Lord Scudamore Academy
Sutton Primary Academy
Kings Caple Primary Academy
St Weonards Academy
Llangrove CE Academy
Marden Primary Academy
Pencombe CE School

Online Safety Policy inc Acceptable Use

December 2025

Date Approved by The Board of Trustees	**11/12/25**
Effective period	**1/12/25 – 31/08/26**
Reviewer	**J Brace**
Date of Review	**26/11/2025**
Next Review Due	**July 26**

Next review date: July 26

Co-ordinator – J Brace

Contents

1. Aims

The HMFA aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and 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')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

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

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schoolshttps://www.gov.uk/government/publications/preventing-and-tackling-bullying
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The people with a governing role

The HMFA has a Board of Trustees, each school in the Multi-Academy Trust has a Local Committee, other schools in the HMFA Federation have Directors or Governors. For the purpose of this policy we will refer to these people collectively as “people with a governing role”. The Board of Trustees and people with a governing role have overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

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

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

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

The people with a governing role will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The people with a governing role will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE’s filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

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

The HMFA Trustee who oversees online safety is Rowena Williams.

All governors will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school’s ICT systems and the internet (appendix 3)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a ‘one size fits all’ approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

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

3.3 The designated safeguarding lead (DSL)

Details of the HMFA designated safeguarding lead (DSLs) and deputies are set out in our Safeguarding and Child Protection Policy, as well as relevant job descriptions.

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

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and people with a governing role to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the IT Director to make sure the appropriate systems and processes are in place
- Working with the headteacher, IT Director and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or people with a governing role
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The IT Director

The IT Director is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.5 Technical Staff

The network manager/technical staff are:-

IT Technicians at Computeam who support Lord Scudamore Academy, Kings Caple Primary Academy, Sutton Primary Academy, St Weonards Academy & Llangrove CE Academy.

IT Technicians at John Finch Computers Ltd who support Marden Primary Academy & Pencombe CE School.
are responsible for ensuring that:

- they are aware of and follow the HMFA Online Safety Policy and Technical Security Policy to carry out their work effectively in line with HMFA policy
- the HMFA/school technical infrastructure is secure and is not open to misuse or malicious attack
- the HMFA/school meets (as a minimum) the required online safety technical requirements as identified by the local authority/MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to DSLs/Heads of Schools and/or Jo Brace for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see 'IT Technical Security Policy')
- monitoring software/systems are implemented and regularly updated as agreed in HMFA policies.

3.6 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by informing the ICT manager and DSL.
- Following the correct procedures by contacting the ICT Manager if they need to have a website unblocked for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

3.6 Parents/carers

Parents/carers are expected to:

- 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.

3.7 Visitors and members of the community

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 to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils are taught about online safety as part of the curriculum. Staff within the HMFA MAT follow the Kapow Primary scheme of work, schools in the federation follow ProjectEVOLVE .

The text below is taken from the National Curriculum computing programmes of study and the government's guidance on relationships education, relationships and sex education (RSE) and health education (for introduction 1 September 2026).

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 (KS) 1**, 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 (KS) 2** will be taught to:

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

By the **end of primary school**, 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

- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with 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.

5. Educating parents/carers about online safety

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

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- the pupils – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or the local authority/MAT
- HMFA Parents also have access to the National College Online Safety resources.

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. 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, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The 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.

6.3 Examining electronic devices –Search and Deletion Policy

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.

The particular changes we deal with here are the added power to screen, confiscate and search for items ‘banned under the school rules’ and the power to ‘delete data’ stored on confiscated electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff.

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question relates to an offence and/or may be used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

Responsibilities

The headteachers / executive headteachers have authorised the Heads of Schools and any member of the HMFA's senior leadership team (SLT) to carry out searches for and of electronic devices and the deletion of data / files on those devices. The school must publicise the school behaviour policy, in writing, to staff, parents/carers and learners at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).

Training/Awareness

Members of staff authorised to carry out searches for and of electronic devices and to access and delete data / files from those devices receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Our Search Policy

Screening

If the headteacher decides to introduce a screening arrangement, they will inform pupils and parents in advance to explain what the screening will involve and why it will be introduced.

Search:

The HMFA Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items.

Pupils are only allowed to bring mobile phones into school from Year 5 onwards- those devices must be kept in a designated area and turned off during the school day.
This Online Safety Policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices. The HMFA's policy on the use of mobile devices is set out in of this page 31 of this policy and the sanctions relating to breaches of these rules on from page 17.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or files on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- **Searching with consent** - Authorised staff may search with the pupil's consent for any item.

- **Searching without consent** - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for.

In carrying out the search:

- The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item i.e., an item banned by the school rules and which can be searched for.
- The authorised member of staff carrying out the search must be the same gender as the pupil being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the pupil being searched.
- There is a limited exception to this rule: authorised staff can carry out a search of a pupil of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

- The person conducting the search may not require the pupil to remove any clothing other than outer clothing
- Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves)
- A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff
- 'Possessions' means any goods over which the pupil has or appears to have control – this includes desks, lockers and bags
- The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do
- Use of force – force cannot be used to search without consent for items banned under the HMFA rules regardless of whether the rules say an item can be searched for.

