Lord Scudamore Academy

Sutton Primary Academy

Kings Caple Primary Academy

St Weonards Academy

Llangrove CE Academy

Marden Primary Academy

Pencombe CofE School

Online Safety Policy including Acceptable Use

Date Approved by The Board of Trustees	26.09.26
Effective period	1/9/26 – 31/08/27
Reviewer	L Orton
Date of Review	Sept 26
Next Review Due	Sept 27

Table of Contents

Introduction ……2

Aims of the Policy ……2

Responsibilities ……3

Education ……6

Cyber Bullying ……11

Examining electronic devices ……11

Searching for electronic devices ……12

Use of Ai ……14

Acceptable Use ……16

Reporting and responding ……20

HMFA Actions ……22

Technology Practice ……25

Filtering and monitoring ……25

Device Management ……27

Public online communications ……29

Digital and video images ……29

Using mobile phones ……29

Training ……31

Outcomes ……35

Appendix

Introduction

Online safety is part of a school's wider duty of care. Through an effective Online Safety Policy, our schools meet statutory obligations to safeguard learners from harm within and outside school and strengthen the schools' position in relation to accountability and legal challenge arising from the use of digital technology.

Aims of the Policy

This policy sets out how schools within the HMFA will safeguard members of our community online, in line with statutory guidance and best practice**.** The schools are aware of the wider statutory requirements that inform this policy.

The HMFA aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, trusteesand governors
- 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')

The 4 key categories of risk:
KCSIE (Para 163 – updated July 2026) describes online safety risks across four broad areas:

- **Content:** - being exposed to illegal, inappropriate, or harmful content, for example: 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 generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct:** behaviour that increases likelihood of harm for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and
- **Commerce:** risks such as gambling, inappropriate advertising, phishing and financial scams

This policy applies to all members of the school community who access or use school digital systems, including staff, learners, trustees, governors, volunteers, parents/carers, visitors and community users**.** It applies to use of school systems both on and off site**,** and to the use of personal devices on the school site (where permitted).

Where online safety concerns or incidents occur outside school and are known to the school, we will respond in line with this policy and related procedures, including the school's Safeguarding and Child Protection, Positive Relationships & Behaviour and Anti-Bullying policies. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of school.

Responsibilities

Online safety is a shared responsibility. All members of the school community are expected to model safe, responsible behaviour, report concerns promptly and learn from incidents and good practice. The roles below clarify accountability.

Headteacher and senior leaders

Senior leaders set the culture and ensure that systems are effective. In line with KCSIE 2026, the DSL/DDSL hold day-to-day lead responsibility.

Senior leaders will:

- Ensure the school meets its safeguarding duty of care, including online safety.
- Know and apply procedures for serious allegations involving staff (Headteacher plus at least one senior leader).
- Ensure that the DSL/ IT provider/technical staff and relevant colleagues are trained and able to fulfil their roles.
- Ensure that all staff receive appropriate online safety training which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring
- ensure that children are taught about how to keep themselves and others safe online, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children.
- Put in place appropriate oversight and support for internal monitoring activity.
- Establish and receive regular online safety reports and act on emerging risks and themes.
- Establish a nominated SLT Lead to work with the DSL and IT provider on the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded

Governors/Trustees

Trustees approve the Online Safety Policy and challenge its effectiveness. KCSIE requires them to:

- Ensure that all staff undergo safeguarding and child protection training (including online safety) which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – at induction and regularly updated
- Ensure that children be taught about safeguarding, including in relation to online safety
- Review the DfE Filtering and Monitoring Standards and discuss with senior staff and service providers what more needs to be done to support the school in meeting this standard.

The Local Committees for each school will nominate a Safeguarding Governor/Trustee who will:

- Meet regularly with the DSL.
- Receive anonymised incident and monitoring summaries.
- Check delivery of key commitments (e.g., education, reporting, staff training).
- Have an understanding of filtering and monitoring and through review, assess the effectiveness of filtering and monitoring with SLT, DSL and IT provider, in line with KCSIE and DfE Filtering and Monitoring standards.

Designated Safeguarding Leads (DSL)

KCSIE (Para 125) states that the DSL leads safeguarding and child protection, including online safety, and understands filtering and monitoring systems and processes. KCSIE requires this to explicit in the DSL's job description.

The DSLs will:

- Lead safeguarding, including online safety.
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.
- Liaise with SLT, the Safeguarding Governor/Trustee, the IT provider and relevant external partners as required.
- Review anonymised incident patterns and filtering/monitoring information.
- With the nominated SLT Lead and the IT provider lead the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded
- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring etc).
- Ensure appropriate support for learners with SEND.

A nominated Online Safety Lead (OSL) may support delivery; the DSL retains lead responsibility.

Curriculum Leads /Online Safety Lead (OSL)

Curriculum leads will work with the DSL to deliver a planned online safety programme through appropriate channels, e.g. Computing, PSHE/RSE, other curriculum areas, assemblies/pastoral provision and national initiatives e.g. Safer Internet Day. They will:

- Help lead with Online Safety and support the DSL day to day.
- Lead development and review of online safety documentation.
- Coordinate awareness, staff confidence and reporting readiness through appropriate training
- Work with curriculum leads to map, embed and evaluate online safety education.
- Liaise with IT and pastoral/support teams.
- Maintain current knowledge of risks across content, contact, conduct and commerce.

Teaching and Support Staff

All staff are expected to uphold professional standards online and contribute to a strong safeguarding culture.

Staff will:

- Follow the Online Safety Policy, Safeguarding/Child Protection Policy, Technical Security Policy and sign/comply with the Staff AUA.
- Maintain professional boundaries (including online/remote learning).
- Supervise learner use of technology and follow procedures for online safety issues
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness.
- Challenge harmful online behaviour and report concerns promptly.

- Use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.
- Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.

IT service provider / technical staff

The IT provider supports leaders and the DSL to meet DfE filtering, monitoring and technical standards. Where services are outsourced, the school remains accountable. IT Technicians at Computeam support Lord Scudamore Academy, Kings Caple Primary Academy, Sutton Primary Academy, St Weonards Academy & Llangrove CE Academy. IT Technicians at John Finch Computers Ltd support Marden Primary Academy & Pencombe CofE School and will:

- Maintain secure infrastructure and managed user access.
- Implement, maintain and update filtering and monitoring; provide reports; act on alerts and concerns.
- Support procurement, risk identification, reviews and checks with SLT/DSL.
- Monitor systems for misuse and report concerns promptly to Headteacher and or DSL
- Follow the school's Online Safety and Technical Security policies and keep technical knowledge current.
- Ensure the HMFA/school meets (as a minimum) the required online safety technical requirements as identified by the local authority/MAT or other relevant body
- Monitor software/systems are implemented and regularly updated as agreed in HMFA policies.

Learners

Learners will:

- Follow the Learner AUA and Online Safety Policy (including personal devices where permitted).
- Report concerns and know how to get help.
- Use technology responsibly, respecting others and their copyright and intellectual property.
- Use AI responsibly: protect original work, check accuracy and avoid plagiarism.
- Understand that out-of-school behaviour may be addressed where it affects the school community.

Parents and carers

Parents/carers are key partners in reinforcing safe online behaviour.

The school will:

- Publish the Online Safety Policy and share the learner AUA *(with local decisions on acknowledgement).*
- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share updates through meetings, newsletters, online channels and campaigns e,g Knowlesley materials for parents, Trustees, Governors and staff.

Parents/Carers will:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the

school's ICT systems and internet (appendices 1 and 2)

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
- The school website.

Parents/carers will be encouraged to reinforce key messages and support safe use of personal devices (where permitted in school).

Visitor & Community users

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected sign a Community User AUA before access is provided. The school welcomes partnership working and shares good practice where appropriate.

Education

Online Safety Education Programme

Online safety education is a core part of the HMFA's safeguarding approach and sits alongside effective technical controls (including filtering and monitoring). In line with KCSIE, online safety is a running and interrelated theme reflected across relevant policies and the curriculum.

