Education My Life Matters

'Success for everyone'

Online Safety Policy

Approved by:	Independent Executive Board	**Date:** Autumn 2026
Last reviewed on:	Autumn Term 2026	
Next review due by:	Autumn Term 2027	

Contents

1.The EMLM Compass Approach 3
2. Aims 3
3. Legislation and guidance 4
4. Roles and responsibilities 5
5. Educating learners about online safety 8
5.1 Key Stage 3 9
5.2 Key Stage 4 9
5.3 By the end of secondary education 9
6. Educating parents/carers about online safety 11
7. Cyberbullying and Technically Assisted Abuse 11
7.4 Suspected nudes or semi-nudes involving children 13
8. Acceptable use of Technology and the Internet 14
9. Learners using mobile phone and personal smart devices 15
10. Staff using work devices outside school 15
11. Filtering and Monitoring 16
12. Cyber Security, Information Security and Access Management 17
14. Training 19
16. Links with other policies 21
Appendix 1: Mobile Phone and Technology Acceptable Use Agreement for Learners, Parents and Carers 23
Mobile phones 23
Online and virtual lessons 23
Internet use 24
Logins and passwords 24
Social media and communication 24
Appendix 2: Acceptable Use agreement for Staff, Governors, Volunteers and Visitors 27
Appendix 3: Online Safety Training Needs Self-Audit for Staff 29
Appendix 4: Online Safety Monitoring and Trends Log 31

1.The EMLM Compass Approach

At Education My Life Matters (EMLM), our work with learners is underpinned by the EMLM Compass Approach. This provides a consistent, trauma-informed and relational framework for responding to safeguarding concerns, behaviour, attendance, wellbeing, bullying, medical needs and all matters relating to the safety, welfare and inclusion of our learners.

This approach provides a consistent, trauma-informed and relational framework for how we respond to all concerns about learners' safety and wellbeing.

It ensures that every member of staff follows a shared, values-led process:

- **NOTICE** – Identify concerns early through professional curiosity
- **LISTEN** – Respond to disclosures in a safe, respectful and trauma-informed way
- **PROTECT** – Take immediate safeguarding action where needed
- **RESPOND** – Investigate, intervene and restore harm appropriately
- **RECORD** – Record concerns accurately on CPOMS without delay
- **REVIEW** – Monitor outcomes and learn from incidents to improve practice

The Compass Approach applies to all forms of concern including bullying, cyberbullying, harassment, discrimination, child-on-child abuse, harmful sexual behaviour, sexual harassment, sexual violence and wider safeguarding concerns.

It ensures consistency, professional accountability and a clear safeguarding pathway across the organisation.

2. Aims

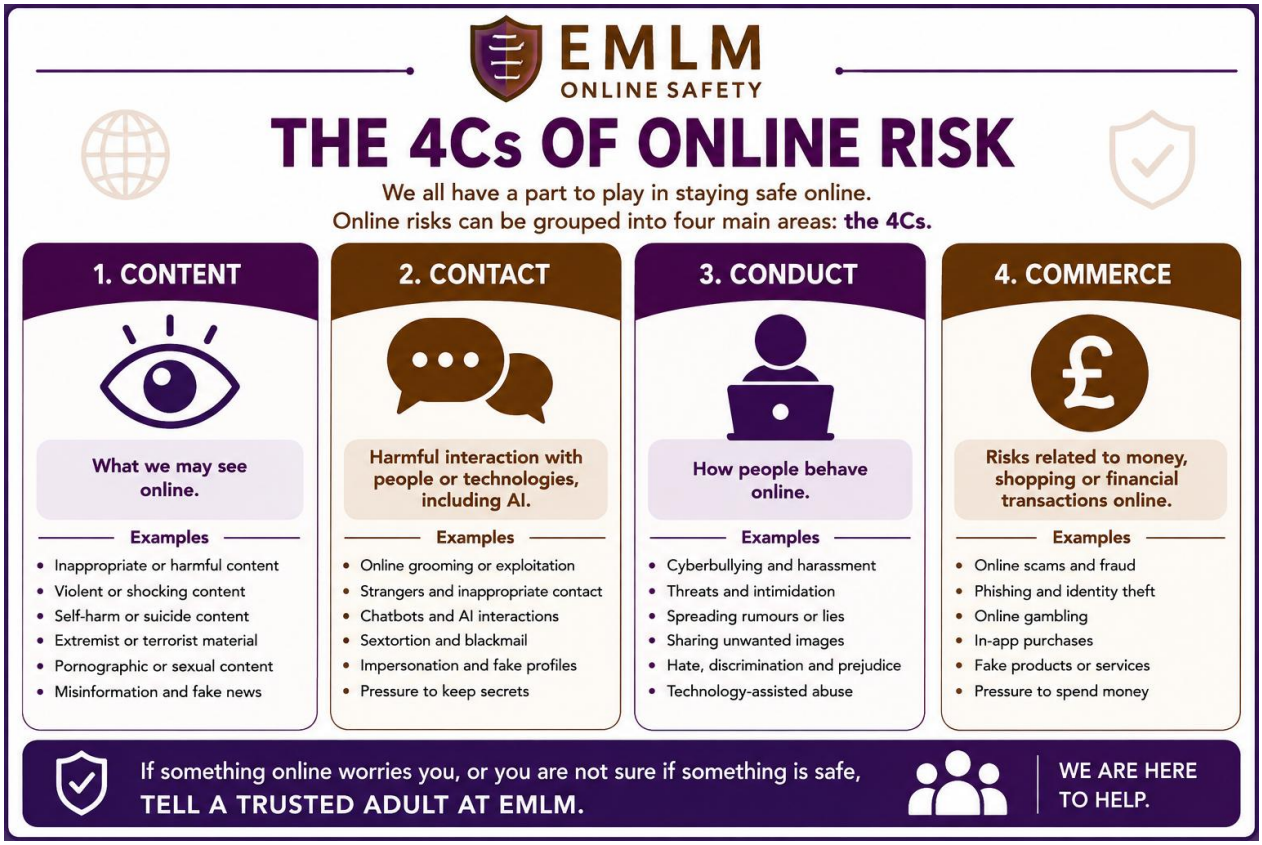
Education My Life Matters (EMLM) aims to:

- Have robust processes in place to safeguard and promote the welfare of learners, staff, volunteers, governors and members of the school community when using technology;
- Identify and support learners who may be at greater risk of online harm, recognising that vulnerability may change over time and that some learners may require a personalised or contextualised approach;
- Deliver an effective whole-school approach to online safety which empowers learners, staff and the wider school community to use technology safely, responsibly, respectfully and critically;
- Ensure that online safety is an integral and interrelated part of safeguarding and child protection, rather than being treated as a standalone issue;
- Promote the safe, responsible and appropriate use of internet-connected technology, including computers, tablets, mobile phones, smart devices, social media and artificial intelligence (AI);
- Establish clear mechanisms to identify, report, intervene in, record and escalate online safety concerns and incidents;
- Ensure appropriate filtering and monitoring arrangements are in place and regularly reviewed;
- Equip learners with the knowledge and skills required to recognise online risks, make informed choices and seek help when needed.

Online safety is considered as part of EMLM's whole-school safeguarding approach and applies to incidents occurring both on and off the school site where they present a safeguarding risk, affect the welfare of a learner or have an impact on the school community.

The 4 key categories of risk

EMLM's approach to online safety is based on addressing the following four categories of risk:



3. Legislation and guidance

This policy has been developed with regard to current legislation and statutory and non-statutory guidance relevant to online safety and safeguarding.

It is based particularly on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education (KCSIE).

It also takes account of relevant Department for Education guidance and advice, including:

- Teaching online safety in schools
- Relationships Education, Relationships and Sex Education (RSE) and Health Education statutory guidance
- Preventing and tackling bullying
- Cyberbullying advice for headteachers and school staff
- Searching, screening and confiscation
- Mobile phones in schools
- Generative artificial intelligence in education
- Filtering and monitoring standards for schools and colleges
- Meeting digital and technology standards in schools and colleges
- Prevent duty guidance
- Sharing nudes and semi-nudes: advice for education settings working with children and young people

This policy also reflects relevant legislation, including, but not limited to:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011
- Equality Act 2010
- Children Act 1989
- Children Act 2004
- Counter-Terrorism and Security Act 2015
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Data (Use and Access) Act 2025
- Online Safety Act 2023

It also takes account of the National Curriculum programmes of study for computing and the school's statutory safeguarding, relationships, sex and health education responsibilities.