Electronic devices

The DfE guidance – Searching, Screening and Confiscation received significant updates in July 2022 and now states:

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.
- As with all prohibited items, staff should first consider the appropriate safeguarding response if they find images, data or files on an electronic device that they reasonably suspect are likely to put a person at risk
- Staff may examine any data or files on an electronic device they have confiscated as a result of a search .. if there is good reason to do so (defined earlier in the guidance as)
    - poses a risk to staff or pupils;

- is prohibited, or identified in the school rules for which a search can be made or
- is evidence in relation to an offence.

- If the member of staff conducting the search suspects they may find an indecent image of a child (sometimes known as nude or semi-nude images), the member of staff should never intentionally view the image, and must never copy, print, share, store or save such images. When an incident might involve an indecent image of a child and/or video, the member of staff should confiscate the device, avoid looking at the device and refer the incident to the designated safeguarding lead (or deputy) as the most appropriate person to advise on the school's response. Handling such reports or concerns can be especially complicated and schools should follow the principles as set out in Keeping children safe in education. The UK Council for Internet Safety also provides the following guidance to support school staff and designated safeguarding leads: Sharing nudes and semi-nudes: advice for education settings working with children and young people.
- If a member of staff finds any image, data or file that they suspect might constitute a specified offence, then they must be delivered to the police as soon as is reasonably practicable.
- In exceptional circumstances members of staff may dispose of the image or data if there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files, the member of staff must have regard to the following guidance issued by the Secretary of State
    - In determining whether there is a 'good reason' to examine the data or files, the member of staff should reasonably suspect that the data or file on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.
    - In determining whether there is a 'good reason' to erase any data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable. If the data or files are not suspected to be evidence in relation to an offence, a member of staff may delete the data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves

Care of Confiscated Devices\

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices.

Audit / Monitoring / Reporting / Review

The Lead DSL will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files. These records will be reviewed by the Headteacher. The Behaviour Policy refers to our Search and Deletion Policy.
https://www.gov.uk/government/publications/searching-screening-and-confiscation

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and learners is, as always, at the forefront of our policy and practice.

Policy Statements

The school 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 HMFA are aware of the safeguarding risks associalted with AI. There is a rise in 'deepfake' AI pornography, and we will ensure that staff are trained on this issue.

- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR.
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The school will ensure that when AI is used, it will not 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.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The SchoolPro DPO service completes risk assessments of all AI systems in use and assists with the creation of DPIAs. The HMFA assess their potential impact on staff, pupils and the school's systems and procedures, creating an AI approved list. Staff must only use AI tools that appear on the approved list.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.

- The school will support parents and carers in their understanding of the use of AI in the school via the sharing of the Artificial Intelligence (AI) Policy on the school and/or HMFA websites and other handouts.
- AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI.
- Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Code of Conduct.

Any use of artificial intelligence should be carried out in accordance with our Artificial Intelligence (AI) policy. It also contains a list of HMFA approved AI tools.

7. Acceptable use

The HMFA has defined what it regards as acceptable/unacceptable use, and this is shown in the tables below.

7.1 Acceptable use agreements

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.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
Users shall not undertake activities that might	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is					X

be classed as cyber-crime under the Computer Misuse Act (1990)	not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information here					
Users shall not undertake activities that are not illegal but are classed as unacceptab	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	
	Promotion of any kind of discrimination				X	

le in school policies:	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright and intellectual property (including through the use of AI services)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

-
-

Consideration should be given for the following activities when undertaken for non-educational purposes: Schools may wish to add further activities to this list.	**Staff and other adults**				**Pupils**			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming			X					X
Online shopping/commerce				X	X			

File sharing				X				X
Social media			X	X				
Messaging/chat			X					X
Entertainment streaming e.g. Netflix, Disney+				X	X			
Use of video broadcasting, e.g. YouTube, Vimeo		X			X			
Mobile phones may be brought to school		X						
Use of mobile phones in social time at school			X					
Taking photos on mobile phones/cameras				X				
Use of other personal devices, e.g. tablets, laptops				X				X
Use of personal e-mail in school or on HMFA network/wi-fi	X				X			
Use of school e-mail for personal e-mails	X				X			
Use of AI services that have not been approved by school	X				X			

When using communication technologies, the HMFA considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the HMFA
- any digital communication between staff and pupils or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the HMFA and its community
- users should immediately report to a nominated person – in accordance with the HMFA policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only HMFA/school e-mail addresses should be used to identify members of staff and pupils.

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

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

More information is set out in the acceptable use agreements in appendices 1 to 3.