The school delivers a planned, progressive and inclusive programme of online safety education for all learners, aligned to nationally recognised guidance and frameworks (including DfE "Teaching Online Safety in Schools", UKCIS "Education for a Connected World", and resources such as SWGfL ProjectEVOLVE). Learning is age-appropriate, builds on prior learning, is matched to need, and is taught through existing curriculum areas (including RSHE/RSE, Health Education, Computing and Citizenship), with assessment and clear intended outcomes.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools In Key Stage KS1, pupils 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 KS2 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, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online

In addition:

- The Online Safety Curriculum incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services)
- Pupils should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services
- Pupils should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the CyberChoices site.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.
- 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 for vulnerable children, victims of abuse and some pupils with SEND.
- KS2 pupils will be taught about deepfakes and how to identify them, that AI chatbots can pose risks by creating fake intimacy or offering harmful advice. In addition, how to critical evaluate AI generated content.
- recognise and manage online risks, including harmful content, contact, conduct and commerce risks;

- understand consent, sexual harassment and sexual violence (including online), supported by safe opportunities for discussion;
- think critically about what they see online, including how to check reliability and accuracy and the role of AI-generated content;
- respect copyright and intellectual property, including when using online material and AI tools;
- understand and follow the learner acceptable use agreement, and act within moral and legal boundaries (including awareness of the Computer Misuse Act 1990).
- understand why online services use minimum-age requirements and how these may support safety, privacy and wellbeing
- make informed decisions about participation in social media, messaging, gaming and other online communities, including services they may not yet be permitted to use
- understand that legal or platform restrictions do not remove the need to learn about online relationships, harmful content, image sharing, scams, exploitation and digital wellbeing
- understand the school's mobile-phone requirements and the safeguarding, behaviour, learning and wellbeing reasons that underpin them.

Where internet use is planned, learners are guided to appropriate resources and supported if unsuitable content is encountered. Where open searching is permitted, staff supervise and remain vigilant. Filtering may be temporarily adjusted for legitimate curriculum research, with auditable approval and clear rationale.

Learner voice is actively used to strengthen the school's approach through feedback, learner representation (e.g. on an Online Safety Group), and opportunities such as digital leaders, peer mentoring, campaigns, and contribution to acceptable use and community-facing online safety activities. Learners are given appropriate opportunities to discuss changes affecting their digital lives and to express concerns about friendship, belonging, access, exclusion and wellbeing.

Staff

In line with DfE Keeping Children Safe in Education (KCSIE), all staff and volunteers receive safeguarding and child protection training, including online safety, at induction and through regular updates (at least annually). Online safety training is integrated into the school's whole-school safeguarding approach, wider staff development and curriculum planning.

- All staff will receive online safety training and understand their responsibilities under this policy.
- A planned programme of online safety, data protection and cybersecurity training for all staff, regularly updated and reinforced. Staff training needs will be reviewed periodically to ensure provision remains relevant and effective.
- staff understand the school's filtering and monitoring requirements, the responsibilities relevant to their role and how concerns or alerts must be reported
- staff understand that filtering and monitoring supports - but does not replace - effective supervision, professional curiosity and safeguarding judgement
- staff are informed of the outcome of the school's annual filtering and monitoring review where relevant to their roles

- staff understand and consistently apply the school's mobile-phone requirements, including expectations for their own professional use of personal devices. They know how authorised exceptions for learners are approved and managed.
- staff follow cyber security policy and requirements.
- Online safety training is provided for all new staff as part of induction, ensuring understanding of the Online Safety Policy and Acceptable Use Agreements, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Lead and Online Safety Lead (or other nominated staff) through external training and review of relevant guidance (e.g. UK Safer Internet Centre, SWGfL, Local Authority or other appropriate organisations).
- Support for staff knowledge-building and consistent practice through structured professional learning resources and, where appropriate, enhanced pathways.
- Regular review of this Online Safety Policy and updates through staff meetings, team briefings and/or INSET.
- Targeted advice, guidance and training from the DSL (or nominated staff) to individuals as required.

Trustees/ Governors

Trustees and Governors should take part in online safety training and awareness activity. This is particularly important for Trustees serving on committees with responsibility for safeguarding, online safety, technology or health and safety.

Training and updates may be provided through (select/delete as appropriate):

- Attendance at training offered by the Local Authority, MAT or other relevant organisations (e.g. Knowlesley).
- Participation in school training and information sessions (for example, staff briefings or parent events). This may include attendance at assemblies or lessons where appropriate.
- Update meetings with the DSL and/or Headteacher to review key themes, incidents and current priorities.

External Stakeholders

Families, the wider community and external agencies play a vital role in supporting the online safety education and wellbeing of learners. The school recognises that parents and carers may have limited awareness of online risks so work to ensure parents are kept informed. Schools may also draw on external agencies to supplement the school's safeguarding approach. The school therefore works actively to build strong partnerships, share key messages, and ensure that families and the wider community are equipped to help keep children safe online.

The following principles underpin the school's engagement with external stakeholders:

Working with Parents and Carers

HMFA will support parents and carers to understand online risks, build confidence, and reinforce safe online behaviours at home. This includes:

- Regular communication and awareness-raising about online safety issues, curriculum content, and reporting routes.
- Providing information through newsletters, the school website, learning platforms, and digital communication tools.
- Offering opportunities such as parent/carer workshops, information events, or drop-ins focused on online safety.
- Involving learners in sharing online safety messages with parents/carers, including contributing to information events.
- Signposting parents and carers to trusted national resources (e.g. UK Safer Internet Centre, Internet Matters, Childnet, SWGfL).
- Promoting and participating in key national events such as Safer Internet Day.
- Ensuring parents and carers understand acceptable use expectations and relevant Trust policies related to online safety.
- clear communication about the school's mobile-phone arrangements, the reasons for the policy, authorised exceptions and the consequences of breaches
- accurate, balanced and age-appropriate information about changes affecting social media and other online services
- guidance and support for parents on managing and supporting their children's online experiences and how to report and manage issues.
- guidance to help parents encourage their children to report online safeguarding concerns, regardless of any restrictions in place
- mechanisms that evaluate the efficacy of school's strategy on mobile phones, online services and family engagement

Wider Community and Agencies

The school recognises the value of working with external organisations to strengthen local online safety awareness and provision. This may include:

- Sharing online safety information, resources or updates with community groups, extended family members and the wider community.
- Providing or supporting family learning opportunities on digital technologies and safe online behaviours.
- Using the school website or social media channels to offer online safety content suitable for the broader community.
- Collaborating with early years settings, childminders, youth and sports groups, libraries, voluntary organisations or other local agencies.
- Drawing on the expertise of external agencies (e.g. UK Safer Internet Centre, CEOP, Local Safeguarding Partnerships, Prevent teams, police and health professionals).

- Participating in shared activities with other schools or settings, including transition projects and multi-school events.
- Supporting external groups to review and improve their own online safety practice, including through recommended tools such as 360 Early Years or 360 Groups.

Cyber-bullying

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the Trust's behaviour policy.)

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 encourage them to do so, including where they are a witness rather than the victim.
Each HMFA 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. Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, Computing and other subjects where appropriate.

All staff, Trustees, Governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

Each school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices –Search and Deletion

The purpose of this policy is to set out HMFAl's lawful and proportionate approach to searching, screening and confiscating electronic devices and examining or deleting data from those devices.

The changing face of information technologies and ever-increasing pupil use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies

which take these changes into account. No such policy can on its own guarantee that the HMFA will not face a legal challenge but having a robust policy which takes account of the Act and applying it in practice will however help to provide the HMFA with justification for what it does.

This policy supports the school's safeguarding responsibilities and must be read alongside the Behaviour Policy, Safeguarding and Child Protection Policy, Online Safety Policy, Technical Security Policy and Data Protection Policy.

