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

Online Safety Policy

September 2024

Date Approved by The Board of Trustees	26/09/24
Effective period	**1/09/24 – 31/08/25**
Reviewer	**J Brace**
Date of Review	**18/09/2024**
Next Review Due	**1/09/2025**

Next review date: September 2025

Co-ordinator – J Brace

Contents

IntroductionScope of the Online Safety Policy 4
1. Policy development, monitoring and review 4
2. Schedule for development, monitoring and review 5
3. Process for monitoring the impact of the Online Safety Policy 6
4. Policy and leadership 6
Responsibilities 6
Headteacher and senior leaders 6
Governors 6
Online Safety Lead 7
Designated Safeguarding Lead (DSL) 7
Curriculum Leads 8
Teaching and support staff 8
Network manager/technical staff 8
Pupils 9
Parents and carers 9
Community users 10
Online Safety Group 10
Professional Standards 10
Policy 11
Online Safety Policy 11
Acceptable use 11
The HMFA has defined what it regards as acceptable/unacceptable use, and this is shown in the tables below. 11
Acceptable use agreements 11
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: 11
User actions 12
Reporting and responding 14
Responding to Pupil Actions 17
Sexting – sharing nudes and semi-nudes 17
Upskirting 18
Bullying 18
Artificial Intelligence 18
Sexual violence and harassment 19
Misuse of school technology (devices, systems, networks or platforms) 19
Responding to Staff Actions 21
Incidents 21
Electronic Devices - Searching & Deletion Policy 21
Responsibilities 22

Training/Awareness 22
Our Search Policy 22
Screening 22
Search: 22
Electronic devices 23
Care of Confiscated Devices 24
Audit / Monitoring / Reporting / Review 25
Online Safety Education Programme 25
Contribution of Pupils 25
Staff, Volunteers and Governor Training 26
Families 30
Adults and Agencies 31
Technology 31
Filtering 31
Monitoring 32
Technical Security 32
Mobile technologies 34
Use of Mobile Technologies (iPads, laptops, wearables & phones etc) 34
Pupil Use of Mobile Phones 34
Staff Use of Mobile Phones and Personal Cameras 35
Mobile Phones and After School Care 35
iPads, Laptops & Chromebooks– HMFA Owned 35
Pupil Use of HMFA Owned iPads & Chromebooks 36
Home Learning devices 36
Social media 37
Personal use 37
Monitoring of public social media 38
Digital and video images 38
Online Publishing 39
Cloud Platforms 41
Data Protection 42
Outcomes 42
Appendix 43

Introduction Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of HMFA (Herefordshire Marches Federation of Academies) to safeguard members of our HMFA community online in accordance with statutory guidance and best practice. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

This Online Safety Policy applies to all members of the HMFA community (including staff, pupils, volunteers, parents and carers, visitors, community users) who have access to and are users of HMFA digital systems, both in and out of the HMFA. It also applies to the use of personal digital technology on the HMFA site (where allowed).

HMFA will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of HMFA.

1. Policy development, monitoring and review

This Online Safety Policy has been developed by the *Online Safety Group* made up of:

- headteacher/senior leaders
- online safety lead
- staff – including teachers/support staff/technical staff
- governors
- parents and carers
- community users

Consultation with the whole HMFA community has taken place through a range of formal and informal meetings.

2. Schedule for development, monitoring and review

This Online Safety Policy was approved by the *HMFA Trustees on:*	*26/09/24*
The implementation of this Online Safety Policy will be monitored by:	*J Brace & 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 2025*
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/

3. Process for monitoring the impact of the Online Safety Policy

The HMFA will monitor the impact of the policy using:

- logs of reported incidents
- monitoring logs of internet activity (including sites visited)
- internal monitoring data for network activity
- surveys/questionnaires of:
    - pupils
    - parents and carers
    - staff.

4. Policy and leadership

Responsibilities

To ensure the online safeguarding of members of our HMFA community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the HMFA.

Headteacher and senior leaders

- The headteachers have a duty of care for ensuring the safety (including online safety) of members of the HMFA community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead
- The headteachers and Safeguarding Manager are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[1]
- The headteachers are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant
- The headteachers will ensure that there is a system in place to allow for monitoring and support of those in HMFA who carry out the internal online safety monitoring role
- The headteacher will receive regular monitoring reports from the Online Safety Lead.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in HMFAs and Colleges – questions from the Governing Body".