Where statutory guidance or legislation is revised after publication of this policy, EMLM will have regard to the most current applicable requirements and will amend this policy where necessary.

4. Roles and responsibilities

4.1 The Independent Executive Board (IEB)

The IEB has overall strategic responsibility for safeguarding, including online safety, and for holding the Head of School to account for the effective implementation of this policy.
The IEB will ensure that online safety is a running and interrelated theme within EMLM's whole-school approach to safeguarding.
The IEB will:

- Ensure that appropriate policies and procedures are in place to safeguard learners online;
- Ensure that all staff receive appropriate safeguarding and child protection training which includes online safety;
- Ensure staff understand their expectations, roles and responsibilities in relation to filtering and monitoring;
- Ensure relevant staff receive regular online safety updates, as required and at least annually, so that they have the knowledge and skills necessary to safeguard learners effectively;
- Ensure learners are taught how to keep themselves and others safe, including online;
- Ensure the school's curriculum reflects current online risks and technological developments;
- Ensure EMLM has appropriate filtering and monitoring systems on school devices and networks;
- Ensure filtering and monitoring arrangements are reviewed for effectiveness at least once every academic year;
- Ensure roles and responsibilities for filtering and monitoring are clearly identified;
- Ensure systems block harmful and inappropriate content without unreasonably restricting teaching and learning;
- Ensure effective monitoring arrangements are in place which reflect the school's safeguarding risks and needs;
- Ensure that the school considers the age range, needs, vulnerabilities and SEND of learners when determining appropriate online safety provision;
- Receive appropriate information from leaders about online safety incidents, trends, filtering and monitoring, training and emerging risks;
- Ensure an annual online safety risk assessment is undertaken;
- Ensure the effectiveness of this policy is reviewed at least annually.

The Board will nominate a member with oversight of safeguarding, including online safety. The current nominated member will be recorded within EMLM's governance information

All Board members will:

- Read and understand this policy.
- Comply with the school's acceptable use requirements.
- Undertake appropriate safeguarding training, including online safety.
- Recognise that a "one size fits all" approach may not be suitable for every learner and that vulnerable learners and learners with SEND may require a more personalised or contextualised approach.

4.2 The Head of School

The Head of School has overall operational responsibility for ensuring that this policy is implemented consistently.
The Head of School will:

- Ensure staff understand and implement this policy;
- Promote a culture in which online safety is recognised as an integral part of safeguarding;
- Ensure sufficient resources, systems and training are available to support effective online safety arrangements;
- Work with the DSL and ICT Lead to ensure appropriate filtering, monitoring, information-security and cyber-security arrangements are in place;
- Ensure appropriate action is taken where online safety requirements are breached.

The Head of School is the senior leadership team member with overall responsibility for ensuring that the school's filtering and monitoring arrangements are appropriately managed and reviewed.

4.3 The Designated Safeguarding Lead

Details of EMLM's Designated Safeguarding Lead (DSL) and deputy/deputies are set out in the Child Protection and Safeguarding Policy and relevant job descriptions. The DSL takes lead safeguarding responsibility for online safety.
The DSL will:

- Ensure staff understand this policy and the safeguarding procedures associated with online safety;
- Work with the Head of School, IEB and relevant staff to review this policy at least annually;
- Have appropriate knowledge and understanding of the filtering and monitoring systems and processes used by EMLM;
- Work with the Head of School, ICT Lead and external providers where appropriate to ensure filtering and monitoring systems meet the safeguarding needs of EMLM;
- Respond to online safeguarding concerns and incidents in accordance with the Child Protection and Safeguarding Policy;
- Ensure relevant online safety concerns and incidents are appropriately recorded;
- Identify patterns, trends or emerging risks arising from online incidents;
- Ensure incidents of cyberbullying are addressed in accordance with safeguarding and behaviour procedures;
- Ensure incidents involving child-on-child abuse, sexual harassment or sexual violence are managed in accordance with safeguarding procedures;
- Provide or arrange appropriate online safety training and updates for staff;
- Liaise with children's social care, police and other agencies where appropriate;
- Provide appropriate reports and assurance regarding online safety to the Head of School and IEB;
- Contribute to the annual review of filtering and monitoring arrangements;
- Undertake or coordinate an annual online safety risk assessment which reflects the risks faced by EMLM learners;

- Ensure vulnerable learners and learners with SEND receive appropriate support and adapted online safety education where required;
- Keep knowledge and skills relating to online safety up to date.

This list is not exhaustive.

4.4 The ICT Lead

The ICT Lead has responsibility for supporting the technical implementation of EMLM's online safety, filtering, monitoring and information-security arrangements.

The ICT Lead will:

- Maintain appropriate filtering and monitoring systems across school-managed devices and networks;
- Ensure technical controls are appropriate to the age, needs and vulnerabilities of EMLM learners;
- Work with the Head of School and DSL to identify and respond to filtering and monitoring risks;
- Ensure filtering is operating appropriately across relevant internet-connected devices and school locations;
- Ensure technical monitoring arrangements operate effectively and alerts or concerns are directed to appropriately trained staff;
- Maintain appropriate security against viruses, malware, ransomware and other cyber threats;
- Ensure operating systems, security software and other critical systems are appropriately updated and patched;
- Restrict unauthorised administrative access;
- Maintain appropriate account and access-management procedures;
- Ensure accounts and access rights are amended or removed when no longer required;
- Support the use of multi-factor authentication where appropriate;
- Take reasonable steps to prevent access to harmful and inappropriate websites and files;
- Conduct appropriate operational security checks;
- Escalate any failure or suspected failure of filtering, monitoring or security systems promptly to the Head of School and DSL;
- Support the formal annual filtering and monitoring review;
- Maintain appropriate records of technical reviews and actions;
- Respond appropriately to cyber-security incidents and data breaches in accordance with school procedures.

Operational ICT checks may take place more frequently than the formal annual safeguarding review of filtering and monitoring and do not replace that review.

4.5 All staff, including contractors and agency staff, and volunteers

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

- Reading, understanding and implementing this policy;
- Recognising that online safety is part of safeguarding;
- Following the school's Child Protection and Safeguarding Policy;
- Following the school's acceptable use requirements;
- Ensuring learners follow relevant acceptable use requirements;
- Understanding their responsibilities in relation to filtering and monitoring;
- Knowing how to report failures or concerns relating to filtering or monitoring;
- Reporting any safeguarding concern arising from online activity through EMLM's safeguarding procedures without delay;

- Not attempting to investigate safeguarding concerns themselves unless specifically instructed by the DSL;
- Following the agreed procedure where access to a legitimately required website or resource has been incorrectly blocked;
- Ensuring online safety incidents are appropriately reported and recorded without delay;
- Responding appropriately to cyberbullying, child-on-child abuse, sexual harassment and sexual violence, whether online or offline;
- Maintaining an attitude of "it could happen here"…;
- Recognising that safeguarding concerns can arise from activity outside school and on personal devices as well as school systems;
- Maintaining appropriate professional boundaries when communicating electronically with learners;
- Protecting confidential and personal information;
- Reporting suspected cyber-security incidents or personal data breaches promptly.

Staff must never disable or bypass the school's filtering, monitoring or security controls unless specifically authorised to undertake a legitimate technical function.

4.6 Parents/carers

Parents and carers play an important role in supporting children to use technology safely.

Parents/carers are expected to:

- Support EMLM's online safety expectations;
- Discuss safe and responsible technology use with their child;
- Reinforce appropriate behaviour online;
- Inform EMLM promptly about online safeguarding concerns that may affect their child or another learner;
- Support the school's mobile-phone arrangements;
- Read and support their child to understand the learner acceptable use agreement;
- Encourage their child to report anything online which makes them uncomfortable, frightened or unsafe.

EMLM will signpost families to appropriate trusted sources of support, including resources produced by the UK Safer Internet Centre and Childnet.

4.7 Visitors and members of the community

Visitors and community members who use EMLM's ICT systems or internet connection will be made aware of relevant expectations and will be required to comply with the school's acceptable use requirements where appropriate.

Access may be restricted or removed if these requirements are breached.