This policy reflects Keeping Children Safe in Education KCSIE), DfE Searching, Screening and Confiscation guidance, DfE Behaviour in Schools guidance, DfE Mobile Phones in Schools statutory guidance and relevant statutory legislation.

This policy applies to:

- All learners
- All authorised staff
- All electronic devices in a learner's possession, including mobile phones and other personal smart or interactive communication devices
- Devices on school premises or used in connection with school activities, or where the school has lawful control or charge of the learner
- Behaviour occurring both on and off site where it impacts safeguarding or discipline

The school will ensure that:

- The Behaviour Policy identifies mobile phones and similar devices as items that may be searched for where the school's rules prohibit or restrict their use
    - Searches are lawful, proportionate and necessary
    - Safeguarding considerations are prioritised
    - Devices are only searched where there are reasonable grounds
    - Deletion of data is undertaken only where there is a lawful and justifiable reason
    - Suspected criminal evidence is preserved and referred to the police where required or appropriate
    - Incidents are recorded securely
    - Staff are appropriately trained

Authorised Staff

- The Headteacher will identify staff authorised to conduct searches. Authorised staff may examine or erase data from a confiscated electronic device only where the legal conditions for doing so are met.
- Authorised staff will receive appropriate training including safeguarding, legal thresholds and digital evidence handling.
- Staff cannot be required to undertake searches.

Searching for Electronic Devices

The Headteacher or authorised staff may search a learner or their possessions where the learner agrees, or where there are reasonable grounds to suspect that they possess a prohibited item or an item identified in the school's Behaviour Policy as one that may be searched for. This should include mobile phones and similar devices where required by school policy.

Reasonable force may only be used where permitted by law to search for statutory prohibited items; it must not be used solely to search for an item banned under school rules, such as a mobile phone.

Searches will:

- Be conducted by authorised staff
- Be carried out privately where possible
- Normally be conducted by a member of staff of the same sex as the learner, with another member of staff present, subject to the limited urgent exception permitted by law
- Involve removal of outer clothing only
- Not extend to strip or intimate searches
- Take account of the learner's age, SEND, disability and other individual circumstances

Examination of Electronic Devices

- Staff may examine data or files on a device confiscated following a lawful search where there is good reason to do so - for example, where they reasonably suspect the data has been or could be used to cause harm, disrupt the safe environment of the school or commit an offence.
- Examination will extend only as far as reasonably necessary to establish the facts.
- Where nude or semi-nude images of a child are suspected, staff must not intentionally view, copy, print, share, store or save the image. The device should be secured and the matter referred immediately to the DSL.
- Where material may constitute a criminal offence, the device will be handed to the police.

Deletion of Data

- Data may only be erased where there is good reason to do so, it is not suspected to be evidence of an offence, and its continued existence is likely to cause harm. Where appropriate, the learner or parent/carer should first be asked to delete the material.
- Deletion decisions must be proportionate and recorded.
- Data suspected to constitute evidence of an offence must not be deleted; the device should be passed to the police as soon as reasonably practicable.

Safeguarding Response

All incidents involving device searches will:

- Be reported to the DSL when they involve statutory prohibited items and immediately where a search identifies or suggests a safeguarding concern.
- Be recorded within the school's safeguarding/reporting systems.
- Trigger a risk assessment where appropriate

- Be notified to Parents/carers in accordance with DfE guidance, unless safeguarding considerations require a different approach.

Confiscation
Mobile phones and other devices may be confiscated as a proportionate sanction in accordance with the Behaviour Policy. The length and arrangements for confiscation will take account of the purpose of the sanction and the learner's individual circumstances, including age, SEND, disability, medical need or other agreed exceptions.

Care of Confiscated Devices
The school will ensure secure storage of confiscated devices, documentation of chain of custody and appropriate return procedures.

Use of Artificial Intelligence (AI)

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. In schools, AI is typically used in three areas: learner support, teacher support, and school operations. All use must be safe, ethical and responsible.

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, and by updating procedures where needed. Safeguarding of learners and staff remains central to our approach.

KCSIE 2026 recognises that learners may be subject to harmful online interaction with other users or generative AI applications that simulate these.

HMFA acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work. The schools will:

- Support appropriate use of AI to enhance learning and teaching, improve outcomes, streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by AI.
- Comply with relevant law and guidance, including Keeping Children Safe in Education (KCSIE) and UK GDPR.
- Provide training and guidance for staff, trustees and governors on the benefits, risks and safe use of AI, and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping learners understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.

Safe use, data protection and security

The schools will:

- Protect personal and sensitive data. Staff must not enter personally identifiable or sensitive information into AI tools. Where AI is used, staff should use anonymised data only.
- Require UK GDPR compliance. Staff must ensure any AI tool used meets data protection and security requirements before use.
- Approve tools and accounts. Only school-approved AI tools may be used for schoolwork, and staff should use school-provided AI accounts where available to support oversight and reduce risk.
- Safeguard sensitive information**.** Internal documents, strategic plans or other sensitive material must not be entered into third-party AI tools unless the tool and purpose have been explicitly approved.

Quality, fairness and integrity

The schools will:

- Maintain human oversight. AI may support work but must not replace professional judgement—especially in decisions that affect people. AI outputs must be checked for accuracy before sharing or publishing.
- Promote transparency. Where AI has materially supported an output (e.g. documents, presentations, communications), staff should make this clear where appropriate.
- Address bias and discrimination. We recognise AI outputs may reflect bias. HMFA will use appropriate safeguards, review processes and procurement checks to prioritise fairness and safety.
- Protect copyright and intellectual property. HMFA will take steps to avoid copyright infringement and protect the intellectual property of staff and learners, including ensuring learners' work is not used to train AI systems without appropriate consent.

Reporting, monitoring and accountability

The school will:

- Require prompt reporting of AI-related concerns, including misuse, data incidents or inappropriate outputs, to the Headteacher/Head of School.
- Engage parents/carers with clear information about how AI is used in school (e.g. an "AI in our school" guide).

Use in assessment and feedback

AI tools may be used to support teachers with assessment processes (e.g. identifying areas for improvement and drafting feedback), and to support learners in improving their work. Teachers remain responsible for outcomes and must ensure accuracy, fairness and appropriate use.

Misuse and disciplinary action

Improper use of AI—including breaches of this policy, data protection failures, misuse of sensitive information, or failure to follow agreed processes—may result in action under the school's Staff Disciplinary Policy.

Acceptable use

The Online Safety Policy and acceptable use agreements define acceptable use at the HMFA schools. The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook
- splash screens
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school websites
- peer support.

Acceptable use is defined through the Online Safety Policy and a suite of Acceptable Use Agreements (AUAs) *(see appendices).* AUAs matter most when they are understood, reinforced and followed—not simply signed.