This review will be carried out by the HMFA Trustees whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

[1] See flow chart on dealing with online safety incidents in 'Responding to incidents of misuse' and relevant local authority/MAT/ HR/other relevant body disciplinary procedures.

- regular meetings with the Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g., online safety education provision and staff training is taking place as intended)
- reporting to relevant governors group/meeting
- membership of the HMFA Online Safety Group
- occasional review of the filtering change control logs and the monitoring of filtering logs (where possible).

The HMFA Trustees or governing body will also support the HMFA in encouraging parents/carers and the wider community to become engaged in online safety activities.

Online Safety Lead

Mrs J Brace is the Online Safety Lead and will:

- lead the Online Safety Group
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), where these roles are not combined
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the HMFA online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the HMFA and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/governors/parents/carers/pupils
- liaise with (HMFA/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team.
- liaises with the local authority/MAT/relevant body.

Designated Safeguarding Lead (DSL)

Jan McColl is Safeguarding Manager/ HMFA Designated Safeguarding Lead is regularly trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- Filtering and monitoring reports
- potential or actual incidents of grooming
- online bullying.

Curriculum Leads

Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme e.g. ProjectEVOLVE and Kapow Computing.

This will be provided through:

- PSHE and SRE programmes
- Computing Schemes of work
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

HMFA staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current HMFA Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to the **DSL** using MyConcern for investigation/action, in line with the HMFA safeguarding procedures
- all digital communications with pupils and parents/carers should be on a professional level and only carried out using official HMFA systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure pupils understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Network manager/technical staff

The network manager/technical staff are:-
IT Peritech Technicians at Entrust Education Technologies 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 CofE School & Clehonger 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.

Pupils

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the HMFA's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The HMFA will take every opportunity to help parents and carers understand these issues through:

- publishing the HMFA Online Safety Policy on the school website
- providing them with a copy of the pupils' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the HMFA
- seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix)
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the HMFA in:

- reinforcing the online safety messages provided to pupils in school
- the use of their children's personal devices in the HMFA schools (where this is allowed).

Community users

Community users who access HMFA systems/website/learning platform as part of the wider HMFA provision will be expected to sign a community user AUA before being provided with access to HMFA systems.

The HMFA encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

Online Safety Group

The Online Safety Group has the following members:

- Online Safety Lead - Jo Brace (Director of IT)
- Jan McColl (Safeguarding Manager, Lord Scudamore Academy LAC member
- IT Peritech Technicians at Entrust Education Technologies who support Lord Scudamore Academy, Kings Caple Primary Academy, Sutton Primary Academy, St Weonards Academy & Llangrove CE Academy
- IT Technicians at John Finch Computing Ltd who support Marden Primary Academy, Pencombe CofE School & Clehonger CE School
- The Heads of Schools and /or DSLs at each school
- The HMFA/Pupil Council & Digital Leaders at each school will be invited to review the HMFA Online Safety scheme of work and all of the pupil Acceptable Use Policies annually.
- Staff will be informed of any updates or amendments to the Online Safety policy.

Members of the Online Safety Group will assist the Online Safety Lead with:

- the production/review/monitoring of the HMFA Online Safety Policy/documents
- the production/review/monitoring of the HMFA filtering policy and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of pupils to staff awareness, emerging trends and the HMFA online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

An Online Safety Group terms of reference template can be found in the appendices.

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of HMFA life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the HMFA and wider community, using officially sanctioned HMFA mechanisms.

Policy

Online Safety Policy

The HMFA Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the HMFA and how they should use this understanding to help safeguard pupils in the digital world
- describes how the HMFA will help prepare pupils to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and saved to the HMFA network/Sharepoint – HMFA Common – Policies and via email
- is published on the school websites.

Acceptable use

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

Acceptable use agreements

An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users. In most HMFA schools they are signed or acknowledged by their staff as part of their conditions of employment. Some may also require pupils and parents/carers to sign them, though it is more important for these to be understood and followed rather than just signed. There is a range of acceptable use agreements in the appendices.

