Online Safety Policy

October 2019

Next Review Due: July 2020

Co-ordinator – Mrs J Brace

Agreed by the board		
Signed by Chair of Directors:		*Date:*
CEO:		*Date:*
Review Date:	*July 2020*	

HMFA Online Safety Policy	
POLICY DATE: October 2019	REVIEW DATE: July 2020

Online Safety Policy

1. Introduction and Overview

The purpose of this policy is to:

- Outline the guiding principles for all members of the school community regarding the use of ICT.
- Safeguard and protect the students and staff and help them to work safely and responsibly with the internet and other communication technologies.
- Set clear expectations of behaviour relating to responsible use of the internet for educational, personal or recreational use.
- Establish clear reporting mechanisms to deal with online abuse such as bullying that are cross referenced with other school policies.
- Ensure that all members of the school community know that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Scope of the policy

This policy applies to all members of school community - staff, students, volunteers, parents and carers, visitors, community users - who have access to and are users of school's ICT systems.

The Education and Inspections Act 2006 empowers the Executive Headteacher and Heads of School to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school sites and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the schools, but is linked to membership of the schools. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the school's Behaviour Policy.

The HMFA schools 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 school.

This policy is read in conjunction with the following policies:

- HMFA Safeguarding & Child Protection Policy
- The school's Data Protection Policy
- HMFA IT Security Policy
- HMFA Behaviour Policy
- HMFA Anti-Bullying Policy
- HMFA Mobile Phone Policy
- HMFA Electronic Devices, Search and Deletion Policy
- HMFA Social Media Policy
- HMFA Staff Code of Conduct

Development, Monitoring and review

This HMFA Online Safety Policy has been developed by the Safeguarding and Online Safety group made up of:

- Head of School (DSL) for Kings Caple Primary Academy
- Head of School (DSL) for Sutton Primary Academy
- Head of School (DSL) for Llangrove CE Academy
- Head of School (DSL) for Canon Pyon CE Academy
- Head of School (DSL) for Clehonger CE Academy
- Head of School (DSL) for Pencombe CE Academy
- Head of School (DSL) for St Weonards Primary School
- Head of School (DSL) for Marden Primary Academy
- Director of IT
- IT Manager
- IT Technicians

Roles and Responsibilities

Directors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Directors receiving regular information about online safety incidents and monitoring reports. A member of the Directors has taken on the role of the

Communication of the policy

The policy will be communicated to the school community in the following ways:

- Displayed on the school websie, and available in the staffroom and classrooms.
- Included as part of the induction pack for new staff.
- Acceptable use Policy agreements discussed with and signed by pupils at the start of each year. These should be held in class transfer folders or in the front of pupils' Computing/ICT folders.
- Acceptable use Policy agreements to be issued to whole school community, usually on entry to the school.
- Staff Acceptable use agreements to be held in personnel files.

Responding to complaints

- The school will take all reasonable precautions to ensure online safety. However, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the academy nor HMFA can accept liability for material accessed, or any consequences of internet access.
- Staff and students are informed of the possible sanctions related to misuse of technology and these are outlined in the Behaviour Policy.
- Our online safety coordinator (Mrs Brace) is the first point of contact for any complaint. Any complaint about staff misuse will be referred to the Executive Headteacher.

- Complaints that relate to online bullying will be dealt with in line with our Anti-Bullying Policy. Complaints related to child protection are dealt with in line with the school child protection procedure.
- The Executive Headteachers, Heads of School and Safeguarding Director (DSLs) should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see Appendix 7 flow chart on dealing with online safety incidents – included in section 2.6 below and relevant Local Authority HR / disciplinary procedures)

Review and Monitoring

Online safety is integral to other school policies including the Computing Policy, Safeguarding & Child Protection Policy, Anti-Bullying Policy, Behaviour Policy, Mobile Phone Policy and HMFA Social Media Policy.