7.2 Reporting and responding

The HMFA will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school and HMFA) which will need intervention. The HMFA will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, IT Director and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), **the incident must be escalated through the agreed school safeguarding procedures, this may include**
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming

    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority / MAT
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss
- Where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority / MAT (as relevant)
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged on My Concern. Behaviour Logs are also completed on Arbor MIS where relevant.
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant).
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - the HMFA SLT for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    - staff, through regular briefings
    - learners, through assemblies/lessons
    - parents/carers, through newsletters, school social media, website
    - governors, through regular safeguarding updates
    - local authority/external agencies, as relevant *(The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of*

the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour"

The HMFA will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

7.3 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:

7.4 Responding to Pupil Actions

Incidents	Refer to class teacher/tutor	Refer to Head of Department / Principal Teacher / Deputy Head	Refer to Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).	X	X	X	X	X	X	X	X	X
Attempting to access or accessing the HMFA network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	X	X	X	X	X	X	X		X

Corrupting or destroying the data of other users.	X	X	X	X	X	X	X	X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X	X
Unauthorised downloading or uploading of files or use of file sharing.	X	X	X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system.	X	X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X		X	X			
Deliberately accessing or trying to access offensive or pornographic material.	X	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X	X	X		X	X	X	X	X
Unauthorised use of digital devices (including taking images)	X							X	X
Unauthorised use of online services	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	X		X	X
Continued infringements of the above, following previous warnings or sanctions.	X	X	X	X	X	X	X		X

7.5 Responding to Staff Act

Incidents	Refer to line manager	Refer to Headteacher / Principal	Refer to local authority/MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X				
Actions which breach data protection or		X	X		X	X	X	X

network / cyber-security rules.								
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system.		X	X		X	X	X	X
Unauthorised downloading or uploading of files or file sharing	X	X	X		X	X		
Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems)		X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	X	X			X	X		
Sending an e-mail, text or message that is regarded as offensive, harassment		X	X		X	X	X	X

or of a bullying nature								
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	X	X	X			X		
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X	X	X			X		
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X	X			X	X		
Actions which could compromise the 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	X
Failing to report incidents whether caused by deliberate or accidental actions		X	X			X		
Continued infringements of the above, following previous warnings or sanctions.		X	X			X	X	X

8. Technology

The HMFA is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

8.1 Filtering & Monitoring

The filtering and monitoring provision at HMFA schools is agreed by senior leaders, governors and the IT Service Provider. It is reviewed annually and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider or IT support provider will have technical responsibility.

8.2 Filtering

The DfE Technical Standards for Schools and Colleges states:

"Schools and colleges have a statutory responsibility to keep children and young people safe online as well as offline. Governing bodies and proprietors should make sure their school or college has appropriate filtering and monitoring systems in place, as detailed in the statutory guidance, Keeping children safe in education .

Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video.

The SLT and a governor, are responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties are clearly defined**.**

It is important that all staff and governors understand what filtering and monitoring is, and that it is in place to prevent children accessing inappropriate and harmful content online while pupils are in school. The HMFA see this as a clear safeguarding and welfare concern and not just a matter for the IT team. The DSL should take lead responsibility for understanding the filtering and monitoring systems in place in each school and it should be covered in the safeguarding policy as well in the safeguarding and child protection training which all staff receive.

- the HMFA filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the HMFA manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering, the DfE's latest filtering and monitoring standards and cyber security standards for schools and colleges
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Filtering systems prevent users from accessing harmful or inappropriate content when using AI. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes (see Appendix for more details)

- the HMFA has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/pupils, etc.)
- younger pupils will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle
- filtering logs are regularly reviewed and alert the HMFA to breaches of the filtering policy, which are then acted upon
- where personal mobile devices have internet access through the HMFA network, content is managed in ways that are consistent with HMFA policy and practice
- access to content through non-browser services (e.g., apps and other mobile technologies) is managed in ways that are consistent with HMFA policy and practice.

If necessary, the HMFA will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

8.3 Monitoring

The HMFA has monitoring systems in place to protect the HMFA, systems and users:

- The HMFA monitors all network use across all its devices and services
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The HMFA follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and HMFA systems through the use of the appropriate blend of strategies strategy informed by the HMFA's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom) and use of Apple Classroom to monitor pupil use of iPads
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the HMFA of breaches to the filtering policy, allowing effective intervention.
- **The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff. It will also involve the responsible governor. The results of the review will be recorded and reported as relevant.**
- where possible, HMFA technical staff regularly monitor and record the activity of users on the HMFA technical systems
- The DSLs and SLT have access to monitoring systems and incidents are usually dealt with on the same day.

9. Technical Security

The HMFA technical systems will be managed in ways that ensure that the HMFA meets recommended technical requirements:

- All users will be provided with a username and password by the HMFA's IT Technician and has the ability to reset passwords
- All computers, email, laptops and HMFA owned iPads must have strong passwords. The passwords must not be shared, and staff are required have passwords that are at least 12 characters, include 3 random words, upper case and lower case, numbers and special characters.
- Passwords for the HMFA network/O365 can be reset by Jo Brace and IT Technicians e.g., used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- In good practice, the account is "locked out" following six successive incorrect log-on attempts.
- A multi-user account is available for visitors to the HMFA (e.g. supply teachers). This has been carefully controlled to give only the access to the system that is needed, and the username and password is given to users as required. The password is changed regularly
- Clearly defined permissions are in place within Active Directory/Entra AD & Sharepoint to determine HMFA-controlled access to areas of the network appropriate to their role
- Staff users have the facility to access all pupil work areas via their normal login. This is to enable monitoring of work and ICT activity by children. Some classes also have a group log-on and password. This is also useful in the situation where a pair or group of children have been working collaboratively and the child whose login was used is unexpectedly absent; the teacher can move the work in question to another child's work area. In this way it is not necessary for a child to login using another child's account
- Encryption software is installed on all staff laptops (where potentially sensitive data is stored and the machines are regularly taken off site)
- All USB memory sticks, and portable hard drives used by staff are encrypted. Encryption keys are stored on the server. Staff are encouraged to save to HMFA shared drives or their HMFA One Drive instead of using USB storage devices
- The administrator passwords for the HMFA ICT system, used by Computeam or John Finch) is also available to the Executive Headteacher and kept in a secure place
- Google Apps for Education/GSUITE passwords can be reset by the IT Director, the IT Technicians and 1 x admin staff at each HMFA school. Staff are given temporary passwords that must be reset on first login. Pupils' network passwords are reset by the HMFA IT Technicians
- School owned devices must not be used by family members at home
- Local install rights is not given to staff in order to prevent them from downloading executable files and installing programmes on HMFA Windows devices
- the use of personal removable media (e.g. memory sticks/CDs/DVDs) should not be used by users on HMFA school devices systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.
- All staff have completed the NCSC Cyber Security training
- Every school has signed up for the Police Cyber Alarm.
- Anti-virus software is installed on the HMFA network and school owned computers
- Multi-factor authentication is set on all O365 and critical IT systems
- All networks are backed up locally and to secure cloud-based storage. O365 is backed up using cloud to cloud secure back up. Back-ups are tested termly.
- HMFA schools use JAMF mobile device management to manage school owned iPads
- Where AI services are used for technical security, their effectiveness is regularly reviewed, updated and monitored for vulnerabilities e.g. HMFA Email Gateway Protection
- Where AI services are used, the school will work with suppliers to understand how these services are trained and will regularly review flagged incidents to ensure equality for all users e.g. avoiding bias.

9.1 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 HMFA schools by 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.

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.

See Acceptable Use Policy for guidance on use of mobile phones on HMFA schools' premises. Visitors (including parents) are requested not to use their phones whilst in the school and to switch them off.

Occasionally, the IT Director or IT technicians may need to use their mobile phones in the vicinity of children in order to report an IT issue to our IT support or to take photos of electronic equipment. They will ensure that no photos of pupils will be shared and the conversation will be brief. It is expected that apologies will be made to the pupils and staff in the room and an explanation of the purpose of the call will be explained.

9.2 Staff using work devices outside school

All staff members using personal devices will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time

- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT Director.

10. Social Media

The HMFA provides the following measures to ensure reasonable steps are in place to minimize risk of harm to pupils through:

- ensuring that personal information is not published
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk
- guidance for pupils, parents/carers.

HMFA staff should ensure that:

- no reference should be made in social media to pupils, parents/carers or HMFA staff
- they do not engage in online discussion on personal matters relating to members of the HMFA community
- personal opinions should not be attributed to the HMFA
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

When official HMFA social media accounts are established, there should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under HMFA disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the HMFA it must be made clear that the member of staff is not communicating on behalf of the HMFA with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the HMFA are outside the scope of this policy
- where excessive personal use of social media in an HMFA school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- the HMFA permits reasonable and appropriate access to personal social media sites during school hours.

Monitoring of public social media

- As part of active social media engagement, the HMFA may pro-actively monitor the Internet for public postings about the HMFA and its schools/settings
- the HMFA should effectively respond to social media comments made by others according to a defined policy or process
- when parents/carers express concerns about the HMFA school on social media we will urge them to make direct contact with the HMFA school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the HMFA complaints procedure.

HMFA use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the HMFA is unable to resolve support may be sought from the Professionals Online Safety Helpline.

11. Digital and video images

When a pupil/student joins the HMFA, 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.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

All photos shared on HMFA schools' websites and their social media links, will be appropriate and show pupils involved in educational activities.

In order to safeguard children and adults and to maintain privacy, cameras are expressly forbidden from being taken into the toilets by adults or children.

All adults, whether teachers, practitioners or volunteers at all HMFA schools/settings understand the difference between appropriate and inappropriate sharing of images.

All images are kept securely in compliance with the Data Protection Act 2018. At HMFA schools/settings events such as carol concerts, parents are allowed to photograph/video their children but are asked to refrain from sharing on social media any photographs/video which may contain children other than their own.

Sometimes the HMFA schools may have to ask that photographs are not taken at all. This is for confidential reasons when we need to protect individual children.

The HMFA will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the HMFA schools may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies. Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education
- when using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images e.g. the risks associated with sharing images that reveal the identity of others and their location
- staff/volunteers must be aware of those pupils whose images must not be taken/published. Those images should only be taken on HMFA devices. The personal devices of staff should not be used for such purposes
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at HMFA 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 pupils in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow HMFA policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that pupils are appropriately dressed
- pupils must not take, use, share, publish or distribute images of others without their permission
- pupils are taught the risks associated with sharing images that reveal the identity of others and their location, such as house number, street name or HMFA school
- photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with Online Safety Policy
- pupils' full names will not be used anywhere on a website, blog or in the credits of a video, particularly in association with photographs
- images will be securely stored in line with the HMFA retention policy
- pupils' work can only be published with the permission of the pupil and parents/carers.