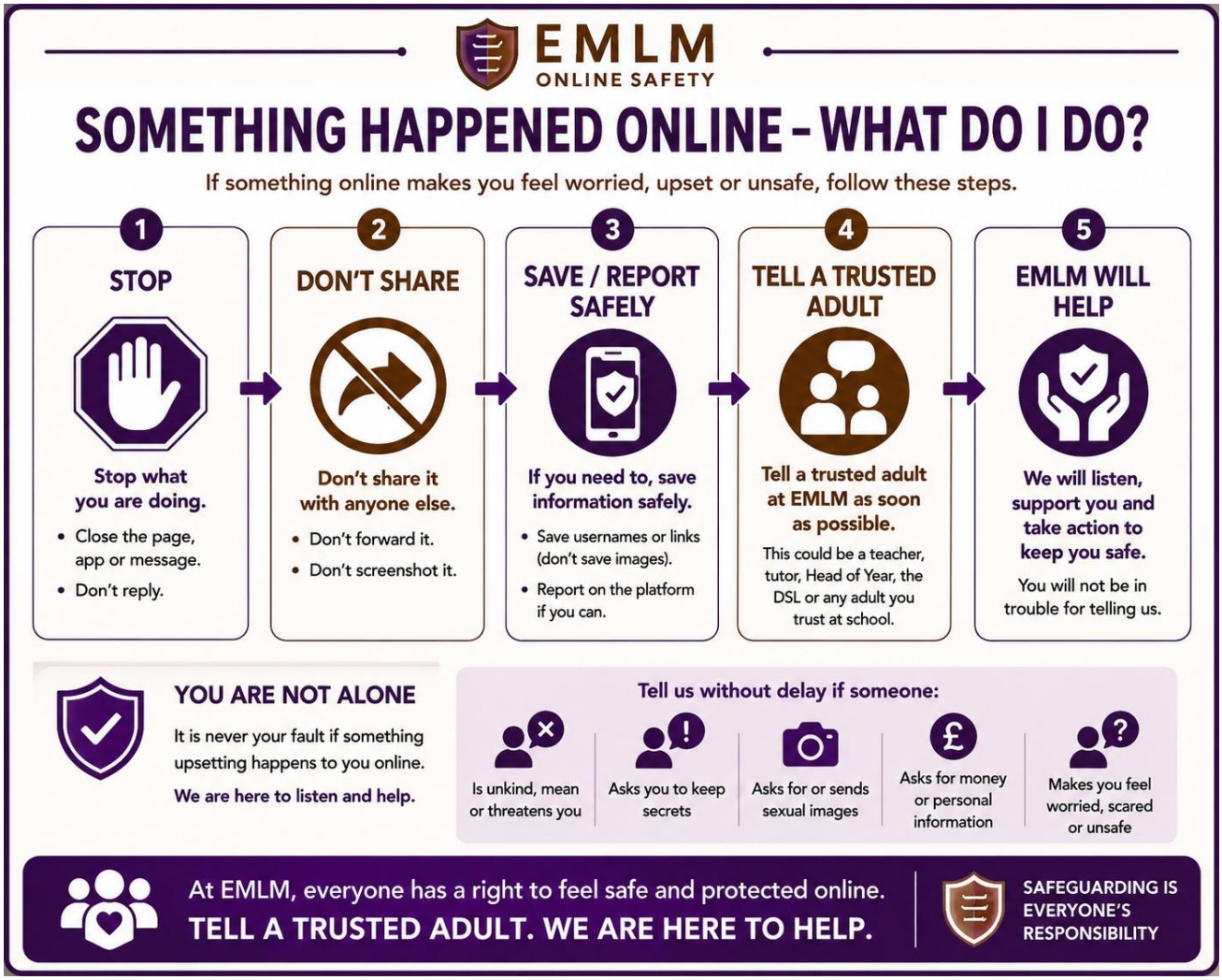
5. Educating learners about online safety

Online safety education will form part of EMLM's safeguarding curriculum and will be reinforced across subjects where appropriate.

Teaching will be age appropriate, developmentally appropriate and responsive to the needs and vulnerabilities of individual learners.

It will reflect statutory Relationships, Sex and Health Education requirements and relevant National Curriculum computing requirements.

Learners will be taught and regularly reminded of the steps they should take if they encounter something online that makes them feel worried, uncomfortable or unsafe, including how to seek help from a trusted adult at EMLM.



5.1 Key Stage 3

Learners will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely;
- Protect their online identity, personal information and privacy;
- Understand privacy and location settings;
- Recognise inappropriate and harmful content, contact, conduct and commercial activity;
- Recognise when online interactions may be unsafe or manipulative;
- Know how, where and when to report concerns and understand that they can speak to any trusted member of staff if something online worries, frightens and makes them feel unsafe.

5.2 Key Stage 4

Learners will be taught:

- How changing technology creates new opportunities and risks;
- Strategies to protect their privacy, identity and personal data;
- How algorithms and online services can influence what users see;
- How to assess the reliability of online content;
- How and where to report a range of online concerns;
- How to respond safely to scams, exploitation, harassment and other online harms.

5.3 By the end of secondary education

Learners will know and understand:

- Their rights, responsibilities and opportunities online and that expectations of appropriate behaviour apply both online and offline;
- The importance of being cautious when sharing personal information online and of using privacy and location settings appropriately;
- The difference between public and private online spaces and the limitations of expecting information shared electronically to remain private;
- The characteristics of social media, including the existence of fake accounts and content which is false, manipulated or generated using artificial intelligence;
- That people may communicate in more extreme ways online than they would face-to-face.
- That people may present exaggerated, edited or idealised versions of themselves online;
- The importance of not providing others with images, information or other material that they would not want distributed further;
- The importance of not forwarding personal, sexual or private material sent to them;
- That once content is shared online it may be copied, manipulated, redistributed or become difficult or impossible to control;
- The risks and potential legal consequences associated with requesting, creating, possessing, sharing or forwarding indecent or sexual imagery involving a person under 18;
- That this includes imagery created or altered using artificial intelligence;
- That learners should seek help if sexual or intimate images of them have been shared and that seeking safeguarding help is encouraged;
- That sharing intimate images involving adults without consent may also constitute a criminal offence;
- What to do and how to report concerns when personal information, images or video have been circulated;
- What deepfakes are, including artificially generated or manipulated video, photographs or audio;
- That deepfakes can be used maliciously as well as for entertainment and can cause significant harm;
- Strategies for critically assessing whether online material may have been digitally manipulated;
- That the internet contains inappropriate, upsetting and illegal content;
- That harmful content can include material encouraging misogyny, hatred, violence, weapon use, self-harm, suicide, extremism or other dangerous behaviour;
- That repeated exposure to online material can normalise or glamorise unhealthy, harmful or abusive behaviour;
- How social media and group communication can escalate disagreements and conflicts;
- Strategies for avoiding escalation and knowing where to seek support;
- How technology and social media can form part of bullying, harassment, stalking, coercive and controlling behaviour and other abusive or illegal behaviour;
- Where and how to seek support about such behaviour;
- How information and personal data are generated, collected, stored, shared and used online;
- That online services may collect information about users for commercial purposes, including profiling and targeted advertising;
- How phishing, fraud and other online scams operate;
- How criminals can use fake websites, messages, accounts or emails to obtain money, login credentials or valuable personal information;
- The risks of financial and sexual extortion, including sextortion;
- How to recognise indicators of sextortion and other sexual scams and how to seek immediate help;
- That paying an offender or complying with further demands may not stop blackmail and that learners should seek support from a trusted adult;
- That generative AI and AI chatbots are developing rapidly;
- That AI systems can produce inaccurate, biased, fabricated, harmful or inappropriate responses;

- That AI chatbots may create an appearance of human understanding or intimacy despite not being human relationships;
- That learners should think critically about the advice, information or emotional interaction generated by AI systems;
- That new technologies should be considered critically in terms of privacy, safeguarding, reliability and potential harm;
- How misinformation, disinformation, conspiracy theories and manipulated content can spread online;
- How to assess the credibility and reliability of information and sources.

The safe use of social media, digital communication, online services and artificial intelligence will also be reinforced within other areas of the curriculum where relevant.

Where required, teaching will be adapted for vulnerable learners, learners who have experienced abuse and learners with SEND.

