Manager/IT support** and also to the DSL where there is a safeguarding implication.

Cyber-bullying or inappropriate pupil use without a safeguarding concern:
Follow the school's **Behaviour, Anti-Bullying and Acceptable Use procedures**.

Follow-up

Record actions and outcomes, inform parents/carers where appropriate and consider whether the incident requires changes to risk assessments, filtering and monitoring, policies, staff training or pupil education.

Appendix 5: Artificial Intelligence (AI)

Safe use by staff and pupils

1. Purpose and scope

Artificial intelligence (AI), including generative AI, can support teaching, resource preparation and administration. Its use must protect pupils, families, staff and the school and must not replace professional judgement.

This framework applies to staff, including supply and agency staff, volunteers, contractors and trustees. It also sets out the school's prohibition on pupil use of AI. It applies to school-related work undertaken on school or personal devices, at school or elsewhere. It does not authorise the use of personal devices where this is prohibited elsewhere in this policy

It covers AI tools that generate, summarise or change text, images, audio, video or other content, including AI features within existing software.

This appendix must be read alongside the school's Child Protection and Safeguarding Policy, Data Protection Policy, ICT and Internet Acceptable Use Policy, Staff Code of Conduct and Behaviour Policy.

2. Approval and oversight

The Trust Board has strategic oversight of the school's approach to AI. The Headteacher has operational responsibility, supported by the DSL/DDSL and ICT Manager/IT support. Specialist data protection advice will be sought where necessary.

The school does not have a school-wide AI subscription. SLT and administration staff have individual paid subscriptions, while some other staff use free ChatGPT. All school-related use requires the Headteacher's approval and must follow this framework. The same information restrictions apply to free and paid accounts.

Staff must only use AI tools and account arrangements that have been approved by the Headteacher for the intended purpose. A tool must not be introduced simply because it is publicly available, free to use or included within an existing subscription.

The school will maintain a register of approved AI tools and uses, recording the account or workspace approved, permitted purposes, restrictions and review date.

Before approval, the school will consider:

- The educational or operational benefit.
- Safeguarding, age restrictions and suitability.
- Data protection, confidentiality and whether a Data Protection Impact Assessment (DPIA) is required.
- Provider terms, model training, data retention, deletion and sharing.
- Account security, permissions and any access to school systems.
- Reliability, accuracy, bias, equality and accessibility.
- Arrangements for human oversight, staff training and review.

A paid subscription does not automatically make a tool suitable for school use. A free account, personal paid account or school-funded account must meet the same approval requirements. Switching off model training does not, by itself, constitute approval.

3. Staff use and protection of information

Staff must not use an unapproved AI tool for school work. Where use has been approved, staff may enter only public, generic or completely anonymised information that is not confidential.

Staff must not enter personal, identifiable, sensitive or confidential school information into AI prompts, conversations, uploads or connected services. This applies to both free and paid accounts.

In particular, staff must not enter:

- Pupil names, class lists, contact details or other identifiable pupil information.
- Safeguarding disclosures, referrals, case notes or CPOMS records.
- Individual SEND, medical, health or wellbeing records.
- Parent correspondence, complaints or information about individual families.
- Staff applications, references, appraisal, disciplinary, absence or other confidential employment records.
- Individual attendance records, assessment records or pupil reports.
- Photographs, audio or video identifying pupils, parents or staff.
- Confidential Trust or school documents, financial information or security arrangements.
- Passwords, access codes or other security credentials.

Staff must not upload actual pupil work under these arrangements. Fictional examples created by staff may be used to develop teaching resources or general assessment guidance.

Where a task requires identifiable or confidential information, staff must use existing approved school systems and procedures.

Any future proposal to use AI to process identifiable or confidential information requires a separate documented assessment, specialist data protection advice and appropriate approval. This framework must be reviewed and amended before such use begins.

4. Complete anonymisation

Removing a name does not necessarily make information anonymous. Staff must consider whether someone could be identified from the remaining information, either on its own or when combined with other information.

Before entering any material, staff must remove:

- Names, initials, contact details, addresses, dates of birth and identification numbers.
- Photographs, voices, signatures and identifiable handwriting.
- Exact dates, class details, family circumstances and distinctive incidents that could identify someone.
- Identifying details in filenames, document properties, comments, tracked changes, headers and screenshots.

Replacing a name with initials, a code or “Pupil A” does not automatically make information anonymous.

Anonymisation must take place before information is entered into AI. Staff must never upload an identifiable document and ask AI to anonymise it.

Staff should use general descriptions or fictional examples wherever possible. For example, they may request general strategies to support early reading without describing a particular child or their circumstances.

If staff are unsure whether information is sufficiently anonymised or suitable to share, they must not enter it and should seek advice from the Headteacher.

5. Permitted staff uses

Subject to approval of the tool and purpose, staff may use AI to support:

- Lesson ideas, quizzes, model texts and practice activities.
- General adaptations of resources for different learning needs.
- Generic report comment banks.
- Templates for routine communications.
- Improving the wording of non-confidential, completely anonymised text.
- Summarising public guidance, with checks against the original source.
- Ideas for assemblies, displays and school activities.

For example, a member of staff may ask AI to draft a general punctuality reminder. They must not paste a parent’s email or a child’s attendance record into the tool.

Names and other personal details must be added afterwards within approved school systems.

AI use is optional. Staff are not expected to purchase personal subscriptions.

6. Professional responsibility and checking outputs

Staff remain professionally responsible for work produced with AI assistance. They must read, check and adapt all output before using or sharing it.