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. HMFAs 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 be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to HMFA 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)					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in HMFA policies:	Accessing inappropriate material/activities online in a HMFA setting including pornography, gambling, drugs. (Informed by the HMFA's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using HMFA systems to run a private business				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the HMFA				X	
	Infringing copyright				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 HMFA or brings the HMFA into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes: HMFAs 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					
File sharing				X				
Social media			X	X				
Messaging/chat			X					
Entertainment streaming e.g. Netflix, Disney+				X				
Use of personal e-mail in school or on HMFA network/wi-fi	X				X			
Use of HMFA e-mail for personal e-mails	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.

Reporting and responding

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

- there are clear reporting routes which are understood and followed by all members of the HMFA community which are consistent with the HMFA safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. Jo Brace will set up the use of online/anonymous reporting systems, which can be used by all members of the HMFA community on the HMFA website.
- all members of the HMFA 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, Online Safety Lead 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 HMFA safeguarding procedures
- 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 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 pupils 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
- 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
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    - staff, through regular briefings
    - pupils, through assemblies/lessons
    - parents/carers, through newsletters, HMFA social media, website
    - governors, through regular safeguarding updates
    - local authority/external agencies, as relevant
    - The HMFA will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
If staff/volunteer or pupil, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes
Monitor situation
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.
Illegal materials or activities found or suspected
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

HMFA actions

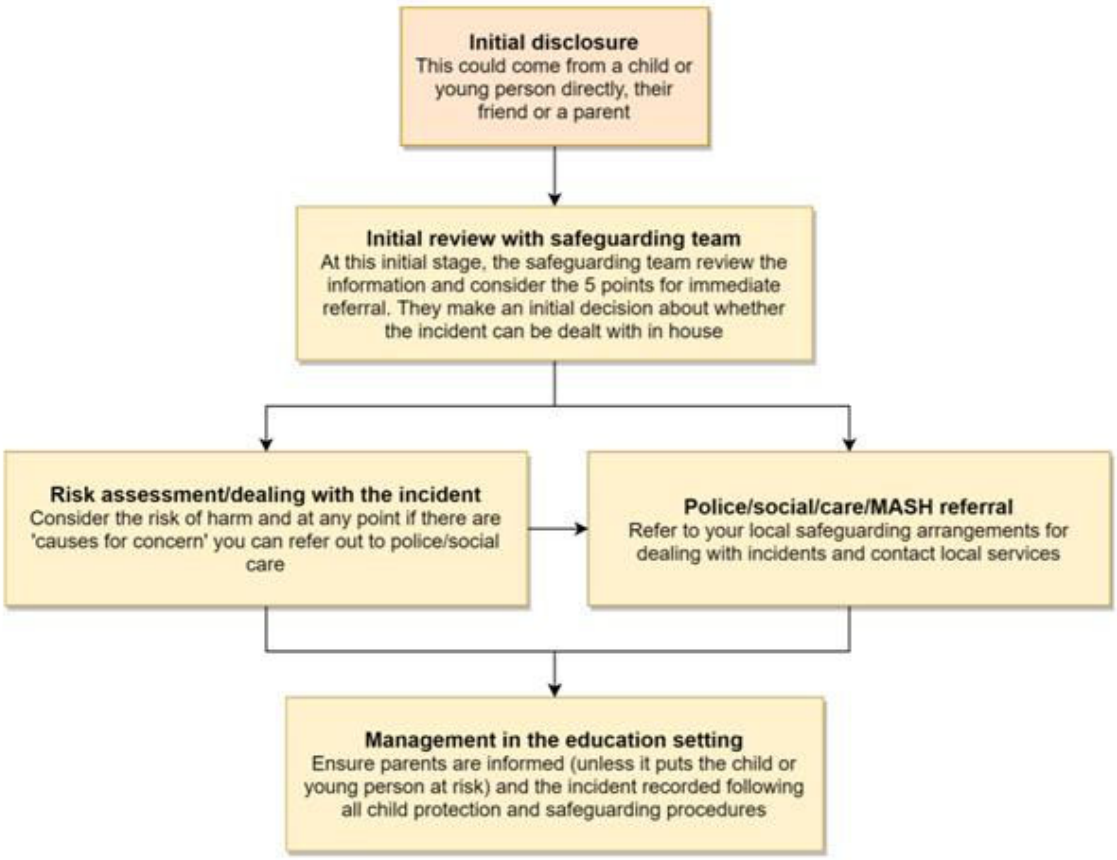
It is more likely that the HMFA will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the HMFA community are aware that incidents have been dealt with.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

Responding to Pupil Actions

Sexting – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.