12. Online Publishing

Our HMFA schools use the public facing websites of https://schoolname.hmfa.org.uk and https://hmfa.org.uk

Below is a list of all of the HMFA schools' websites: -

https://kingscaple.hmfa.org.uk

https://llangrove.hmfa.org.uk

https://lordscudamore.hmfa.org.uk

https://marden.hmfa.org.uk

https://stweonards.hmfa.org.uk

https://sutton.hmfa.org.uk

https://pencombe.hmfa.org.uk

Our websites are a key public-facing information portal for the HMFA community (both existing and prospective stakeholders) with a key reputational value. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content. Personal information should not be posted on the HMFA website and only official email addresses (provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).

Detailed calendars of Off-site events are not published on the HMFA or schools' websites.

Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:

- schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited, and material only used with permission. If in doubt, check with Jo Brace. There are many open-access libraries of high-quality public-domain images that can be used (e.g., pixabay.com for marketing materials – beware some adult content on this site)
- pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
- where pupils are undertaking PE/dance activities images, show respect & dignity for the pupils
- images are not able to be copied or downloaded from the websites.

The HMFA ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the HMFA community, through such publications.

Where pupil work, images or videos are published, their identities are protected, and full names are not published.

The HMFA public online publishing provides information about online safety e.g. publishing the HMFA's Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on each school's website.

The websites include an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.

13. Cloud Platforms

The 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.

14. Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The HMFA and each federated school:

- has a Data Protection Policy. See HMFA and school websites.
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest. All HMFA Schools use the SchoolPro Ltd DPO service.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the HMFA and each school looks after their data and what their rights are in a clear Privacy Notices (see HMFA and school websites)

- has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff
- ensures that where AI services are used, data privacy is prioritised. The SchoolPro DPO service conducts risk assessments of all AI services considered and adopted by HMFA.

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

15. Cyber Security

The DfE Cyber security standards for schools and colleges explains:

“Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- the school has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards
- the school will conduct a cyber risk assessment annually and review each term
- the school has reviewed the DfE Cyber security standards for schools and colleges and is working
- the school, (in partnership with their technology support partner), has identified the most critical parts of the school’s digital and technology services and sought assurance about their cyber security
- the school has an effective backup and restoration plan in place in the event of cyber attacks
- the school’s governance and IT policies reflect the importance of good cyber security
- staff and Governors receive training on the common cyber security threats and incidents that schools experience
- the school’s education programmes include cyber awareness for learners
- the school has a business continuity and incident management plan in place
- there are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

10. How the school will respond to issues of misuse

Where a pupil misuses the school’s ICT systems or internet, we will follow the procedures set out in our policies on Acceptable use and Behaviour.The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school’s ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

16. Training

16.1 Staff, 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.

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 child protection and safeguarding 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** **IT Director**
NCSC Cyber Security Training	**NCSC Staff training – for RPA insurance**	**Annual – Autumn Term** **On Induction**	**IT Director** **Head of School** **Deputy Headteachers** **Headteachers**
Annual Certificate in Cyber Security for Staff for Primary Schools & Academies	**National College**	**Biennial – Spring Term**	**IT Director** **Head of School** **Deputy Headteachers**
Annual Certificate in Data Protection & GDPR for Staff for	**National College**	**Biennial – Spring Term**	**IT Director** **DPO** **Head of School**

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

Annual Certificate in Cyber Security for Staff for Primary Schools & Academies	**National College**	**Biennial – Spring Term**	**IT Director** **CEO**
Annual Certificate in Data Protection & GDPR for Leaders for Primary Schools & Academies	**National College**	**Biennial – Spring Term** **On induction**	**IT Director** **DPO** **CEO**

Senior Leaders with Cyber Security & Online Safety role - IT Director, 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**
Filtering & Monitoring in line with KCSIE	National College	On induction	**Headteachers** **CEO**
NCSC Cyber Security Training	**NCSC Staff training – for RPA insurance**	**Annual – Autumn Term** **On Induction**	**IT Director** **Headteachers**
Annual Certificate in Cyber Security for Staff for Primary Schools & Academies	**National College**	**Biennial – Spring Term**	**IT Director** **Headteachers**
Annual Certificate in Data Protection & GDPR for Staff for Primary Schools & Academies	**National College**	**Biennial – Spring Term** **On induction**	**IT Director** **DPO** **CEO**

DSLs			
Training Course title	**Provider**	**Frequency**	**Monitored by**
Annual Advanced Certificate in Online Safety for DSLs &	**National College**	**Annual**	**Headteachers** **IT Director**