6. Educating parents/carers about online safety

EMLM will support parents and carers to understand current online risks and the school's approach to online safety. This may be achieved through:

- Letters and other communications;
- Newsletters;
- Information on the EMLM website;
- Parent meetings or consultations;
- Workshops or information sessions;
- Signposting to trusted external resources;
- Communications in response to emerging online risks.

EMLM will provide parents/carers with appropriate information about:

- The school's approach to filtering and monitoring;
- How learners are expected to use technology at school;
- The school's mobile-phone requirements;
- Relevant online services used for teaching and learning;
- Emerging safeguarding issues where communication with families would support learner safety;
- Practical guidance to help parents/carers recognise and respond to emerging online risks, including where appropriate risks associated with social media, artificial intelligence, scams, sextortion and manipulated or AI-generated content;
- How concerns can be reported.

Detailed technical information about filtering, monitoring or security arrangements will not be disclosed where doing so could compromise the effectiveness or security of those systems.

Parents/carers should raise individual safeguarding concerns with the DSL or a member of staff as soon as possible.

Questions about this policy may be raised with the Head of School or DSL.

7. Cyberbullying and Technically Assisted Abuse

7.1 Definition

Cyberbullying is bullying that takes place using technology, including social media, messaging services, online games, email, forums, image-sharing services and other digital platforms.

Bullying is usually behaviour that is repeated over time and intentionally hurts another individual or group, often involving an imbalance of power.
However, EMLM recognises that a single online incident may still cause serious and widespread harm because online content can be rapidly copied, shared and viewed by a large audience.

A harmful online incident will therefore be addressed according to its nature and impact even where the school's definition of bullying is not met.

7.2 Preventing and addressing cyber-bullying

EMLM will ensure learners understand:

- What cyberbullying is;
- Different ways in which technology can be used to harm others;
- How to behave responsibly online;
- How to preserve appropriate evidence without forwarding harmful material;
- How to block and report users where appropriate;
- How to report concerns to EMLM, including that they can speak to any trusted member of staff and do not need to investigate or resolve the matter themselves;
- That learners who witness harmful behaviour are encouraged to report it.

Cyberbullying will be addressed through appropriate areas of the curriculum and wider safeguarding education.

Staff, governors and relevant volunteers will receive appropriate training.

Incidents will be managed in accordance with EMLM's safeguarding and behaviour procedures. Where harmful or inappropriate content has been distributed, EMLM will take reasonable steps to:

- Safeguard those affected;
- Prevent further distribution where possible;
- Preserve appropriate evidence;
- Avoid unnecessary viewing or copying of harmful content;
- Consider whether external agencies or online platforms should be contacted;
- Determine whether referral to children's social care or police is required.

Where an incident may constitute child-on-child abuse, sexual harassment or sexual violence, safeguarding procedures will take precedence.

7.3 Searching and Examining Electronic Devices

Searching, screening and confiscation will be undertaken in accordance with current Department for Education guidance, safeguarding requirements and EMLM's Behaviour Policy.

Only authorised members of staff may carry out searches.

A search may be considered where there are reasonable grounds to suspect that an item:

- Poses a risk to learners or staff;
- Is a prohibited or banned item for which a search is permitted;
- May constitute evidence relating to an offence.

Before conducting a search, the authorised member of staff will consider:

- The urgency and safeguarding implications;
- The risk to the learner or others;
- Whether advice from the DSL is required;
- How the reason for and process of the search will be explained to the learner;
- The learner's cooperation;
- Any vulnerability, SEND or other individual needs.

Where permitted by law and relevant guidance, authorised staff may examine data or files stored on a confiscated electronic device if there is a good reason to do so.

A good reason may exist where there are reasonable grounds to suspect the device has been, or could be, used to:

- Cause harm;
- Undermine the safe environment of EMLM;
- Significantly disrupt teaching and learning;
- Commit an offence.

Safeguarding considerations will take priority where information or files may place a person at risk.

7.4 Suspected nudes or semi-nudes involving children

Where a member of staff suspects that a device may contain a nude, semi-nude, sexual or indecent image involving a child, including an AI-generated or digitally altered image, they must:

- Not deliberately view the image;
- Not copy, print, forward, save or share the image;
- Secure the device where appropriate;
- Report the matter to the DSL immediately;
- Follow the DSL's instructions.

The DSL will manage the incident in accordance with KCSIE and current UKCIS guidance on sharing nudes and semi-nudes.

The DSL will determine whether referral to children's social care, police and/or another agency is appropriate.

Staff should not conduct their own investigation or ask a learner to send or forward an image.

Any search will be undertaken in accordance with current DfE searching, screening and confiscation guidance, UKCIS guidance, safeguarding requirements and EMLM's Behaviour Policy.

Complaints relating to searches or confiscation will be considered under EMLM's Complaints Procedure.

7.5 Artificial intelligence (AI)

EMLM recognises that artificial intelligence, including generative AI, can provide benefits for teaching, learning and administration but can also create safeguarding, privacy, accuracy, bias, copyright, information-security and academic-integrity risks.

AI will therefore be used in a safe, responsible, proportionate and educationally appropriate way. Where AI tools are made available to learners through EMLM:

- Their educational purpose will be considered;
- Age restrictions and product terms will be considered;
- Appropriate safeguarding, supervision, filtering and monitoring arrangements will be in place;
- Privacy and data-protection implications will be considered;
- Learners will be taught to critically evaluate AI-generated outputs;
- Staff will remain professionally accountable for decisions and work for which they are responsible.

Staff must use only AI tools or services authorised by EMLM for activities involving school information, learner information or EMLM business.

Staff and learners must not enter confidential, personal or special-category personal information about learners, families, staff or other identifiable individuals into publicly available or unauthorised generative AI services.

AI-generated information must not automatically be assumed to be accurate. Users should consider the possibility of:

- Fabricated facts or sources;
- Bias;
- Outdated information;
- Inappropriate advice;
- Misinformation or disinformation;
- Copyright or intellectual-property issues.

Learners must follow EMLM's expectations regarding academic integrity and acknowledge the use of AI where required.

AI must not be used to:

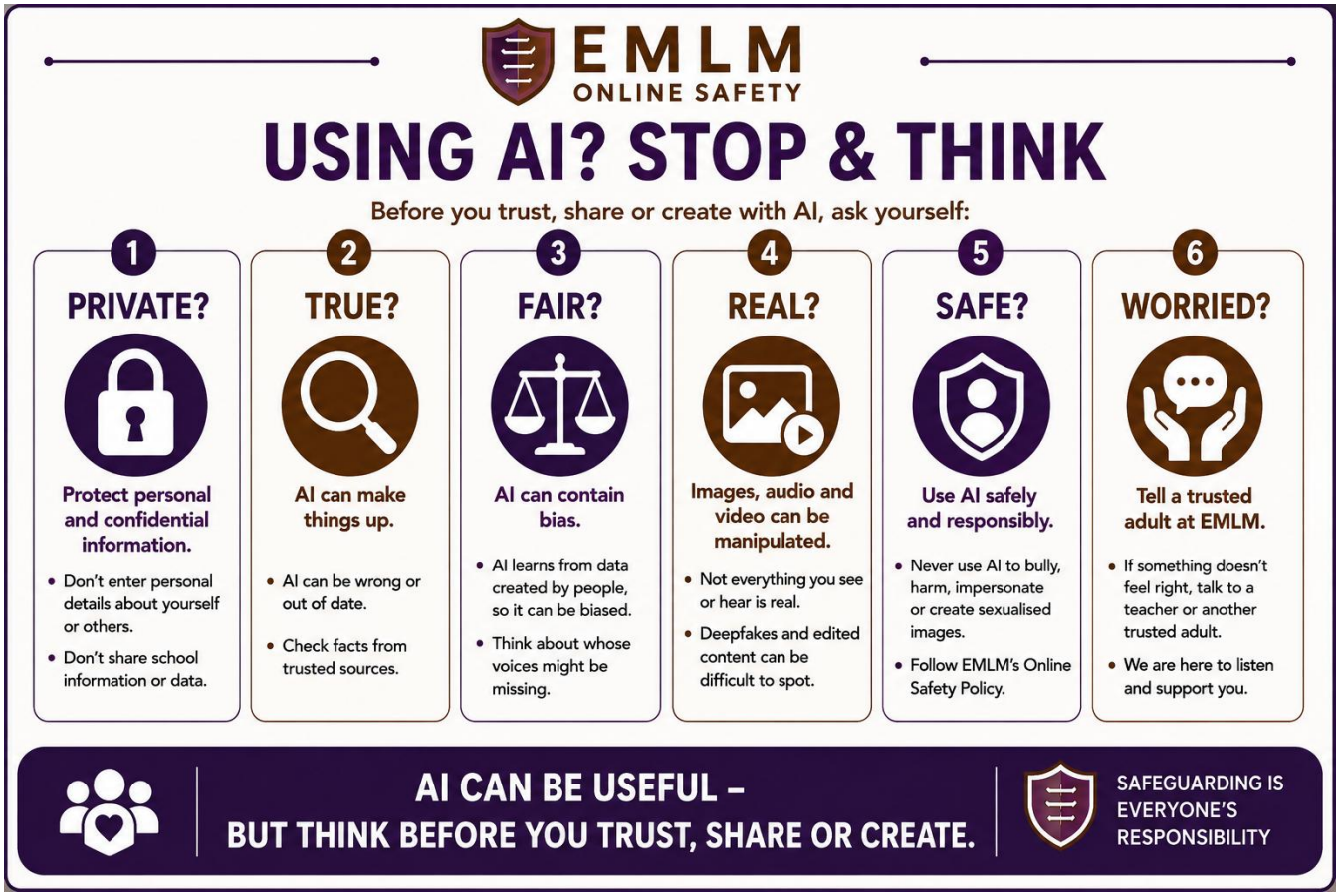
- Bully, intimidate, threaten or humiliate another person;
- Impersonate another person for a harmful or deceptive purpose;