The school DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.

***Consider the 5 points for immediate referral at initial review:**

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involve sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.
The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child-on-child abuse pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Artificial Intelligence

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

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

HMFA will treat any use of AI to bully pupils in line with our Anti-bullying and Behaviour policies.

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

Sexual violence and harassment

DfE guidance on sexual violence and harassment has now been incorporated into Keeping Children Safe in Education and is no longer a document in its own right. It would be useful for all staff to be aware of this updated guidance: Part 5 covers the immediate response to a report, providing reassurance and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that the same applies for any home learning that may take place in future periods of absence/ closure/quarantine etc.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Incidents	Refer to class teacher/tutor	Refer to DSL	Refer to Headteacher	Refer to Police/Social Work	Refer to 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 pupil) or allowing others to access HMFA 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 HMFA'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 HMFA into disrepute or breach the integrity or the ethos of the HMFA.	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

Responding to Staff Actions

Staff need to know that if they are involved in any incident, including those detailed below could result in the Disciplinary procedure being instigated which has a number of sanctions, including dismissal. *The* HMFA Staff Code of Conduct policy does not specify every incident possible but it doesn't need to. Incidents fall into one of the categories listed in the Code. For example, 5.25 covers sharing concerns and recording incidents, but it just refers to 'incidents' and does not give specific examples; section 5.5 Propriety and Behaviour and/or 5.3 Power and Position of Trust also covers a number of the incidents listed but without being specific.

Incidents

- **Deliberately accessing or trying to access material that could be considered illegal** (see list in earlier section on unsuitable / inappropriate activities)
- Deliberate actions to breach data protection or network security rules
- Deliberately accessing or trying to access offensive or pornographic material
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Using proxy sites or other means to subvert the HMFA schools' filtering systems.
- Unauthorised downloading or uploading of files or file sharing
- Breaching copyright or licensing regulations.
- Allowing others to access HMFA networks by sharing username and passwords or attempting to access or accessing the HMFA networks using another person's account.
- Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature
- Using personal e-mail/social networking/messaging to carry out digital communications with pupils and parents/carers
- Inappropriate personal use of the digital technologies e.g. social media / personal e-mail
- Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner
- Actions which could compromise the staff member's professional standing
- Actions which could compromise the staff member's professional standing
- Failing to report incidents whether caused by deliberate or accidental actions
- Continued infringements of the above, following previous warnings or sanctions.

Electronic Devices - Searching & 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 Online Safety Coordinator 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.

See DFE Gov advise document – Searching, Screening and confiscation.

Online Safety Education Programme

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways: -

- A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and regularly taught in a variety of contexts
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Pupil need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g., PSHE; RSE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to pupils at different ages and abilities such as those with additional learning needs or those with English as an additional language
- pupils are helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside HMFA
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where pupils are allowed to freely search the internet, staff should be vigilant in supervising the pupils and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Contribution of Pupils

The HMFA acknowledges, learns from, and uses the skills and knowledge of pupils in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the

HMFA community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvas pupil feedback and opinion
- appointment of digital leaders/anti-bullying ambassadors/peer mentors
- the Online Safety Group has pupil representation
- pupils contribute to the online safety education programme e.g., peer education, digital leaders leading lessons for younger pupils, online safety campaigns
- pupils designing/updating acceptable use agreements
- contributing to online safety events with the wider HMFA community e.g., parents' evenings, family learning programmes etc.