Deputy DSLs for Primary Schools & Academies		**On Induction**	
NCSC Cyber Security Training	**NCSC Staff training – for RPA insurance**	**Annual – Autumn Term** **On Induction**	**IT Director** **Headteachers**
Annual Certificate in Cyber Security for Staff for Primary Schools & Academies	**National College**	**Biennial – Spring Term**	**IT Director** **Headteachers**
Annual Certificate in Data Protection & GDPR for Staff for Primary Schools & Academies	**National College**	**Biennial – Spring Term** **On induction**	**IT Director & DPO** **Headteachers**
Filtering & Monitoring bespoke to school/academy	**IT Support company (Entrust or JFC)** **IT Director**	**When changes are made to filtering & monitoring systems** **On induction**	**IT Director** **Headteachers** **CEO**

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** **IT Director** **Clerk to Governors** **Lead Governance Professional (LGP)**
NCSC Cyber Security Training	**NCSC Staff training – for RPA insurance**	**Annual – Autumn Term** **On Induction**	**IT Director** **Clerk to Governors** **LGP** **CEO**
Annual Certificate in Cyber Security for Governors for Primary Schools & Academies	**National College**	**Biennial – Spring Term**	**IT Director** **Clerk to Governors** **LGP** **CEO**
Annual Certificate in Data Protection &	**National College**	**Biennial – Spring Term**	**IT Director** **DPO**

GDPR for Governors for Primary Schools & Academies		**On induction**	**Clerk to Governors** **LGP** **CEO**

16.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

17. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the CEO, IT Director and the lead DSL. At every review, the policy will be shared with the people with a governing role. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

This Online Safety Policy was approved by the *HMFA Trustees on:*	
The implementation of this Online Safety Policy will be monitored by:	*JBrace & HMFA DSLs*
Monitoring will take place at regular intervals:	*Annually*
The *HMFA Trustees &/or LABs* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*September 2026*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	**https://westmidlands.procedures.org.uk** **The Herefordshire LADO is Terry Pilliner** LADO@herefordshire.gov.uk or tpilliner@herefordshire.gov.uk Tel: 01432 261739 **MASH (Multi Agency Safeguarding Hub)** Weekdays - 01432 260800 Out of hours - 01905 768020 **Police** – **999** (emergencies) **101** contactus@westmercia.police.uk **CEOP (Child Exploitation and Online Protection)** https://www.ceop.police.uk/Safety-Centre/ **Professionals Online Safety Helpline** Tel: 0344 381 4772 helpline@saferinternet.org.uk **Report Harmful Content** https://reportharmfulcontent.com/

18. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- RPA Cyber Response Plans
- Business Continuity Plan

Appendix

The appendices are as follows:

A1 - Pupil Acceptable Use Agreement (AUP)– (Foundation/KS1)
A2 - Pupil Acceptable Use Agreement (AUP) – KS2
A3 - Parent/Carer Acceptable Use Agreement/ Permissions Form & Photos and Videos Permissions

A4 - Staff (and Volunteer) Acceptable Use Policy Agreement (AUP)
A5 - Visitor Users Acceptable Use Agreement (AUP)
A6 - Training Needs Audit Log
A7 - Responding to incidents of misuse – flow chart
A8 – Record of reviewing devices/internet sites (responding to incidents of misuse)

Credits

Elements of this policy have been taken from SWGfL and The Key templates.

Appendix 1 – Acceptable Use Policy Agreement - EYFS/KS1 pupils

Our Technology Rules

I will follow these rules to use computers, tablets and the internet safely 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.

These rules help us all stay safe and have fun using computers and tablets at school!

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

Appendix 2 – KS2 Pupil AUP

HMFA HEREFORDSHIRE MARCHES FEDERATION OF ACADEMIES

Acceptable Use Agreement

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

Keeping Safe Online

The school will check how I use devices and the internet 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 Computers and the Internet Sensibly

I will only use devices, apps and sites that I am allowed to, and will check if I am unsure.

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 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.

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.

~~~~~~~~~~~~~~~~~~~~~

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult:

at school , my trusted adults are_____

Outside school, my trusted adults are_____

I know I can also get in touch with Childline

Name:		Date:
Y3: Signed		
Y4: Signed		
Y5: Signed		
Y6: Signed		
~~~~~~~~~~~~~~~~~~~~~

Appendix 3 – Pupil & Parent/carer AUP

HMFA HEREFORDSHIRE MARCHES FEDERATION OF ACADEMIES

Acceptable Use Policy Agreement and Permission Forms – Pupil & Parent/Carer

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

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 / academy 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 pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy

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.

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose or access any inappropriate websites
- Use them without a teacher being present, or without a teacher's permission
- Access social networking, chat rooms or blog sites (unless my teacher has expressly allowed this as part of a learning activity)
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone
- without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate
- material or use inappropriate language when communicating online
- I agree that the school will monitor the websites I visit.
- I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
- I will always use the school's ICT systems and internet responsibly.
- If I bring a personal mobile phone or other personal electronic device into school: I will not use it during lessons and I will hand it in to the school office

Name of Pupil: **Signed (pupil):**	**Date:**

Parent**/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

I understand that the school will teach my child online safety and my child will sign the AUP forms annually. (See Online Safety Policy - appendices 1 & 2).

Signed (parent/carer):	Date:

Permission to publish my child's work (including on the internet)

It is our school's policy, from time to time, to publish the work of pupils by way of celebration. This includes on the internet; via the school website, school blog, in a book /magazine or in the Learning Platform.