Acceptable/Unacceptable Actions

Schools should agree what is acceptable/unacceptable for their context (age, setting and systems) and record this in the tables below.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
Users must not use online services (apps, games, sites) to create, share, download, upload, transfer or communicate material or comments that are:	Any illegal activity, for example: • Child sexual abuse imagery (CSAM)* • Child sexual abuse/exploitation and grooming • Terrorism-related content • Encouraging, promoting or assisting suicide/self-harm • Sexual image offences (including intimate image abuse/revenge porn and extreme pornography) • Incitement to, or threats of, violence • Hate crime • Public order offences (including harassment and stalking) • Drug-related offences • Weapons/firearms offences • Fraud and financial crime (including money laundering) • *Note: follow UKSIC and UKCIS guidance*					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
	when responding to self-generated intimate images (SGII).					
Users must not attempt or support cybercrime (Computer Misuse Act 1990), including:	• Misusing someone else's username/ID or password to access data, software or systems without authorisation • Gaining unauthorised access to school networks, data or files (including bypassing security controls) • Creating, introducing or spreading malware (viruses, ransomware, harmful scripts) • Phishing, credential theft, or attempting to capture passwords or personal data • Revealing, copying or publishing confidential information (e.g., personal/financial data, databases, access codes) • Disabling, impairing or disrupting network/services (e.g., denial of service) • Using penetration-testing tools without explicit permission *Note: schools should decide whether incidents are dealt with internally or reported to police. Serious or repeat offences should be reported. The National Crime Agency provides routes to divert young people away from cybercrime* and into positive pathways.					X
Unacceptable (not illegal) under school policies, for example:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promoting discrimination, harassment or hateful content				X	
	Using school systems to run a private business or make unauthorised financial gain				X	
	Using tools/services to bypass filtering, monitoring or other safeguards (e.g., VPN/proxy, anonymisers, alternative DNS)				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
	Infringing copyright or intellectual property (including via AI tools, stream ripping or unauthorised copying/sharing)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Sharing content that is offensive, undermines the school's ethos, breaches integrity, or brings the school into disrepute				X	

Consider the following activities when used for non-educational purposes. Add or amend items to reflect current technology, age restrictions and your school's device policy.	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff oversight
Online gaming and in-game chat/voice (*e.g. Roblox, Fortnite, Minecraft*)			x					x
Online shopping and digital commerce (*including in-app purchases, marketplaces, subscriptions)*				x	x			
Cloud storage and file sharing (*e.g., Google Drive, OneDrive, Dropbox, WeTransfer; P2P/torrents*)				x				x

Social media and user-generated platforms *(e.g. TikTok, Instagram, Snapchat, X, Reddit) and other age-restricted services*			x	x				
Messaging, chat and voice *(e.g., WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts)*			x					x
Streaming entertainment/media (video, music, podcasts) *e.g. Netflix, Disney+, Spotify*				x	x			
Video platforms and livestreaming *(e.g. YouTube, Twitch, TikTok LIVE, Instagram Live)*		x			x			
Personal mobile phones and smart devices on site *(phones, smartwatches, earbuds).*				x	X			
Taking photos/video/audio on devices (including sharing, location data and consent)				x				
Other personal devices *(e.g., tablets, handheld consoles, VR headsets, wearables)*				x				x
Personal email accounts on site or on the school network/Wi-Fi *(e.g., Gmail, Outlook.com)*	x				x			
School email used for personal communication (non-work/non-learning)	x				x			
Unapproved AI tools/services *(generative AI chatbots and image/video tools, AI companions, browser extensions)*	x				x			

Reporting and responding

The HMFA is committed to creating a culture where all members of the community feel confident, safe, and supported in reporting online safety concerns. In line with *Keeping Children Safe in Education (KCSIE)*, the HMFA recognises that online risks may occur in school or outside school and may affect children in any setting. Reporting routes must therefore be clear, accessible, inclusive, and consistently understood by all.

The HMFA recognises national findings, including the Ofsted *Review of Sexual Abuse in Schools and Colleges* (2021), which highlight that children may not always feel able to report. The school assumes that harmful online behaviours may be occurring, even where none have been disclosed, and responds by maintaining strong systems for reporting, analysing, and addressing concerns. KCSIE suggests that staff should have a professional curiosity and speak to the designated safeguarding lead (or a deputy) if they have concerns.

Reporting Concerns

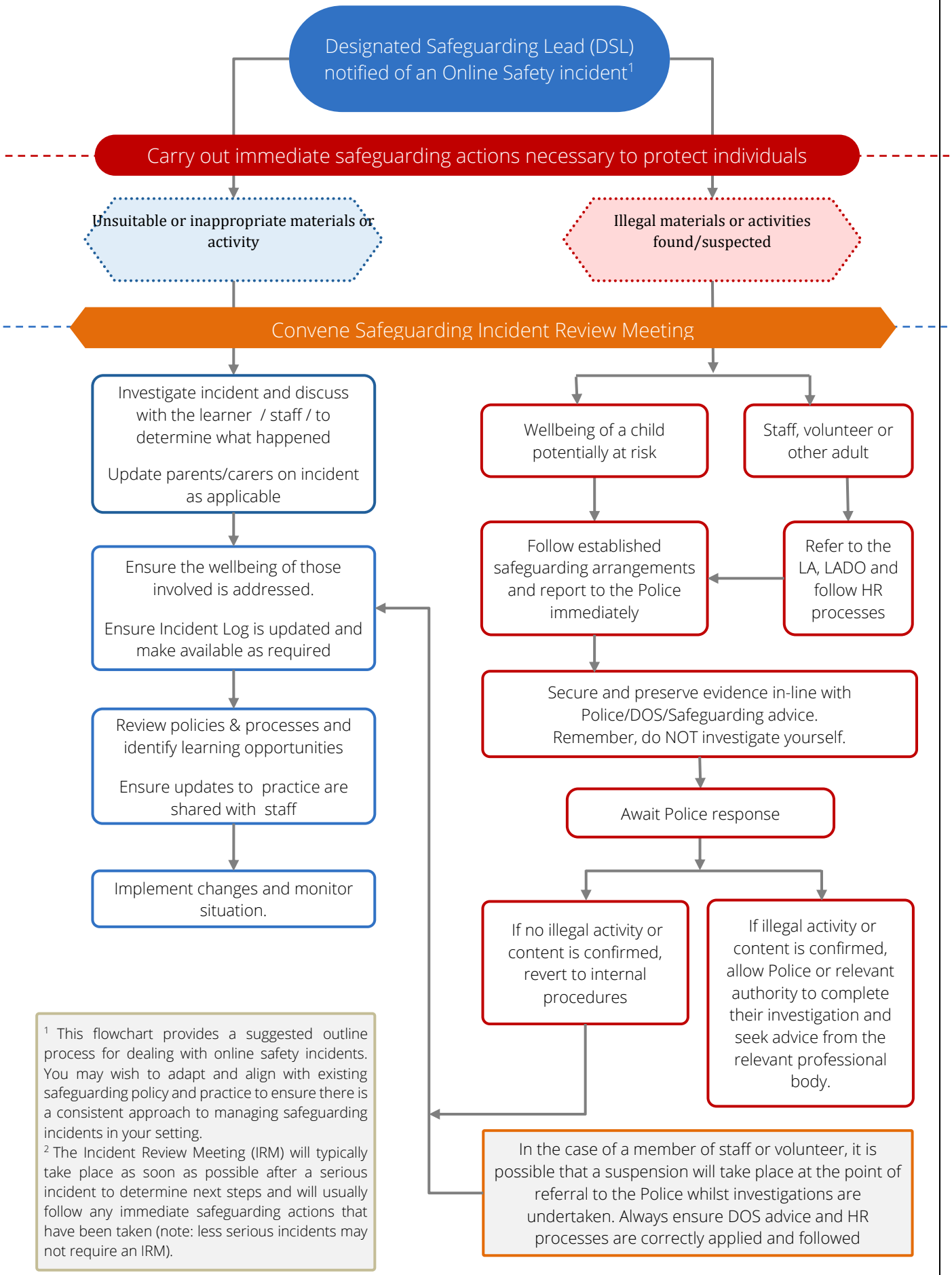
HMFA will ensure that:

- Clear, accessible reporting routes are in place for all members of the school community, including pupils, staff, trustees governors, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies.
- Multiple reporting options are available, such as speaking with the Designated Safeguarding Lead (DSL), email contact, or in-person disclosures.
- Reporting routes are well publicised through induction, assemblies, posters, the school website, and digital platforms.
- All users understand that any online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual imagery.

Responding to Concerns

HMFA will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The DSL and senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):
    - Child sexual abuse material (CSAM)
    - Non-consensual or self-generated images
    - Grooming, exploitation, or sexual harassment
    - Terrorism or extremism
    - Hate crime, fraud, extortion, stalking
    - Cyber offences under the Computer Misuse Act
    - Sale of illegal substances or goods
- Where concerns do not involve suspected illegal activity, devices may be checked using a safe, controlled, and documented process involving senior staff and a designated review device.
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.