Checks must include:

- Factual accuracy, calculations, answers and references.
- Suitability for pupils’ ages, learning needs and curriculum.
- Bias, stereotypes and unfair assumptions.
- Consistency with the school’s Islamic ethos and respect for others.
- Copyright and permission to use material.
- Consistency with school policies and current official guidance.

Qur’anic quotations, hadith, translations and religious references must be checked against reliable sources by an appropriately knowledgeable member of staff.

AI must not be used to fabricate information, assessment findings, lesson observations, meeting records, inspection evidence or events that did not occur.

AI must not determine individual decisions about safeguarding, SEND, behaviour, admissions, recruitment, staff performance, welfare or assessment. These decisions remain the responsibility of the relevant professionals.

Staff must acknowledge substantial AI assistance when submitting policies, reports or other substantive documents for approval. Routine spelling or grammar assistance does not require a separate declaration.

7. Accounts, integrations and security

Staff must follow the approved account arrangements, keep login details secure and use multifactor authentication where available. Accounts and passwords must not be shared.

Staff must not connect AI to school email, shared drives, pupil records or other school systems without separate approval and assessment.

AI meeting recording, transcription, browser extensions and automated actions also require separate approval. Staff must not enable these features simply because they are available within software they already use.

Staff must check privacy, model-training and sharing settings, with IT support where needed, and switch off use of their content for model training wherever this option is available. These settings do not remove the restrictions on information that may be entered.

Staff must not use public sharing links for school AI conversations or outputs unless expressly authorised.

8. Copyright and intellectual property

Staff must respect the intellectual property rights of pupils, colleagues and other copyright holders.

Published resources, subscription materials, textbooks, examination materials and other protected content must not be uploaded unless the relevant permission or licence allows that use.

Staff must not assume that material generated by AI is free from copyright restrictions. Material intended for wider publication must be checked carefully, with advice sought where necessary.

9. Pupil use and classroom practice

Pupils are not permitted to use AI tools in school. This applies to all year groups, including EYFS. Staff must not give pupils access to staff AI accounts or ask pupils to use AI to complete school activities.

Staff may use approved AI tools to prepare teaching materials, provided they follow this framework and check all materials before showing or distributing them to pupils. Live AI conversations must not be displayed to pupils.

Staff must keep their accounts secure and lock unattended devices.

Pupils may be taught about AI, its limitations and online safety through age-appropriate discussion and pre-checked examples. This does not require pupils to access AI tools.

Any future proposal to introduce pupil use must be separately risk assessed and approved, and this policy amended before use begins.

10. Harmful content and safeguarding

AI must not be used to generate, alter or distribute material that is harmful, abusive, discriminatory, sexualised, threatening, bullying or otherwise inappropriate.

The creation or sharing of deepfakes, AI-generated sexual imagery, false audio or video, or other material intended to impersonate, deceive, humiliate or harm another person is prohibited.

AI must never replace the school's safeguarding procedures, the DSL/DDSL or established reporting routes. AI-generated safeguarding advice or conclusions must not be relied upon in place of professional safeguarding judgement.

Any safeguarding concern arising from AI use must be reported immediately to the DSL/DDSL and managed under the Child Protection and Safeguarding Policy. Staff must not copy or forward harmful material unnecessarily and must follow the school's procedures for handling evidence.

11. Equality, SEND and accessibility

AI-generated resources must be reviewed to ensure that they are inclusive, accessible and appropriate for the pupils who will use them.

The school will consider whether AI use could disadvantage pupils because of disability, learning needs, language or unequal access to technology.

Any proposed AI-supported assistive technology must be considered separately according to the pupil's needs, educational benefit, safety and data protection requirements. This appendix does not authorise staff to enter identifiable SEND or medical information into AI tools.

Any proposal involving direct pupil use of AI remains subject to the prohibition in section 9 and cannot proceed without prior assessment, approval and amendment of this policy.

12. Reporting errors, disclosures and misuse

Any accidental or suspected disclosure of personal or confidential information through AI must be reported immediately to the Headteacher. Where there is a safeguarding concern, the DSL/DDSL must also be informed immediately.

Staff must stop the activity and report, through a secure school route:

- The tool and account used.
- When the incident occurred.
- The nature of the information entered.
- Whether files, sharing links or connected services were involved.

Staff must not assume that deleting a conversation resolves the incident. The Headteacher, supported by IT support and specialist advice where necessary, will coordinate the response under the school's data-breach procedures.

Other concerns, including inaccurate material already used, unfair outcomes, harmful content or security weaknesses, must be reported promptly to the appropriate school lead.

Incidents will be managed through the existing safeguarding, online safety, data protection, ICT-security, behaviour or staff conduct procedures. Concerns involving the Headteacher must follow the established escalation or whistleblowing route.

13. Training, monitoring and review

The school will identify existing AI use and provide staff with guidance on approved tools, anonymisation, confidentiality, copyright, verification and incident reporting.

Staff must read and follow this framework. Existing subscriptions or previous use must not be treated as approval.

The Headteacher will oversee implementation, supported by the DSL/DDSL and ICT Manager/IT support. Monitoring will be proportionate and consistent with existing ICT and data protection arrangements.

Breaches will be considered under the relevant conduct, disciplinary or behaviour procedures. Concerns raised by parents or pupils will be addressed through the school's established complaints and safeguarding procedures, as appropriate.

The school will maintain separate AI tool risk assessments and an approved AI tools register. These will be reviewed following significant changes to products, account arrangements, purposes, integrations or provider terms, and following relevant incidents.

This appendix will be reviewed as part of the annual review of the Online and E-Safety Policy, or sooner where required.

Implementation will be reviewed within half a term of adoption to check that staff understand the rules and the precautions are operating.