As the parent / carer of the above child I give my permission for this activity.

Signed (parent/carer):	Date:

Use of cloud based systems – permission form

Some of the apps we use make use of cloud storage. The school strives for compliance with the data protection laws in all respects here. We use Google Apps for Education to enable your child to create, edit and share files and websites for school related projects and communicate via email with other pupils and

members of staff. These services are entirely online and available 24/7 from any internet-connected computer.
We ask for your consent to your child making use of **Google Apps for Education.**

Signed (parent/carer):	Date:

Our pupils also save work to a cloud based online portfolios called Seesaw. This is used to teach safe collaborative blogging and peer-assessment. It is also a fun way to save work from our iPads.

We ask for your consent to your child making use of **Seesaw.**

Signed (parent/carer):	Date:

Photos/videos taken by parents/carers

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 Data Protection laws). 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 students / pupils in digital / video images.
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.

Signed (parent/carer):	Date:

Photo and Video Consent Form

During your child's time at our school, we may wish to take photographs or videos of your child. These photographs and videos may be used for displays, promotional material, our website, our newsletter, social media, training materials and in the newspaper. We believe that it is important to promote the school and celebrate the educational achievements of our children; however, we also recognise that it is important that you have control and choices about how we use photographs and videos.

When we do take photographs or videos, we will review them; any images that may cause embarrassment or distress will not be used nor will images associated with material on issues that are sensitive.

When filming or photography is carried out by the media, children will only be named if there is a reason to do so (e.g. they have won a prize), and home addresses will never be given out.

Before taking any photographs of your child for these purposes, we need your consent. This is necessary to comply with data protection laws. Without your consent, we will not be able to use your child's photographs or videos. Although we are requesting your consent to use photographs and videos for the purposes below, we do not require your consent to use them for purely educational purposes e.g. as part of class-based learning.

We would be grateful if you could confirm your preferences by ticking the appropriate boxes below:-

	Please tick	Yes	No

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

If you give consent for photographs or videos to be used as described above, you may withdraw your consent at any time. If you decide to withdraw your consent, please contact the school office so that we can update our records accordingly.

When you provide your consent, this will remain valid for the period of time that your child attends the school and for 12 months after your child leaves the school (unless you chose to withdraw your consent earlier). Historic photographs will, however, remain on our website and HMFA website, on social media feeds or, in some cases, when forming part of decorative displays situated inside the school building.

Child's name: _____	Class: _____
Signed (parent/carer): _____	Date: _____

Appendix 4 - Staff AUP

HMFA HEREFORDSHIRE MARCHES FEDERATION OF ACADEMIES

Acceptable Use Policy Agreement - Staff, teaching student, governors & volunteers

Background

We ask all children, young people and adults involved in the life of HMFA schools & academies to sign an Acceptable Use* Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and I will be asked to sign it upon entry to the school and every time changes are made.

Why do we need an AUP?

All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy 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.

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

What am I agreeing to?

1. I have read and understood HMFA Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult).
3. I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education / UK GDPR)
4. I will take a zero-tolerance approach to all forms of child-on-child abuse, not dismissing it as banter - this includes bullying, sexual violence and harassment - and maintain an attitude of 'it could happen here'
5. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language
6. I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with the PSHE curriculum, as well as safeguarding considerations when supporting pupils remotely.
7. I will be professional in my communications and actions when using digital technologies and systems:
    - 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 not engage in any online activity that may compromise my professional responsibilities.

8. I understand that in any periods of home learning, school closures or potential lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.
9. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
10. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:
    - not sharing other's images or details without permission
    - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
11. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the HMFA Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.
12. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy If I am not sure if I am allowed to do something in or related to school, I will not do it and seek guidance from the DSL.
13. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either. More guidance on this point can be found in this Online Reputation guidance for schools and in school or HMFA social media policy/guidance.
14. I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify the IT Director or my Headteacher if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.
15. I will not store school-related data on personal devices, storage or cloud platforms. USB keys, if allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
16. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
17. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.
18. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
19. I understand that breach of this AUP and/or of the HMFA Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.
20. 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
21. 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

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

To be completed by Headteacher, Head of School, Director of IT, HR Manager

I approve this user to be allocated credentials for school systems as relevant to their role.

Systems: _____

Additional permissions (e.g. admin) _____

Signature: _____

Name: _____

Role: _____

Date: _____

Appendix 5 - Visitor AUP

Acceptable Use Policy Agreement for Visitor/Community user

Background
We ask all children, young people and adults involved in the life of any HMFA school or academy to sign an Acceptable Use* Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media. Visitors and contractors are asked to sign this document before they are allowed access to the school or its pupils. Many of these rules are common sense – if you are in any doubt or have questions, please ask.

Further details of our approach to online safety can be found in the overall school Online Safety Policy.
If I have any questions during my visit, I will ask the person accompanying me (if appropriate).
If questions arise after my visit, I will ask – Jo Brace (IT Director) IT@hmfa.org.uk

What am I agreeing to?