[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.

[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows: (the school will need to agree upon its own responses and place the ticks in the relevant columns). They may also wish to add additional text to the column(s) on the left to clarify issues.

HMFA actions

It is more likely that the HMFA will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the HMFA community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to DSL / ODSL	Refer to SLT	Refer to Police/Social Services	Refer to IT Services Provider	Inform parents/carers	Issue a warning / intervention	Remove device / network /internet / access rights	Further sanction, in line with behaviour policy
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.	x	X	X	X	X	X	X	X	x
Unauthorised access to the school network, including using another person's account or sharing usernames/passwords.	x	X	X	X	X	X		X	x
Damaging, corrupting or deleting another user's data.	X	X	X	X	X	X	X	X	x
Sending offensive, harassing or bullying emails, texts or messages.	X	X	X	X	X	X	X	X	x
Unauthorised downloading/uploading, file sharing or distribution of files.	X	X	X	X	X	X	X	X	x
Bypassing filtering (e.g. proxy sites, VPNs or similar tools).	X	X	X		X	X	X	X	x
Failing to report accidental access to offensive or pornographic material	X	X	X		X	x			

Deliberately accessing offensive or pornographic material (or attempting to)	X	X	X	X	X	X	X	X	x
Sharing or receiving content that breaches copyright or data protection law.	X	X	X		X	X	X	X	x
Unauthorised use of devices, including taking photos/videos or audio recordings and using a smartphone in school	x							x	x
Unauthorised use of online services (apps, websites or platforms).	x							x	x
Any online behaviour that could bring the school into disrepute or undermines the school's ethos.	X	X	X		X	X		X	x
Repeated breaches of these rules following previous warnings or sanctions.	X	X	X	X	X	X	X		x

Responding to Staff Actions

Incidents	Refer to line manager	Refer to SLT / Headteacher	Refer to MAT / LA	Refer to Police / LADO	Refer to IT Services Provider	Issue a warning	Further Disciplinary action in line with Behaviour Policy
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.		X	X	X			
Breaching data protection or cyber-security requirements, including network security rules.		x	x		x	x	x
Accessing offensive or pornographic material (or attempting to).		x	x		x	x	x
Damaging systems or data, including corrupting/deleting others' data or deliberately damaging hardware/software.		x	x	x	x	x	x
Bypassing filtering controls (e.g. proxy sites, VPNs or similar methods).		x	x		x	x	x
Unauthorised downloading, uploading or file sharing.	x	x	x		x	x	
Breaching copyright, licensing or intellectual property, including misuse of AI systems.		x			x	x	
Unauthorised account/network access, including sharing passwords, using another person's account, or allowing others access.	x	x			x	x	
Sending offensive, harassing or bullying emails, texts or messages.		x	x		x	x	x
Use of personal email/social media/messaging to communicate with learners or parents/carers.	x	x	x			x	
Inappropriate personal use of school technology, including personal email and	x	x	x			x	

social media use during work time/using school systems.							
Mishandling personal data, including storing, displaying or transferring it insecurely.	x	x			x	x	
Any action that undermines professional conduct or a staff member's professional standing.	x	x				x	
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		x	x			x	x
Failing to report incidents, whether accidental or deliberate.		x	x			x	
Repeated breaches following previous warnings or sanctions.		x	x			x	x

Technology Practice

Purpose

HMFArecognises that the safe and responsible day-to-day use of technology plays a vital role in safeguarding children, supporting learning, and protecting the school community. Clear expectations, consistent practice and informed users help reduce risk while enabling positive and purposeful use of digital technologies.

This approach supports the safeguarding duties set out in *Keeping Children Safe in Education*, emphasising safeguarding and whole-school responsibility, including the requirement to address online safety through policy, practice, education and staff training. It also supports the DfE digital and technology standards and the school's responsibilities for filtering, monitoring, cyber security and digital leadership.

Detailed arrangements are set out in the relevant policy template appendices, including the Technical Security, Cyber Security, Data Security including Filtering and Monitoring and Device Management.

Filtering and Monitoring

The purpose of this policy is to ensure that appropriate filtering and monitoring systems are in place to safeguard learners and staff from harmful or illegal online content, while enabling safe and effective teaching, learning and professional practice. Filtering and monitoring form part of the school's wider safeguarding responsibilities and are implemented in line with Keeping Children Safe in Education (KCSIE) and the DfE Filtering and Monitoring and Technical Standards.

This policy applies to:

- All users of the school's IT systems
- All school-owned devices

- Any device accessing the school's network or internet connection
- Filtering and monitoring provided through third-party or managed services

Roles and Responsibilities

- Trustees provide strategic oversight and assurance that filtering and monitoring standards are met.
- Senior leaders ensure appropriate systems are in place, reviewed and resourced.
- The DSL leads safeguarding responses arising from filtering or monitoring alerts.
- The IT service provider maintains systems and provides reports as agreed.
- All staff report concerns relating to access, alerts or system effectiveness.

HMFAwill ensure that:

- Internet access is filtered to block illegal, harmful and inappropriate content
- Monitoring systems are in place to identify safeguarding concerns and enable timely intervention
- Filtering and monitoring are proportionate, transparent and risk-based
- Roles and responsibilities are clearly defined and understood
- Provision is reviewed regularly and improved in response to risk, practice and guidance
- that staff understand the filtering and monitoring arrangements, their purpose, the responsibilities relevant to their role and the procedures for reporting concerns.
- Filtering and monitoring provision will be reviewed at least annually, with the review considering safeguarding risks, emerging technologies, generative AI, changes in learner behaviour and the effectiveness of technical and procedural controls.
- Trustees will receive sufficient information to assure themselves that the DfE Filtering and Monitoring Standard is being met and that identified actions are followed through.
- Filtering and monitoring are recognised as supporting safeguarding, not replacing education, supervision or professional judgement.
- Filtering
- The school will ensure that filtering systems:
- Block access to illegal content, including child sexual abuse material, terrorist material and other unlawful content
- Manage inappropriate and/or harmful content (including search terms and results). These may include:
    - Gambling
    - Hate speech/discrimination
    - Harmful content
    - Mis/Disinformation
    - Piracy and copyright theft
    - Pornography
    - Self-harm and eating disorders
    - Violence against women and girls
    - AI-generated or AI-enabled harmful content, where technically feasible and proportionate
- Are age-appropriate and suitable for an educational environment
- Are applied consistently to all users, devices and internet connections, including backup connections
- Allow the identification of individual users and devices in the event of breaches of the filtering policy
- No user should be able to deactivate or bypass systems that filter illegal content.

- Detect and, where technically possible, prevent unauthorised circumvention through VPNs, proxy services
  or other methods designed to bypass filtering.
- Support differentiated access for different user groups (e.g. staff and learners)
- Are reviewed regularly to avoid inappropriate over-blocking that may restrict teaching and learning
- The school understands the capabilities and limitations of the system and potential impact on implementation and policy is understood.
- HMFA will use recognised tools and guidance to assure the effectiveness of filtering provision e.g., testfiltering.com

Monitoring

HMFA will ensure that monitoring:

- Enables the identification of safeguarding concerns in a timely manner
- Uses a combination of physical supervision, manual checks and technical systems as appropriate
- Generates alerts that can be prioritised and acted upon by trained staff
- Is subject to human review and professional judgement
- Is clearly communicated to users through policy and acceptable use agreements

Monitoring should be proportionate to the school's risk profile and should not create a culture of surveillance.

Review and Training

Filtering and monitoring provision should be reviewed at least annually and whenever risks or technologies change. Staff, trustees, governors and those with specific responsibilities will receive appropriate training.