Staff, Volunteers and Governor Training

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 Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g., UKSIC / SWGfL / MAT / LA / Entrust Education Technologies, 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 Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Teachers			
Training Course title	**Provider**	**Frequency & term**	**Monitored by**

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

Support Staff (Teaching Assistants, Lunchtime Supervisors, Site Staff incl. cleaners, Business & Admin role)			
Training Course title	**Provider**	**Frequency & term**	**Monitored by**
Annual Certificate in Online Safety for Support Staff for Primary Schools & Academies	**National College**	**Annual – Autumn** **On Induction**	**Head of school** **Deputy Headteachers** **Headteachers** **DSLs** **IT Director**
NCSC Cyber Security Training	**NCSC Staff training – for RPA insurance**	**Annual – Autumn** **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 & term**	**Monitored by**
Annual Advanced Certificate in Online Safety for SENCOs for Primary Schools & Academies	**National College**	**Annual – Autumn** **On Induction**	**CEO** **DSLs** **IT Director**
NCSC Cyber Security Training	**NCSC Staff training – for RPA insurance**	**Annual – Autumn** **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 & term**	**Monitored by**
Annual Certificate in Online Safety for Teaching Staff for Primary Schools & Academies	**National College**	**Annual – Autumn** **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** **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 & term**	**Monitored by**
Annual Advanced Certificate in Online Safety for DSLs & Deputy DSLs for Primary Schools & Academies	**National College**	**Annual – Autumn On Induction**	**Headteachers IT Director**
NCSC Cyber Security Training	**NCSC Staff training – for RPA insurance**	**Annual – Autumn 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 & term	Monitored by
Annual Certificate in Online Safety for Governors for Primary Schools & Academies	**National College**	**Annual – Autumn** **On Induction**	**Headteachers** **IT Director** **Clerk to Governors** **Lead Governance Professional (LGP)**
NCSC Cyber Security Training	**NCSC Staff training – for RPA insurance**	**Annual – Autumn** **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 & GDPR for Governors for Primary Schools & Academies	**National College**	**Biennial – Spring Term** **On induction**	**IT Director** **DPO** **Clerk to Governors** **LGP** **CEO**

Families

The HMFA 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 pupils 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 HMFAs in clusters and or the local authority/MAT.

Adults and Agencies

The HMFA will provide opportunities for local community groups and members of the wider community to gain from the HMFA's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards families and relatives.
- providing family learning courses in use of digital technologies and online safety
- the HMFA will provide online safety information via their website and social media for the wider community
- supporting community groups, e.g. HMFA early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision. We will support these groups with an online safety review using 360 Groups or 360 Early Years.

Technology

The HMFA is responsible for ensuring that the HMFA infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The HMFA ensures 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.

Filtering

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. 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.

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)
- 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.
- where possible, HMFA technical staff regularly monitor and record the activity of users on the HMFA technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to HMFA monitoring lead(s).

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 who will keep an up-to-date record of users and their usernames 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 & 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 Entrust Education or Edu-Tech) is also available to the Executive Headteacher and kept in a secure place
- Google Apps for Education/GSUITE passwords can be reset by the Head of HMFA and 1 x admin staff at each HMFA. At Lord Scudamore Academy, Jo Brace and Sian Holden can reset passwords. 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 sued 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.

Mobile technologies

The HMFA acceptable use agreements for staff, pupils, parents, and carers outline the expectations around the use of mobile technologies.

Use of Mobile Technologies (iPads, laptops, wearables & phones etc)

Personal mobile phones and mobile devices brought into HMFA are the responsibility of the device owner. The HMFA accepts no responsibility for the loss, theft or damage of personal mobile phones or mobile devices.

The HMFA allows:

	HMFA devices			**Personal devices**		
	HMFA owned for individual use	HMFA owned for multiple users	Authorised device[2]	Pupil owned	Staff owned	Visitor owned
Allowed in HMFA	**Yes**	**Yes**	**Yes**	Y5 & 6	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only				N/A	Yes	Yes
No network access				N/A		Yes

Pupil Use of Mobile Phones

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 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.

Authorised staff can search student's electronic devices if they have good reason to think that the device has been or could be used to cause harm, disrupt teaching or break HMFA rules. Any search will be carried out in line with the HMFA's Search Policy – Electronic Devices (p21 of this document).

2 Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

Staff Use of Mobile Phones and Personal Cameras

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.