- Create discriminatory or abusive content;
- Create or manipulate sexual or intimate images of another person;
- Generate material designed to facilitate an offence or safeguarding harm;
- Circumvent filtering, monitoring or other security controls.

The creation or distribution of AI-generated sexual imagery involving a child or purporting to depict a child will be treated as a serious safeguarding concern.

The creation or sharing of non-consensual sexualised deepfake imagery involving any member of the school community will also be treated seriously and may result in safeguarding, disciplinary and/or police action.

The following EMLM "Stop & Think" guide summarises the key expectations learners should consider when using artificial intelligence.



EMLM will keep its AI arrangements under review as technology and associated risks develop.

.

8. Acceptable use of Technology and the Internet

All learners, staff, governors, volunteers and relevant visitors are expected to comply with EMLM's acceptable use requirements.

Learners and parents/carers will receive the learner acceptable use agreement in Appendix 1.

Staff, governors, volunteers and relevant visitors will comply with Appendix 2.

School technology and internet access should be used for educational purposes or for the legitimate fulfilment of a person's role.

Reasonable personal use by staff, where permitted by EMLM, must not:

- Interfere with work duties;
- Create a safeguarding or security risk;
- Breach professional standards;
- Breach data-protection requirements;
- Circumvent filtering or monitoring;
- Damage the reputation or interests of EMLM.

EMLM will operate appropriate filtering and monitoring systems to safeguard learners and protect school systems.

Filtering and monitoring will not be relied upon as a substitute for effective supervision, education, safeguarding practice or professional judgement.

Attempts to circumvent filtering, monitoring or cyber-security controls are prohibited unless specifically authorised for legitimate technical testing or administration.

9. Learners using mobile phone and personal smart devices

EMLM recognises that mobile phones can be important to families, particularly while learners travel to and from school.
EMLM operates as a **mobile-phone-free during the school day.** Learners may bring a mobile phone to school for use when travelling to and from school but personal mobile phones must not be accessed or used during the school day unless an authorised exception applies.
On arrival:

- The phone must be switched off;
- The learner must hand the phone to the designated member of staff;
- It will be stored in accordance with EMLM's arrangements;
- It will normally be returned at the end of the school day.

Learners will **not** have access to their personal mobile phones during:

- Lessons;
- Movement between lessons;
- Breaktimes;
- Lunchtimes;
- Other activities forming part of the school day.

This applies to smartphones and other personal smart devices capable of communication, recording or internet access where EMLM determines that the device falls within these arrangements.

Exceptions
An exception may be made where authorised by the Head of School or appropriate senior leader because of:

- A learner's disability;
- A medical need;
- A reasonable adjustment;
- A specific safeguarding requirement;
- Another exceptional circumstance.

Any exception will be managed in a way that protects the learner and the wider school community.

Parents/carers who need to contact a learner during the school day should do so through EMLM.

Learners needing to contact a parent/carer during the school day should speak to a member of staff.

Unauthorised possession or use of a phone during the school day may result in action under the Behaviour Policy, including confiscation where appropriate.

Searching or examining a confiscated device will only take place where lawful and in accordance with section 7.3, Searching and Examining Electronic Devices, of this policy.

10. Staff using work devices outside school

Staff members must take appropriate steps to ensure work devices and information remain secure both on and off the school site.

Staff will:

- Use strong, unique passwords or passphrases;
- Use multi-factor authentication where provided or required;
- Use an approved password manager where authorised;
- Change passwords promptly where compromise is known or suspected;
- Keep devices appropriately locked when unattended;
- Use encryption where provided;
- Install security and operating-system updates promptly;
- Use approved antivirus and security controls;
- Not allow family members, friends or other unauthorised people to use school devices;
- Keep confidential information secure;
- Follow EMLM's data-protection requirements;
- Report lost or stolen devices immediately;
- Report suspected cyber-security incidents or personal data breaches promptly.

Routine password changes will not be required solely for the purpose of changing a password unless this forms part of a specific school security requirement. Passwords must be changed immediately where compromise is suspected or identified.

Staff must not use personal accounts or unauthorised applications or unauthorised online services, including generative AI services, to store, process or transmit confidential school information or personal data.

Work devices must primarily be used for authorised work purposes and must not be used in any way that breaches professional, safeguarding, acceptable-use, information-security or data-protection requirements.

Staff must take reasonable steps to prevent confidential or personal information being seen, overheard or accessed by unauthorised persons when working away from the school site.

Staff must seek advice promptly if they have concerns about the security of a device or account.

11. Filtering and Monitoring

Filtering and monitoring form part of EMLM's wider safeguarding arrangements. EMLM will maintain systems which aim to:

- Prevent access to illegal and inappropriate content;
- Reduce learners' exposure to harmful online material;
- Identify concerning online behaviour or searches where technically possible;
- Support appropriate safeguarding intervention;
- Avoid unreasonably restricting teaching and learning.

The Head of School will ensure that roles and responsibilities for filtering and monitoring are clearly assigned.

The DSL will understand the safeguarding implications of the school's systems.

The ICT Lead will support technical implementation and maintenance.

Relevant staff will understand:

- Their role in relation to filtering and monitoring;
- What the systems do and do not do;
- How to report a concern;
- How to report a system failure;
- Filtering and monitoring systems do not replace professional curiosity, appropriate supervision or the requirement to report safeguarding concerns;
- How alerts and concerns are escalated.

Annual effectiveness review

The effectiveness of EMLM's filtering and monitoring arrangements will be formally reviewed at least once every academic year.

The review will be led by the responsible senior leader and it will consider:

- Whether filtering is working appropriately on relevant internet-connected devices;
- Whether arrangements are effective across relevant locations;
- Whether monitoring identifies the types of safeguarding risks faced by EMLM learners;
- Learners' ages, needs and vulnerabilities;
- SEND and accessibility considerations;
- Emerging risks and technology, including generative AI;
- Any incidents, attempted circumvention or system failures;
- Whether relevant staff understand their responsibilities;
- Feedback from staff and, where appropriate, learners about the effectiveness and impact of filtering and monitoring arrangements;
- Whether escalation and response arrangements are effective.

The outcome of the review, any identified risks and any required actions will be recorded.

Operational or technical checks undertaken throughout the year do not replace this formal annual review.

Where a legitimate educational resource is incorrectly blocked, staff must follow the school's agreed request procedure. They must not circumvent technical safeguards themselves.

12. Cyber Security, Information Security and Access Management

EMLM recognises that weaknesses in information security and cyber-security can create safeguarding as well as operational and data-protection risks.

EMLM will maintain proportionate security arrangements informed by current DfE digital and technology standards and National Cyber Security Centre advice.