Device Management

HMFA schools manage the use of digital devices in a way that supports safeguarding, learning and responsible behaviour. This reflects KCSIE's requirement for a clear mobile/smart technology policy and explicitly links device use to behaviour, safeguarding and education

The school ensures that:

- expectations for the use of school-owned and personal devices are clearly defined and communicated
- device use is consistent with safeguarding, behaviour, data protection and acceptable use policies
- appropriate technical and procedural controls are in place to support safe use
- staff, learners and visitors have been trained/educated/informed and understand their responsibilities when using devices on school premises or systems
- education on the safe and responsible use of devices forms part of the Trust's online safety education
- learners do not have access to mobile phones or other personal smart devices throughout the school day, in accordance with the school's Behaviour and Mobile Phone policies (in line with the DfE statutory guidance)
- any exceptions are limited, clearly defined, authorised and managed appropriately, for example where required for medical, safeguarding, accessibility or SEND-related reasons

- staff model HMFA's requirements and use personal devices only where authorised and professionally appropriate
- procedures cover possession, storage, confiscation, searching and return of devices, in accordance with school policy and current national guidance.

Record of Reviewing Devices / Internet Sites (responding to incidents of misuse)

School	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and Location of Computer Used for Review (for websites) Website(s) Address

/ Device *Reason for Concern*

Conclusion and Action Proposed of Taken

Public Online Communications

HMFA and its schools use public online communications to inform, celebrate success and engage with the wider community, while managing associated risks. It supports KCSIE expectations around professional boundaries and staff conduct online, addresses reputational and safeguarding risk from public platforms while

reinforcing parental engagement and transparency. It has considered the risks of AI manipulation of images as highlighted in the UK Online Harms Early Warning group guidance on Protecting your setting's images from AI manipulation and abuse

The schools ensure that:

- public online communications are appropriate, accurate and well-managed
- public communications from or regarding the school are monitored and addressed where appropriate
- published content complies with safeguarding, data protection and statutory requirements
- to reduce the risk of illegal manipulation of publicly available images of staff and learners, the school has procedures in place to control how those images are shared online. (guidance is available from UKSIC)
- publishing public communications is restricted to authorised and trained staff
- AI-assisted public communications are checked by an authorised person before publication and remain subject to human accountability. AI assisted content should be clearly labelled as such.
- online safety information is shared with parents, carers and the wider community
- staff understand expectations around professional conduct and online behaviour
- the school communicates confirmed changes to policy in line with best practice and Government guidance.

Digital and video images

When a pupil/student joins an HMFA school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent). Parents answer as follows:

- used on HMFA school owned social media
- used in the HMFA school newsletter
- used in HMFA and/or school promotional material / prospectus
- being published in the newspaper (and their online outlets)
- used on the HMFA website and school website
- used on display in the HMFA school (this may also include your child's work and their name or on a TV in the school)
- being used for training purposes.

Parents can withdraw their consent at any time.

Using mobile phones in school

The HMFA strongly advises that pupil mobile phones should not be brought into HMFA.

Where pupils bring mobile phones to a HMFA schoolby prior agreement these are stored in the classroom (or school office) during the school day. They should be clearly labelled with the child's name and passcode protected. Pupil mobile phones must be turned off or placed on silent.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff must not use their mobile phones in the vicinity of the children. They may make calls at break or lunch times on their mobile phones when children are not in their classroom or they may use one of the office phones. Where phones are needed for 2 factor authentication, staff should explain this to the children so that the children know why the phone is out and the purpose of use.

Appropriate use of mobile phones is essential at Breakfast and Kids Club. The use of mobile phones does not detract from the quality of supervision and care of children. All parents have the mobile phone number that is used and are encouraged to text or phone. Practitioners are able to use their personal mobile phones during their break times. During working hours, they must be kept out of the reach of children and parents, in a secure area accessible only to staff. All staff are made aware of their duty to follow this procedure which is set out in the Code of Conduct.

All HMFA staff are asked to be vigilant in challenging other staff/parents/visitors to abide by the above requests.

Mobile phones and other devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or other personal devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team.

Staff personal mobile phones and cameras should not be used to take photographs of children either in the classroom or on HMFA/school trips. School owned iPads are available and should be used in conjunction with the Acceptable Use Policy.

Visitors (including parents) are requested not to use their phones whilst in the school and to switch them off.

Cloud Platforms

HMFA schools are currently using cloud-based Learning platforms that can also provide an online portfolio of their work. These Learning Platforms (LPs) are Tapestry, Google Workspace for Education & Seesaw. In addition, HMFA schools use Microsoft's O365 for staff use.

All cloud-based systems used have been designed specifically for education purposes. The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO (Data Protection Officer) approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only HMFA-approved platforms are used by students or staff to store pupil work

- Class teachers monitor the use of cloud-based systems by pupils regularly in all areas, but with particular regard to messaging and communication
- Pupils are advised on acceptable conduct and use when using the learning platform
- Only members of the current pupil, parent/carers and staff community will have accounts. When staff, pupils etc leave the HMFA school/setting their account or rights to specific HMFA areas will be disabled.

Any concerns with content may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by a member of staff if the user does not comply.
c) Access to the system for the user may be suspended.
d) A pupil's parent/carer may be informed.

Training

Staff, Trustees, Governors and volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- a planned programme of formal online safety, data protection & cyber security training will be made available to all staff via the HMFA's Membership of the National College. This is regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly
- all training will be an integral part of the HMFA's annual safeguarding, cyber security and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the HMFA online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours

The Lead Designated Safeguarding Lead (and other nominated persons) will receive regular updates through attendance at external training events, (e.g., UKSIC/SWGfL/MAT/LA/ Computeam, John Finch Computing Ltd and by reviewing guidance documents released by relevant organisations

- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the IT Director will provide advice/guidance/training to

  individuals as required. Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSLs and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trustees and Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and child protection policy.

In addition to the training below, staff and people with a governing role will be required to complete the following training:

Safeguarding Against Deepfakes: Risks of Generative AI

Teachers			
Training Course title	**Provider**	**Frequency**	**Monitored by**
Annual Certificate in Online Safety for Teaching Staff for Primary Schools & Academies	National College	Annual On Induction	Head of school/Deputy Headteachers Headteachers DSLs
NCSC Cyber Security Training	NCSC Staff training – for RPA insurance	Annual – Autumn Term On Induction	Head of School/ Headteachers/ Deputy Headteachers
Annual Certificate in Cyber Security for Staff for Primary Schools & Academies	National College	Biennial – Spring Term	Head of School/ Headteachers/ Deputy Headteachers
Annual Certificate in Data Protection & GDPR for Staff for Primary Schools & Academies	National College	Biennial – Spring Term On induction	DPO Head of School/ Headteachers/ Deputy Headteachers

Support Staff (Teaching Assistants, Lunchtime Supervisors, Site Staff incl. cleaners, Business & Admin role)			
Training Course title	**Provider**	**Frequency**	**Monitored by**
Annual Certificate in Online Safety for Support Staff for Primary Schools & Academies	National College	Annual On Induction	Head of School/ Headteachers/ Deputy Headteachers DSLs

NCSC Cyber Security Training	NCSC Staff training – for RPA insurance	Annual – Autumn Term On Induction	Head of School/ Headteachers/ Deputy Headteachers
Annual Certificate in Cyber Security for Staff for Primary Schools & Academies	National College	Biennial – Spring Term	Head of School/ Headteachers/ Deputy Headteachers
Annual Certificate in Data Protection & GDPR for Staff for Primary Schools & Academies	National College	Biennial – Spring Term On induction	DPO Head of School/ Headteachers/ Deputy Headteachers

SENCOs			
Training Course title	**Provider**	**Frequency**	**Monitored by**
Annual Advanced Certificate in Online Safety for SENCOs for Primary Schools & Academies	National College	Annual On Induction	CEO DSLs
NCSC Cyber Security Training	NCSC Staff training – for RPA insurance	Annual – Autumn Term On Induction	Head of School/ Headteachers/ Deputy Headteachers
Annual Certificate in Cyber Security for Staff for Primary Schools & Academies	National College	Biennial – Spring Term	CEO
Annual Certificate in Data Protection & GDPR for Leaders for Primary Schools & Academies	National College	Biennial – Spring Term On induction	DPO CEO