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 cameras 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 Online Safety Lead (Jo Brace) may need to use their mobile phones in the vicinity of children in order to report an IT issue to our IT support. 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.

Mobile Phones and After School Care

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 should not use their own devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

Where staff are required to use a mobile phone for HMFA school duties – e.g. in case of emergency during off-site activities, or for contacting students or parents - then a school mobile phone will be provided. In an emergency where staff do not have access to a school device, they should use their own device and hide their own number (by dialing 141 first).

iPads, Laptops & Chromebooks– HMFA Owned

Staff Use

- Unique IDs (provided by the HMFA schools) are used on staff tablets (to avoid accidental data transfer to colleague's tablets). Necessary passwords are given to the member of staff
- Personal IDs (often with associated personal media collections, e.g. music from iTunes) are not to be used on HMFA owned devices

- Children may only have access to staff tablets if the teacher has set the iPad to Guided Access mode using the Accessibility features in Settings
- A passcode is used on dedicated staff tablets (ensuring appropriate encryption of the device). All data is removed from tablets before it is allocated to a different member of staff
- Individual teachers are responsible for ensuring that any data, apps, photographs etc stored on the iPad are appropriate and professional. This is particularly important when mirroring to interactive whiteboards / screens
- Members of staff must report immediately any loss or compromise of the device or data contained on it
- Our schools are moving towards using a mobile device management system (mdm) that will manage and track staff tablets
- Members of staff are encouraged to use devices on home Wi-Fi but are required to be vigilant as to possible security breaches with public Wi-Fi.

Pupil Use of HMFA Owned iPads & Chromebooks

- A growing number of iPads are available for children to use in all HMFA schools. The HMFA schools have also started purchasing chrome books for pupil use
- iPads are managed via a mobile device management (mdm) system at Lord Scudamore Academy, Kings Caple, Sutton, Llangrove, St Weonards , Marden and Pencombe CofE School
- At Clehonger, the iPads are managed locally using Apple Configurator on a school owned MacBook
- Age-appropriate apps are purchased via Apple HMFA Manager website and deployed with due regard to licensing and copyright
- Files are transferred to, from and between iPads using a variety of methods. The One Drive app is installed on all iPads and the HMFA schools' one drive accounts are logged into on all iPads. Children are not given the password. HMFA schools/settings are developing the use of Online Portfolios services (Tapestry EYFS and Seesaw (KS1 & KS2). In addition, all HMFA schools now have the Google Classroom Learning Platform with Google Drive set up according to DFE (Department for Education) guidelines. Pupils can also use Airdrop to share files with each other and their teacher
- We make use of cloud services in other carefully chosen apps
- Parents give their permission for this via the parents' AUP (Acceptable Use Policy) agreement and permissions form (see appendix 3). There is the option to withdraw consent at any time
- Chrome books are set up using the HMFA domain and restrictions have been added by Entrust following DFE guidance. All links and apps are set up using Google mdm.

Home Learning devices

- Some of our iPads & chrome books are being loaned to families if needed. These devices are set up with mobile device management. Pupils and parents must sign a loan agreement before they can be taken off site. A passcode is to be set on all of the pupil

iPads before they are allowed to go home and the pupil's first name and class to be added to the description in the Zuludesk/Jamf mdm
- Parents can add their home Wi-Fi credentials to the loan device. The devices have restrictions that prevent access to content that is inappropriate to the age of the child
- Apps cannot be installed by the parent or pupil. If a parent requires any advice or help with this, they must contact the school.

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.

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.

Online Publishing

Our HMFA schools use the public facing websites of https://schoolname.hmfa.org.uk) and https://hmfa.org.uk apart from Clehonger CE School.

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

https://clehongerschool.co.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.

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.

Data Protection

"GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in HMFA schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed to stand in the way** of promoting the welfare and protecting the safety of children."

All pupils, staff, governors, volunteers, contractors and parents are bound by each school's data protection policy and agreements, which can be found on the schools' websites.

The headteachers, SLT, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be always treated with the strictest confidentiality, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of ANYCOMMS / Egress to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, pupils; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to HMFA SLT leadership, Trustees and Governors
- parents/carers are informed of patterns of online safety incidents as part of the HMFA's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

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 - Community 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)
A9 - Online Safety Group Terms of Reference Template

Credits

Elements of this policy have been taken from SWGfL and LGFL Digisafe templates.