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 will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
- I will leave my phone in my pocket and turned off. Under no circumstances will I use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils/students. If required (e.g., to take photos of equipment or buildings), I will have the prior permission of the headteacher (this may be delegated to other staff) and it will be done in the presence of a member staff.
- If I am given access to school-owned devices, networks, cloud platforms or other technology:
    - I will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use
    - I will not attempt to access any pupil / staff / general school data unless expressly instructed to do so as part of my role
    - I will not attempt to make contact with any pupils/students or to gain any contact details under any circumstances
    - I will protect my username/password and notify the school of any concerns
    - I will abide by the terms of the school Data Protection Policy and GDPR protections

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. This form will be stored in the school office/HMFA Network for a minimum of 6 months after I have left the school.

~~~~~~~~~~~~~~~~~~~~~~

To be completed by the visitor/contractor:

I have read, understood and agreed to this policy.

Signature/s: _____

Name: _____

Organisation: _____

Visiting / accompanied by: _____

Date / time: _____

To be completed by the school (only when exceptions apply):

Exceptions to the above policy: _____

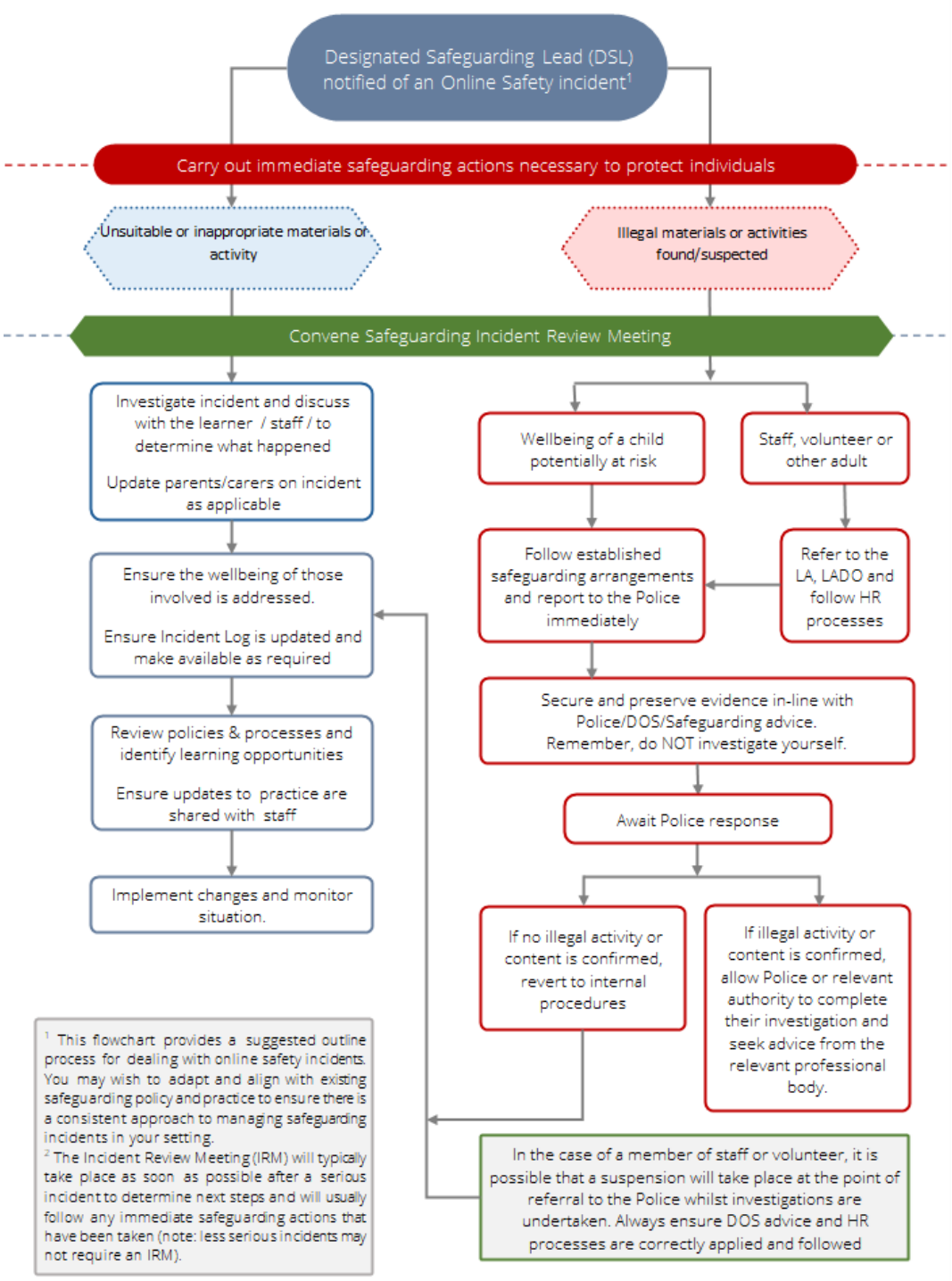
Name / role / date / time: _____

Appendix 6: 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, 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?	

Appendix 7: incident reporting flowchart



Appendix 8 - Record of reviewing websites

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