Senior Leaders with Cyber Security & Online Safety role - Headteachers, Lead DSL			
Training Course title	**Provider**	**Frequency**	**Monitored by**
Annual Certificate in Online Safety for Teaching Staff for Primary Schools & Academies	National College	Annual On Induction	Headteachers CEO

Filtering & Monitoring in line with KCSIE	National College	On induction	DSLs Headteachers CEO
NCSC Cyber Security Training	NCSC Staff training – for RPA insurance	Annual – Autumn Term On Induction	Head of School/ Headteachers/ Deputy Headteachers
Annual Certificate in Cyber Security for Staff for Primary Schools & Academies	National College	Biennial – Spring Term	Head of School/ Headteachers/ Deputy Headteachers
Annual Certificate in Data Protection & GDPR for Staff for Primary Schools & Academies	National College	Biennial – Spring Term On induction	Head of School/ Headteachers/ Deputy Headteachers DPO CEO

DSLs			
Training Course title	**Provider**	**Frequency**	**Monitored by**
Annual Advanced Certificate in Online Safety for DSLs &	National College	Annual	Head of School/ Headteachers/ Deputy Headteachers
Deputy DSLs for Primary Schools & Academies		On Induction	
NCSC Cyber Security Training	NCSC Staff training – for RPA insurance	Annual – Autumn Term On Induction	Head of School/ Headteachers/ Deputy Headteachers
Annual Certificate in Cyber Security for Staff for Primary Schools & Academies	National College	Biennial – Spring Term	Head of School/ Headteachers/ Deputy Headteachers
Annual Certificate in Data Protection & GDPR for Staff for Primary Schools & Academies	National College	Biennial – Spring Term On induction	DPO Head of School/ Headteachers/ Deputy Headteachers
Filtering & Monitoring bespoke to school/academy	IT Support company (Computeam or JFC)	When changes are made to filtering & monitoring systems On induction	Head of School/ Headteachers/ Deputy Headteachers CEO

Trustees/Governors			
Training Course title	**Provider**	**Frequency**	**Monitored by**
Annual Certificate in Online Safety for Governors for Primary Schools & Academies	National College	Annual On Induction	Headteachers Clerk to Governors Lead Governance Professional (LGP)

NCSC Cyber Security Training	NCSC Staff training – for RPA insurance	Annual – Autumn Term On Induction	Clerk to Governors LGP CEO
Annual Certificate in Cyber Security for Governors for Primary Schools & Academies	National College	Biennial – Spring Term	Clerk to Governors LGP CEO
Annual Certificate in Data Protection &	National College	Biennial – Spring Term	DPO
GDPR for Governors for Primary Schools & Academies		On induction	Clerk to Governors LGP CEO

Outcomes

The impact of the Online Safety Policy and practice is evaluated regularly using evidence such as online safety incident logs, behaviour and bullying records, and surveys of staff, learners and parents/carers.

This process ensures that:

- Evidence from audits and reviews is discussed through balanced professional debate, alongside the impact of preventative work (education, awareness and training).
- Clear reporting routes are in place so patterns, themes and outcomes are shared regularly with senior leaders and governors.
- Parents/carers are informed of key patterns and learning through the school's online safety communication and awareness activity.
- Online safety and related policies and procedures are updated in response to evidence and emerging risks.
- Learning and evidence of impact are shared, where appropriate, with other schools, agencies and local authorities to support a consistent local approach to online safety

The Online Safety Policy is part of the school safeguarding framework and should be read alongside Safeguarding/Child Protection, Behaviour, Anti-Bullying and Data Protection, Technical Security, Cyber Security and AI policies.

Implementation, monitoring and review

- Reviewed at least annually (KCSIE Para 121) , and sooner if risks/technology change.
- Monitored by the DSLs and governors using anonymised incident trends, filtering/monitoring reports and education review activity.
- Findings inform improvement planning and staff training priorities.

Communication and accessibility

36

- Shared at staff induction and reinforced through training.
- Communicated to learners and parents/carers through AUAs and awareness activity.
- Published on the school website.

Appendix A1 -

Acceptable Use Agreement Template – for younger learners (EY/KS1)

Our Technology Rules

I will follow these rules to use computers, tablets and the internet safely at school. These rules help us all stay safe and have fun using computers and tablets at school!

Staying Safe

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- I will keep my passwords secret and tell my teacher if I need help.
- I understand that people online are not always who they say they are. I will only talk to people online if my teacher or a trusted adult says it's OK.
- I will not share my name, address, or pictures without asking my teacher or a trusted adult first.
- If I see something that makes me feel worried or upset, I will tell my teacher or a trusted adult straight away.
- I will only use apps, games or websites my teacher says are safe.

Using Technology Kindly

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and tablets I use.
- I will only look at things my teacher says are OK.

Making Good Choices

- I will ask my teacher before I use someone else's pictures or work.
- I will take breaks from screens and do other fun things too.
- I know that I can say no / please stop to anyone online who makes me feel sad, uncomfortable, embarrassed or upset.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

What Happens If I Forget the Rules

- If I forget the rules, my teacher will help me learn to make better choices next time.

My Name:		Date:
R: Signed		
Y1: Signed		
Y2: Signed		

Appendix A2

Acceptable Use Agreement Template – for KS2 Learners

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

I agree to use the school's digital systems, devices and online services safely and responsibly to protect me, other learners and the school.

Keeping Safe Online

- The school will check how I use devices and online services to keep everyone safe.
- I will keep my usernames and passwords private and tell a trusted adult if someone else knows them.
- I will be careful when talking to people online and will only talk to people I know and trust.
- I will not share personal information like my name, address, or photos without asking a trusted adult.
- I will only take or share images of myself, or others, when fully dressed.
- If I see or hear something online that worries or upsets me, I will tell a trusted adult straight away.
- I will only meet people I have spoken to online if a trusted adult is with me.

Using Devices and Online Services Sensibly

- I will only use devices, apps, games and websites that my teacher or parent/carer says are suitable for my age.
- I know that I am not allowed to use some online services and I know what they are.
- I will always ask permission and check with a trusted adult before using someone else's work or pictures.
- I will make sure the information I find online is true by checking carefully.
- I will only use apps or tools, like AI, that my teacher has said are OK, and I will ask for help if I'm unsure.
- I will not copy or use music, videos, or games unless I have permission.
- I will tell a trusted adult about any damage to devices or if anything else goes wrong.
- I will check with trusted adults before clicking on any unexpected messages or links (even if these look as though they are from people that I already know).

Being Respectful and Responsible

- I will treat others kindly online, just as I do in real life.
- I will make good choices about what I share online to protect myself and others.
- I understand that not every app or website is suitable for children my age.
- If I want to join a new app, game or online community, I will speak to a trusted adult first.
- I will spend a healthy amount of time using devices and make time for other activities too.
- I will always think about how my behaviour online could affect me, my friends, and my school.
- If I make a mistake online, I know I can ask a trusted adult for help

What Happens If I Break These Rules?

- If I don't follow these rules, my teacher may stop me from using computers or devices, speak to my parents, or take other actions to help me make better choices in the future.

By following these rules, I can enjoy using technology safely and responsibly.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

My Name:		Date:
R: Signed		
Y1: Signed		
Y2: Signed		

Appendix A3 –

Parent/Carer Acceptable Use Agreement Template

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that learners have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the learner acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work. (Schools will need to decide whether they wish parents to sign the acceptable use agreement on behalf of their child)

Permission Form

Parent/Carers Name: .....

Learner Name: .....

As the parent/carer of the above learners, I give permission for my son/daughter to have access to the digital technologies at school.

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using devices.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of digital technologies at home and will inform the school if I have concerns over my child's online safety.