Appendix 1 – EYFS/KS1AUP

Acceptable Use Policy Agreement – EYFS/KS1 Pupils

I agree to keep these computer rules:

- I always tell an adult if I see something that upsets me on a computer.
- I ask an adult to help me if I am not sure what to do or if something goes wrong.
- I only do the things that an adult says are OK.
- I only use a computer when there is an adult around.
- I tell an adult if anyone that I don't know sends me a message or is mean to me.
- I make sure that everything I do on a computer is the best it can be.
- I am always nice about people and the things they have done at the computer.
- I take care of the computers and iPads.
- I don't change clothes or get dressed in front of a camera.
- I don't share personal information online.
- I know that if I break the rules I might not be allowed to use a computer/tablet

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

Appendix 2 – KS2 Pupil AUP

Acceptable Use Policy Agreement – KS2 Pupils

These statements can keep me and others safe and happy at school and home

1. ***I learn online*** – I use the school's internet, devices and logins for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.
2. ***I behave the same way on devices as face to face in the classroom, and so do my teachers*** **–** If I get asked to do anything that I would find strange in school, I will tell another teacher.
3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. ***I am creative online*** – As well as looking at things from other people on apps, sites and games, I also get creative to learn and make things, and I remember my Digital 5 A Day.
5. ***I am a friend online*** – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am not a bully*** – I know just calling something banter doesn't make it ok as it could become bullying. I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
7. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
8. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
9. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
10. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
11. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
12. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
13. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
14. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
15. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
16. ***I say no online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes

me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
17. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
18. ***I follow age rules*** – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
19. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
20. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
21. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
22. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
23. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
24. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult.

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

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		

LGFL - DigiSafe

Appendix 3 –

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

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 follow the guidance in the safeguarding and online-safety policies for reporting incidents: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handing incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.
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 RSHE curriculum, as well as safeguarding considerations when supporting pupils remotely.
7. During remote learning:
    - I will not behave any differently towards students compared to when I am in school. 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 not attempt to use a personal system or personal login for remote teaching or set up any system on behalf of the school without SLT approval.
    - I will not take secret recordings or screenshots of myself or pupils during live lessons.
    - I will conduct any video lessons in a professional environment as if I am in school. This means I will be correctly dressed and not in a bedroom / impossible to tell that it is a bedroom if this is unavoidable (e.g. even if the camera slips). The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background, I will do so.
    - I will log and report any issues for live lessons immediately to the Designated Safeguarding Lead (if by a child) or Headteacher/Principal (if by an adult). if anything inappropriate happens or anything which could be construed in this way. This is for my protection as well as that of pupils.
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 Jo Brace 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.

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 (Director of IT) IT@hmfa.org.uk

What am I agreeing to?

1. I understand that any activity on a school device or using school networks, platforms, internet and logins may be captured by one of the school's systems security, monitoring and filtering systems and/or viewed by an appropriate member of staff.
2. 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.
3. 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.
4. 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
5. I will not share any information about the school or members of its community that I gain as a result of my visit in any way or on any platform except where relevant to the purpose of my visit and agreed in advance with the school.
6. I will not reveal any new information on social media or in private which shows the school in a bad light or could be perceived to do so.
7. I will not do or say anything to undermine the positive online-safety messages that the school disseminates to pupils/students and will not give any advice on online-safety issues unless this is the purpose of my visit and this is pre-agreed by

the school. NB – if this is the case, the school will ask me to complete Annex A and consider Annex B of 'Using External Visitors to Support Online Safety' from the UK Council for Child Internet Safety (UKCIS).

8. I 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).
9. I will only use any technology during my visit, whether provided by the school or my personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to my visit and agreed in advance. I will not view material which is or could be perceived to be inappropriate for children or an educational setting.