Arrangements will include, where appropriate:

- Appropriate firewall and network security;
- Filtering and monitoring;
- Antivirus and malware protection;
- Security updates and patching;
- Secure backup arrangements;
- Role-based access to systems and data;
- Prompt creation, amendment and removal of user accounts;
- Controls over administrative and privileged accounts;
- Multi-factor authentication;
- Secure password arrangements;
- Appropriate device encryption;
- Appropriate control over removable media;
- Staff awareness of phishing and social engineering;
- Incident and data-breach reporting arrangements.

Staff and learners must not attempt to discover, obtain or use another person's password.

Users must not deliberately introduce malicious software, interfere with school systems, carry out unauthorised testing, attempt to bypass security controls, or attempt to access systems, accounts or information for which they do not have permission.

Users must report suspected cyber-security incidents, compromised accounts, phishing attempts or other security concerns promptly in accordance with EMLM's reporting procedures.

Cyber-security incidents that create safeguarding concern will be reported to the DSL as well as the person responsible for ICT.

Suspected or actual personal data breaches must be reported promptly and will be managed in accordance with EMLM's data-protection procedures.

13. Responding to Online Safety Incidents and Misuse

Online safety incidents will be responded to in accordance with the EMLM Compass Approach: Notice, Listen, Protect, Respond, Record and Review. The safety and welfare of learners will be the primary consideration, and safeguarding procedures will take precedence where there is a concern that a learner may be at risk of harm.

EMLM recognises that a learner involved in an online safety incident may have experienced harm, may have caused harm, or may be both at risk of harm and displaying harmful behaviour. The circumstances will be considered carefully, and the response will be proportionate to the individual learner's needs and the nature of the incident.

Where a learner misuses EMLM's ICT systems, internet connection, AI tools or other technology, the school will respond in accordance with safeguarding and behaviour procedures.
Responses will take account of:

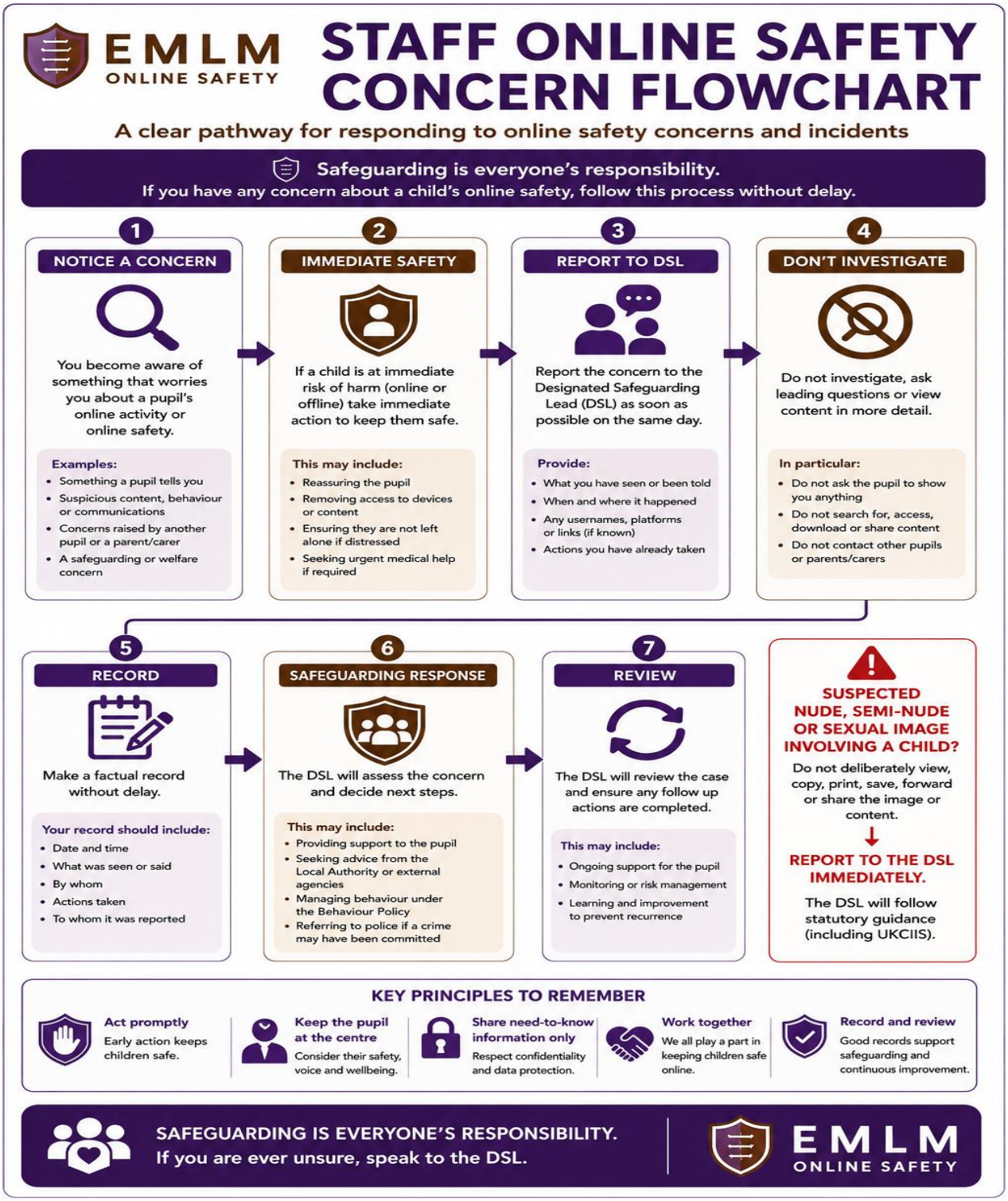
- The learner's age and understanding;
- SEND or other vulnerabilities;
- The nature of the activity;
- Intent;
- The level of harm or potential harm;
- Whether other learners or adults are affected;
- Whether the behaviour is repeated;
- The wider context in which the incident occurred;
- Whether coercion, exploitation or grooming may be involved;
- Whether a criminal offence may have been committed.

Safeguarding needs will be identified and considered before any decision is made about disciplinary action.

Where a member of staff misuses EMLM systems or a personal device in circumstances connected to their professional role, the matter may be dealt with under:

- Safeguarding procedures;
- Staff Code of Conduct;
- Staff disciplinary procedures;
- Managing Allegations procedures;
- Data-protection or cyber-security procedures.

EMLM will consider whether serious incidents or suspected criminal activity should be referred to the police, children's social care, Local Authority Designated Officer or another relevant agency.



14. Training

All new staff will receive appropriate online-safety information and training as part of their induction and safeguarding training.

All staff will receive appropriate refresher safeguarding training, including online safety, at least annually, together with updates when required.

Training will ensure that staff understand that technology is a significant component in many safeguarding and wellbeing issues.

Staff will be made aware that children may abuse or harm other children online, including through:

- Abusive, threatening, discriminatory or harassing messages;
- Misogynistic or sexualised abuse;
- Online bullying;
- Sharing nudes or semi-nudes;
- Non-consensual sharing of intimate imagery;
- Sharing pornography or other unwanted sexual material;
- AI-generated or digitally altered sexual images;
- Impersonation or fake accounts;
- Coercion, exploitation and sextortion;
- Technology-assisted stalking or controlling behaviour;
- Initiation or hazing behaviour with an online element;
- Online elements of physical or sexual abuse.

Training will support staff to:

- Recognise signs of online harm and abuse;
- Respond appropriately to disclosures;
- Understand the school's filtering and monitoring arrangements;
- Understand how to report failures or concerns;
- Understanding that learners may experience online harm, cause online harm, or both and respond in a safeguarding-led and proportionate way;
- Understand the immediate actions required where an incident involves suspected nudes or semi-nudes, including AI-generated or digitally altered sexual imagery;
- Recognise emerging technological risks;
- Support learners to identify and manage risk;
- Maintain appropriate professional boundaries;
- Understand expectations surrounding AI;
- Recognise phishing, social-engineering and cyber-security threats.

The DSL and deputies will undertake appropriate DSL safeguarding training, including online safety, at least every two years and update their knowledge and skills regularly and at least annually.

Governors will receive appropriate safeguarding training which includes online safety.
Volunteers will receive training and information proportionate to their role.