As the schools is collecting personal data by issuing this form, it should inform parents/carers as to:

This form will be included in all new starter packs and should be completed and returned to the school. From time to time, the school may ask parents/carers to complete an updated form to ensure that the information and permissions we hold remain current.

Completed forms will be accessible only to relevant authorised staff, including administration staff and class teachers, where appropriate. Paper copies will be stored securely within pupil records, and relevant information will also be recorded electronically on the school's MIS, Arbor, in accordance with the school's data protection procedures.

Signed: .....

Date: .....

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Learners and members of staff may record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's **delete as relevant** first name/initials will be used.

The school will comply with the Data Protection Act and request parent's/carer's permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

As the schools is collecting personal data by issuing this form, it should inform parents/carers as to:

This form will be included in all new starter packs and should be completed and returned to the school. From time to time, the school may ask parents/carers to complete an updated form to ensure that the information and permissions we hold remain current.

Completed forms will be accessible only to relevant authorised staff, including administration staff and class teachers, where appropriate. Paper copies will be stored securely within pupil records, and relevant

information will also be recorded electronically on the school's MIS, Arbor, in accordance with the school's data protection procedures.

During your child's time at school, photographs and digital images may be taken to celebrate achievements, record school activities and share the life of the school. Where appropriate consent has been provided, these images may be published in the school newsletter, on the school website and on the school's Facebook page.

Digital images may be stored securely on school devices and the school's cloud-based network and will only be accessible to authorised staff as appropriate.

Parents/carers may withdraw their consent or request the deletion of images by contacting the school at admin@lordscudamore.hmfa.org.uk. The school will respond to such requests in accordance with its data protection procedures.

Digital/Video Images Permission Form

Parent/Carers Name:..... Learner Name:.....

As the parent/carer of the above learner, I agree to the school taking digital/video images of my child/children.	Yes/No
I agree to these images being used:	
• to support learning activities.	Yes/No
• in publicity that reasonably celebrates success and promotes the work of the school.	Yes/No
I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes/No

Signed: .....

Date: .....

Appendix A4 - Staff (and Volunteer) Acceptable Use Agreement Template

School Policy

Digital technologies have become integral to the lives of everyone, including children and young people , both within schools and in their lives outside school. The internet and digital technologies are powerful tools, which can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. HMFA has the right to protect itself and its systems and all users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while online and using digital technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff are protected from potential risk in their use of technology in their everyday work.

HMFA will try to ensure that staff and volunteers have good access to digital technology to enhance their work, to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible, informed and professionally competent users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to minimise the risk to the safety, privacy or security of the school community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that filtering and monitoring are safeguarding measures designed to protect learners, staff and school systems. Where my role requires it, I will act promptly on concerns or alerts in accordance with the school's safeguarding procedures.
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of the school
- I understand that the school devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will store my passwords securely and in line with the school's relevant security policy.
- I will immediately report any safeguarding, cyber security, filtering, monitoring or data protection concern using the school's agreed reporting procedures.
- I will complete the online safety, safeguarding and cyber security training required by the school and keep my knowledge up to date.

Protecting Learners, School Systems and Information:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language, and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images and taking account of parental permissions. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the school in accordance with school policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will only communicate with learners, parents/carers and colleagues using school-approved systems. Any such communication will be professional in tone and manner
- I will not engage in any online activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education/UK GDPR)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack
- When using AI systems in my professional role I will use these responsibly and:
  - will only use AI technologies approved by the school
  - will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
  - to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
  - will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
  - ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance
  - critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
  - will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being
  - I recognise that AI supports, but does not replace, my professional judgement. I remain responsible for the accuracy, appropriateness and safeguarding implications of any AI-assisted work.
- I will follow the school's expectations for the professional use of mobile phones and other connected devices, ensuring only permitted use
- When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.
- I will not use personal accounts on school systems.

- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will protect school systems by following the school's cyber security procedures.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will respect filtering, monitoring and other security measures and report any concerns about their effectiveness.
- I understand that some websites or services may be restricted for safeguarding reasons and will use the school's agreed process where access is required for legitimate educational purposes.
- I will not install or attempt to install unauthorised programmes of any type on a school device , nor will I try to alter device settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Security Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will only use school-approved cloud services and digital platforms for storing or sharing school information.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using digital technologies in my professional capacity or for school sanctioned personal use:

- I will ensure that I have appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content
- Where content is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that my professional responsibilities extend to my conduct in public online spaces where this could affect learners, colleagues or the reputation of the school.
- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.
- I will model safe, responsible and balanced use of digital technology in my professional practice.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a disciplinary investigation, a suspension, referral to the LADO, and in the event of illegal activities, the involvement of the Police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

Appendix A5 - Acceptable Use Agreement for Community Users

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: ..... Signed: ..... Date: …….

Appendix A6 - Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Appendix A7 Online Safety Training Needs – Self -audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	

ONLINE SAFETY TRAINING NEEDS AUDIT	
Are you familiar with the school's acceptable use agreement for staff, volunteers, trustees, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	

Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Legislation

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

The Data (Use and Access) Act 2025 (DUAA)

Updates, rather than replaces, existing UK data protection law, including UK GDPR and the Data Protection Act 2018. For schools, the fundamental requirements to handle personal data lawfully, fairly, transparently and securely remain, but the Act introduces and clarifies provisions relating to areas such as lawful processing, automated decision-making, data sharing and the handling of data protection complaints. Schools should review their data protection policies, privacy information and procedures to ensure they reflect the changes, paying particular attention to how pupil, staff and

parent/carer data is collected, accessed, shared and used, and to the use of emerging technologies and online services that process personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.

Monitoring but not recording is also permissible in order to:

- Ascertain whether the communication is business or personal;
- Protect or support help line staff.

The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child

under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of learners when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices for DfE guidance)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

https://www.gov.uk/guidance/what-academies-free-schools-and-colleges-should-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

Online Safety Act 2023

The Online Safety Act 2023 is a new set of laws that protects children and adults online. It puts a range of new duties on social media companies and search services, making them more responsible for their users' safety on their platforms. The Act will give providers new duties to implement systems and processes to reduce risks their services are used for illegal activity, and to take down illegal content when it does appear.

Ofcom is the independent regulator of Online Safety. It will set out steps providers can take to fulfil their safety duties in codes of practice. It has a broad range of powers to assess and enforce providers' compliance with the framework.

Links to other organisations or documents

UK Safer Internet Centre
Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/
Harmful Sexual Support Service

CEOP
CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools / Resources for Schools / other organisations

Whisper Anonymous Reporting Tool - https://swgfl.org.uk/products/whisper/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

SWGfL Test filtering - http://testfiltering.com/

SWGfL 360 Groups – online safety self review tool for organisations working with children

SWGfL 360 Early Years - online safety self review tool for early years organisations

Childline – Report / Remove

SWGfL- Assisted Monitoring

SWGfL – Resources for Education

DfE Using AI in education settings: support materials

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Childnet – Cyberbullying guidance and practical PSHE toolkit:
http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk

SWGfL - ProjectEvolveEdu

UKCCIS – Education for a connected world framework

Department for Education: Teaching Online Safety in Schools

Teach Today – www.teachtoday.eu/

Data Protection

DfE – Data Protection in schools toolkit

ICO Guides for Organisations

ICO Guidance on taking photos in schools

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

UK Safer Internet Centre Professionals Online Safety Helpline

SWGfL – Online Safety Training

Infrastructure/Technical Support/Cyber-security

DfE – Technical Standards for Schools and Colleges

UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

SWGfL - Cyber Security in Schools.

NCA – Guide to the Computer Misuse Act

SWGfL- Assisted Monitoring

Secure Schools – Cyber Security

Working with parents and carers
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent
Prevent Duty Guidance
Childnet – Trust Me

Research
Ofcom – Childrens Media Habits
Ofsted: Review of sexual abuse in schools and colleges

Further links can be found at the end of the UKCIS Education for a Connected World Framework