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

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: _____

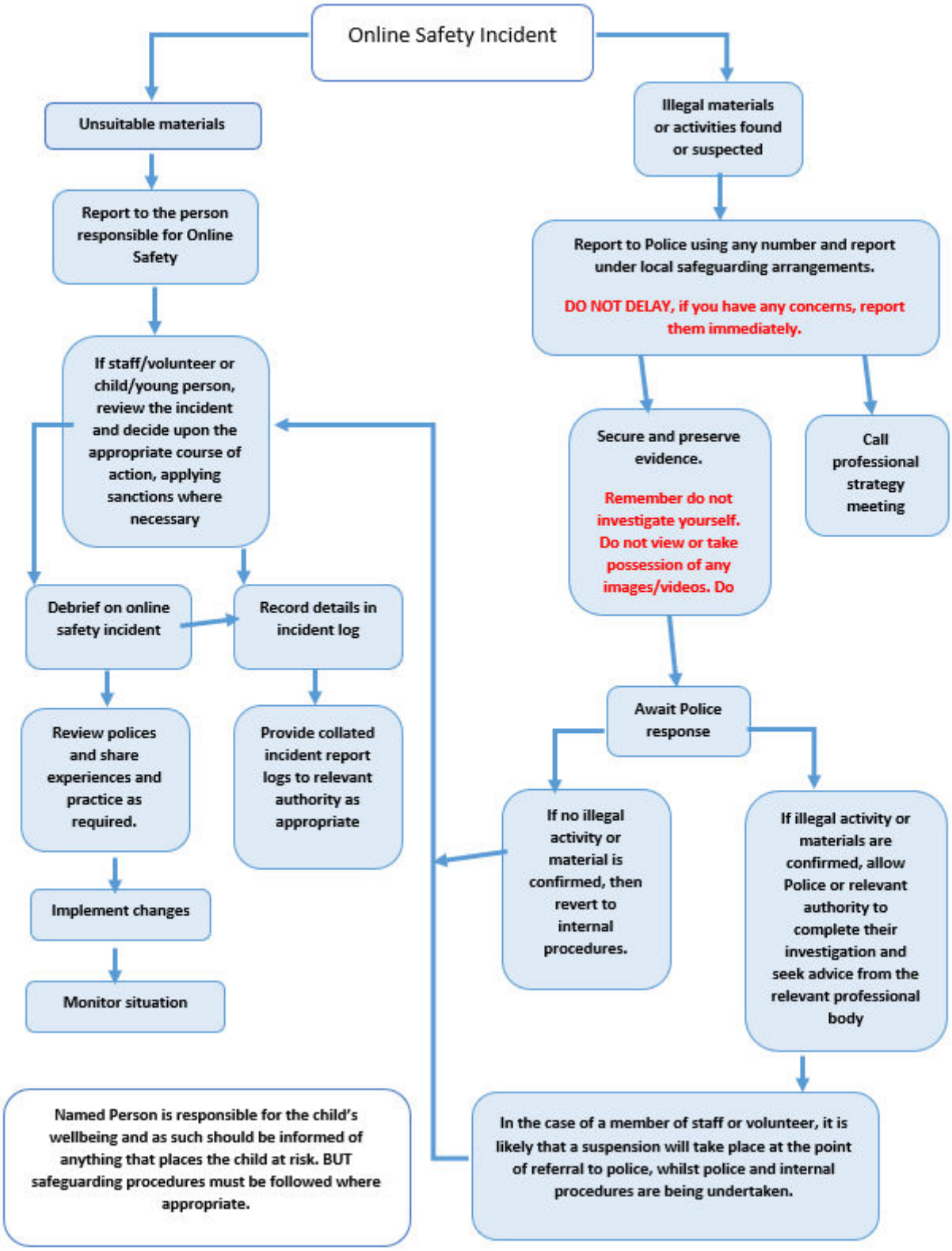
Name / role / date / time: _____
~~~~~~~~~~~~~~~~~~~~~~

Appendix 6 – Training Log – Online Safety, Parental Engagement & Digital Safeguarding

Group: Date:

Staff member name	Role/title	Relevant training in past year	Training need identified	Need to be met by	Cost	Review date

Appendix 7 - Incident Response Flowchart



Appendix 8 –

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

Appendix 9– Online Safety Reporting Log

Date	Time	Incident	Action taken		Incident reported by	Signed
			What?	By Whom?		