14.1 Online Safety Education for Learners

All learners will receive age-appropriate online safety and cyber-security education.
This may include:

- How criminals and hackers seek to obtain personal information;
- Password and passphrase security;
- Multi-factor authentication;
- Phishing and social engineering;
- Safe use of school accounts;
- Risks associated with removable storage devices;
- How to recognise scams;
- How to report a cyber incident or suspected attack;
- How to report a suspected personal data breach;
- Cyberbullying;
- Grooming and exploitation;
- Online radicalisation and extremism;
- Sextortion;
- Sharing nudes and semi-nudes;
- Misinformation and disinformation;
- AI, deepfakes and manipulated content;
- Safe use of social media;
- Privacy and personal information;

- How to seek help.

Teaching will be age appropriate and developmentally appropriate and will reflect learners' individual needs and vulnerabilities, including SEND, where relevant.

15. Monitoring Arrangements

The DSL will ensure appropriate safeguarding concerns relating to online safety are recorded on CPOMS in accordance with EMLM's safeguarding recording arrangements.

The school will monitor patterns and trends in incidents so that emerging risks can inform:

- Safeguarding practice;
- Curriculum planning;
- Staff training;
- Parent/carer information;
- Filtering and monitoring;
- Behaviour and pastoral support;
- The school's online safety risk assessment.

The Online Safety Policy will be reviewed at least annually. The review will be supported by:

- An annual online safety risk assessment;
- The annual filtering and monitoring effectiveness review;
- Analysis of safeguarding incidents;
- Feedback from staff and learners where appropriate;
- Relevant changes to technology and emerging online risks;
- Current legislation and statutory guidance.

The policy may be reviewed earlier where there is:

- A significant online safety incident;
- A significant change in technology or school systems;
- A change in statutory guidance or legislation;
- Evidence that current arrangements are no longer effective.

The reviewed policy will be presented to the IEB for approval.

16. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff Code of Conduct
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Staff Acceptable Use Agreement
- Learner Acceptable Use Agreement
- Cyber-Security Policies and Procedures, where applicable

Appendix 1: Mobile Phone and Technology Acceptable Use Agreement for Learners, Parents and Carers

Staying safe when using technology at EMLM

Technology can help us learn, communicate and access information. Everyone at EMLM has a responsibility to use technology safely, respectfully and responsibly.

These expectations apply whenever learners use:

- EMLM computers or tablets
- The EMLM internet connection
- School accounts
- Online learning platforms
- School-approved AI tools
- Other digital technology used as part of learning.

They may also apply to online behaviour outside EMLM where that behaviour affects the safety or wellbeing of an EMLM learner or member of the school community.

Mobile phones

EMLM operates a mobile-phone-free school day. Learners may bring a mobile phone to EMLM for use when travelling to and from school.

On arrival:

- I will switch my phone off
- I will hand it to the designated member of staff
- I understand that it will normally be returned at the end of the school day
- I will not keep or use another personal phone or smart device without permission.

If I need to contact a parent/carer during the school day, I will speak to a member of staff.

If my parent/carer needs to contact me, they should contact EMLM.

An exception may be made where EMLM has agreed that I need access to a device because of a medical need, disability, reasonable adjustment, safeguarding need or another exceptional circumstance.

Online and virtual lessons

During online, recorded or live teaching I will follow the same standards of behaviour expected at EMLM.

I will:

- Join learning using the account or link provided to me
- Be respectful to staff and other learners
- Follow staff instructions
- Use chat functions appropriately
- Keep my microphone muted when asked
- Wear appropriate clothing where video is used
- Use an appropriate background where video is used.

I will not:

- Record a lesson without permission
- Take or distribute screenshots without permission
- Share lesson links or login information with unauthorised people
- Disrupt an online lesson
- Share inappropriate content.

Internet use

I will use EMLM's internet and technology for learning and other authorised purposes.
I will not deliberately access, create, search for, save or share the following content:

- Pornographic or sexual content
- Violent or extremely distressing content
- Racist, discriminatory or hateful material
- Content promoting self-harm or suicide
- Extremist or terrorist material
- Illegal material
- Content designed to harm, bully or intimidate another person.

If I accidentally see something upsetting, inappropriate or worrying, I will stop accessing it and tell a member of staff.

I understand that I will not be punished simply for reporting something I have accidentally encountered or asking for safeguarding help.

Logins and passwords

I will:

- Keep my password private
- Use a strong password or passphrase
- Use multi-factor authentication if asked
- Log out of systems when required
- Tell a member of staff if I think someone knows my password.

I will not:

- Use another person's login details
- Ask another learner for their password
- Try to access another person's account.

Social media and communication

I will behave online as I would be expected to behave in person.

I will not:

- Bully, threaten or harass others
- Create harmful fake accounts
- Impersonate another person
- Share another person's personal information without permission
- Share images or recordings of others without appropriate permission
- Deliberately spread false or harmful information.

I understand that content shared online can be copied, altered, screenshotted and distributed beyond the audience I originally intended.

I will think carefully before posting or sharing anything.

People I meet online

I understand that people online may not always be who they claim to be
I will be cautious if someone:

- Asks me to keep a relationship secret
- Requests sexual images
- Requests money
- Requests passwords or financial information
- Pressures me to move conversations to a private platform
- Tries to isolate me from trusted adults
- Threatens or blackmails me
- Pressures me to meet them

I will not arrange to meet someone I only know online without first speaking to a trusted adult.

If someone online makes me frightened, uncomfortable or unsafe, I will tell a trusted adult.

Nudes, semi-nudes and sexual images

- I will not ask another person to send me a nude or sexual image
- I will not create, send or share a nude or sexual image of myself or another young person
- If I have already created or shared an image, or someone has pressured or tricked me into doing so, I can still ask EMLM for help
- I will not forward a sexual image someone sends me
- If someone sends me an unwanted sexual image or asks me for one, I will tell a trusted adult
- If an image of me has been shared, I understand that I can ask EMLM for help and will be supported.

Artificial intelligence

If EMLM allows me to use an AI tool, I will follow staff instructions.
I understand that AI can:

- Make mistakes.
- Invent information.
- Produce biased content.
- Produce inappropriate or harmful responses.
- Make fake images, video, audio or text appear real.

I will check important information rather than assuming AI is correct.

I will not use AI to:

- Bully someone.
- Create a fake sexual image.
- Impersonate someone in order to harm them.
- Produce threatening or discriminatory content.
- Cheat or misrepresent work as my own.
- Circumvent EMLM's safety systems.

I will not enter my own or another person's confidential or personal information into an AI system unless a member of staff has specifically instructed me that it is safe and appropriate to do so using an EMLM approved system.

Extremism and radicalisation

I understand that extremist organisations and individuals can use the internet to influence, groom or exploit people.

If I see content that worries me, or someone tries to pressure me towards extremist views or activity, I will tell a trusted adult.

EMLM uses filtering and monitoring systems to help protect learners.

Attempts to access concerning material will be considered in context and safeguarding action will be taken where appropriate.

Security

I will not:

- Attempt to bypass filtering or monitoring

- Use proxy services or other tools to avoid EMLM's security controls
- Attempt to hack another account or system
- Install unauthorised software
- Deliberately download harmful files
- Introduce malware or viruses
- Interfere with EMLM's ICT systems

If I discover a security problem, I will tell a member of staff rather than trying to exploit it.

Copyright and academic integrity

- I will respect the work of other people
- I will not present someone else's work as my own
- I will identify sources where required
- I will follow staff instructions about whether and how AI may be used in my work.

Cyberbullying

- I will not use technology to bully, embarrass, harass, threaten or deliberately exclude another person
- If I experience or witness cyberbullying, I will tell a trusted adult or report it using EMLM's reporting arrangements.

ICT equipment

I will:

- Treat EMLM equipment carefully
- Use equipment only as instructed
- Report damage or technical problems
- Keep food or drink away from equipment where instructed.

Consequences

If I deliberately misuse EMLM's technology or breach this agreement, EMLM will decide on an appropriate response.

The response will depend upon the seriousness, circumstances and impact of what has happened.

Safeguarding concerns will be dealt with as safeguarding matters.

Serious incidents may be referred to parents/carers, children's social care, police or another appropriate agency.

I understand that if I experience online harm, I can ask for help and EMLM will respond as a safeguarding matter where appropriate.

Agreement and understanding

I understand that:

- EMLM may filter and monitor use of its ICT systems and internet connection for safeguarding, security and other legitimate purposes.
- Activity using school accounts or school systems should not be treated as completely private.
- Any monitoring will be undertaken in accordance with applicable safeguarding and data-protection requirements.
- I should report anything online that makes me feel unsafe, worried or uncomfortable.

Learner name: _____

Learner signature: _____

Date: _____

Parent/carer name: _____

Parent/carer signature: _____

Date: _____

Appendix 2: Acceptable Use agreement for Staff, Governors, Volunteers and Visitors

ACCEPTABLE USE OF EMLM TECHNOLOGY, ICT SYSTEMS AND INTERNET SERVICES.
Name: **Role:**

ACCEPTABLE USE OF EMLM TECHNOLOGY, ICT SYSTEMS AND INTERNET SERVICES.

When using EMLM's ICT systems, accounts, internet connection or work devices, I will:

- Use technology responsibly and professionally.
- Follow safeguarding requirements.
- Protect confidential and personal information.
- Keep passwords and authentication details secure.
- Use only accounts and information I am authorised to access.
- Use only EMLM approved AI services when processing school information or personal data and comply with EMLMs requirements for the use of generative AI.
- Keep work devices appropriately secure.
- Follow EMLM's data-protection requirements.
- Report suspected cyber-security incidents and data breaches promptly.
- Report online safeguarding concerns to the DSL.
- Follow EMLM's filtering and monitoring procedures.
- Ensure learners in my care use technology appropriately.

I will not:

- Deliberately access, create, save or distribute illegal or inappropriate content.
- Create, share, link to or distribute violent, criminal, pornographic, hateful or otherwise harmful material except where specifically authorised as part of a legitimate safeguarding process and handled in accordance with safeguarding guidance.
- Use EMLM technology in a way that could reasonably bring EMLM into disrepute.
- Access social networking, messaging, chat or similar services for personal or unauthorised purposes where prohibited.
- Use abusive, discriminatory or inappropriate language.
- Install unauthorised software.
- Connect unauthorised equipment to the network.
- Share passwords.
- Use another person's login details.
- Access, change or distribute information without authority.
- Share confidential information without lawful authority.
- Circumvent filtering, monitoring or security controls.
- Use unauthorised AI services to process confidential or personal information.
- Take or distribute photographs or recordings of learners other than in accordance with EMLM's procedures.
- Use EMLM systems to promote private commercial interests without authorisation.

I understand that EMLM may lawfully monitor use of its ICT systems and internet connection for safeguarding, security and other legitimate purposes.

If a learner tells me that they have encountered something upsetting, harmful or inappropriate online, or I encounter a safeguarding concern myself, I will report it without delay through EMLM's safeguarding procedures.

If I become aware of suspected child sexual imagery, including AI-generated or manipulated imagery, I will not deliberately view, copy, print, save or forward the image and will report the matter to the DSL immediately.

I understand my responsibilities in relation to filtering and monitoring and know how to report a failure or concern.

I understand that filtering and monitoring do not replace professional curiosity, appropriate supervision or my responsibility to report safeguarding concerns.

I will maintain appropriate professional boundaries when communicating electronically with learners.

I agree to use EMLM's technology safely, lawfully, professionally and responsibly.

Signed: _____ **Date:** _____

Appendix 3: Online Safety Training Needs Self-Audit for Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name: **Role:**	**Date**:
Question	**Yes/Partly/No/Training Required (add comments if necessary)**
Do you know who the DSL and deputy DSLs are?	
Do you understand that online safety is part of safeguarding?	
Do you know how learners can abuse or harm other learners online?	
Do you know what to do if a learner reports an online concern?	
Do you understand that a learner involved in an online incident may have experienced harm, caused harm, or both?	
Do you know which AI tools/services are authorised by EMLM and what information must not be entered into unauthorised AI systems?	
Do you understand that filtering and monitoring systems do not replace professional curiosity, appropriate supervision or safeguarding reporting?	
Do you know what to do if you suspect a device contains a nude, semi-nude or sexual image of a child?	
Do you understand EMLM's mobile-phone arrangements?	
Are you familiar with EMLM's acceptable use requirements?	
Are you familiar with EMLM's filtering and monitoring arrangements?	
Do you understand your responsibilities for filtering and monitoring?	
Do you know how to report a filtering or monitoring failure?	

ONLINE SAFETY TRAINING NEEDS AUDIT	
Do you know how to report a safeguarding concern arising from monitoring?	
Do you understand the principal online risks associated with AI and deepfakes?	
Do you understand EMLM's expectations regarding staff use of generative AI?	
Do you understand the risks of phishing and social engineering?	
Do you use strong, unique passwords/passphrases and MFA where required?	
Do you know how to report a cyber-security incident or suspected personal data breach?	
Are you familiar with EMLM's approach to cyberbullying and technology-assisted abuse?	
Do you understand the online aspects of child-on-child abuse, sexual harassment, coercive control and exploitation?	
Are there areas of online safety in which you require further training?	
Training/actions Identified: •	
Date Actions Completed	

Appendix 4: Online Safety Monitoring and Trends Log

This log is used to support EMLM's monitoring of online safety incidents, patterns and emerging risks. It does not replace safeguarding records on CPOMS. Individual safeguarding concerns must be recorded and managed in accordance with EMLM's safeguarding procedures.



APPENDIX 4: ONLINE SAFETY MONITORING AND TRENDS LOG

Purpose: This log is used to support EMLM's monitoring of online safety incidents, patterns and emerging risks.

This log does not replace individual safeguarding records on CPOMS.

Safeguarding concerns must be reported and recorded in accordance with EMLM's safeguarding procedures and recorded on CPOMS.

Date / Time of Incident	CPOMS Ref.	Year / KS	Category (4Cs)	Type of Concern	Platform / Technology	Location / Context	Safeguarding Action Taken	Parent / Carer Informed	External Referral (where applicable)	Follow-up / Outcome

KEY TO COLUMNS

CATEGORY (4Cs)

Use the 4Cs model to identify the principal category.

- **Content** — Harmful or inappropriate content
- **Contact** — Harmful interaction, grooming, exploitation etc.
- **Conduct** — Harmful online behaviour by or involving a learner
- **Commerce** — Scams, fraud, gambling or financial harm

TYPE OF CONCERN (Examples)

- Cyberbullying
- Grooming / exploitation
- Sextortion
- Nudes / semi-nudes
- Sexual harassment / abuse
- AI / deepfake
- Harmful content
- Self-harm / suicide content
- Misogyny / hate / discrimination
- Extremism / radicalisation
- Scam / phishing / fraud
- Impersonation / fake account
- Privacy / personal information
- Cyber-security
- Filtering / monitoring concern
- Other

PLATFORM / TECHNOLOGY (Examples)

- Social media
- Messaging app
- Gaming platform
- AI tool / service
- School account / system
- Website
- Email
- Other / unknown

LOCATION / CONTEXT (Examples)

- In school
- Outside school
- Home
- Journey to / from school
- Online lesson / virtual learning
- Unknown

NOTES

Do not record pupil names in this log.

Use the CPOMS reference for each incident.

TERMLY / PERIODIC ONLINE SAFETY REVIEW

REVIEW AREA	FINDINGS / ACTIONS
Number and nature of incidents	
Recurring categories/types of harm	
Platforms/technologies of concern	
Patterns involving particular year groups/cohorts	
Emerging risks identified	
Curriculum / online safety education action required	
Staff training required	
Parent/carer information required	
Filtering/monitoring changes to consider	
Pastoral/safeguarding actions	
Online safety risk assessment updated?	Yes ☐ No ☐ N/A ☐
Actions, owner and timescale	

HOW TO USE THIS LOG

- Record every online safety incident or concern that is reported to staff.
- Use the key above to categorise the incident.
- Record the CPOMS reference number.
- Do not include names or identifiable information in this log.
- Review trends regularly (e.g. termly) to identify emerging risks and action required.
- Use findings to inform safeguarding, curriculum, training, parent information, filtering/monitoring and pastoral support.

ALL SAFEGUARDING CONCERNS MUST BE MANAGED ON CPOMS IN ACCORDANCE WITH EMLM'S SAFEGUARDING PROCEDURES.

This log helps EMLM identify patterns and emerging risks so that we can keep all our learners safe online.