Jo Brace is the HMFA online safety coordinator and is responsible for writing, reviewing and updating the policy. The policy will be reviewed annually or more frequently in response to changing technology and online safety issues in the school.

This policy has been developed in consultation with the school's online safety committee and approved by the Senior Leadership Team and Board of Governors. Staff will be informed of any updates or amendments to it.

The Online Safety Committee is comprised of:-

Jo Brace (Director of IT)

Jan McColl (Safeguarding Manager, HMFA Director - Lord Scudamore Academy LAB member),

Sherry Morris-Davies (ICT Co-ordinator & Lord Scudamore Academy LAB member),

IT Peritech Technicians at IBS Schools - all HMFA schools apart from Marden Primary Academy, Pencombe CE Primary School & Clehonger CE Primary School),

The School/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.

2. Education and Curriculum

Pupils online safety curriculum

HMFA has a clear, progressive online safety education programme primarily as part of the Computing and PSHE curricula, but referenced in all areas of school life. It covers a range of skills and behaviours appropriate to students' ages and experience, including:

- Digital literacy.
- Acceptable online behaviour.
- Understanding of online risks.
- Privacy and security.
- Reporting concerns.

The HMFA federation will:

- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

- Remind students about their responsibilities using the Acceptable Use Agreement signed by every student.
- Ensure that staff model safe and responsible behaviour in their own use of technology during lessons.
- Ensure that staff and students understand issues around plagiarism and copyright/intellectual property rights; and understand how to critically assess the validity of the websites they use.
- Staff and governor training

The school will ensure that:

- Staff understand the requirements of the Data Protection Act 1998 in terms of sending and receiving sensitive personal information.
- Regular training is available to staff on online safety issues and the school's online safety education programme.
- Information and guidance on the Safeguarding policy and the school's Acceptable Use Policy is provided to all new staff and governors.
- Training Audit Log to be updated annually (Appendix 6).

Parent engagement

The school recognises the important role parents and carers have in ensuring children and young people are safe, responsible and can flourish online. To support parents to understand online risks and the work of the school in this area we will provide:

- Acceptable Use Policy Agreements (including permissions) to all new parents. Parents are reminded of these permissions annually via email and invited to amend these permissions at any time.
- Regular, up to date information in newsletters and on the website and social media, particularly in response to emerging trends.
- Face to face sessions in school.
- Opportunities to share in their children's online safety learning (e.g. assemblies, performances).
- Support and advice on online safety for their children outside of school.
- Signposting to further resources and websites.

3.a Conduct and Incident management

Conduct

All users are responsible for using the school ICT systems in line with the Acceptable Use Agreements they have signed. They should understand the consequences of misuse, or accessing inappropriate materials.

All members of the school community should know that this policy also covers their online activity outside of school if it relates to their membership of the school.

Parents and carers will be asked to give consent for their children to use the internet and other technologies in school, by signing an Acceptable Use Agreement. They will also be given clear information about the sanctions that might result from misuse.

Incident Management

All members of the school community understand they have a responsibility to report issues and are confident that anything raised will be handled quickly and sensitively, in line with the school's Misuse Plan. HMFA actively seeks advice and support from external agencies in handling online safety issues. Parents and carers will be informed of any online safety incidents relating to their own children, unless doing so may put the child at risk. All parents and carers will receive more general online safety advice in response to incidents, without revealing any sensitive or personal information about students.

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context (those in bold are illegal) and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- ***child sexual abuse images (illegal - The Protection of Children Act 1978)***
- ***grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)***
- ***possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)***
- ***criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)***
- *pornography*
- *promotion of any kind of discrimination*
- *promotion of radicalisation and/or extremism*
- *promotion of racial or religious hatred*
- *threatening behaviour, including promotion of physical violence or mental harm*
- *any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute*

Additionally the following activities are also considered unacceptable on ICT kit provided by the school:

- *Using school systems to run a private business*
- *Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school*
- *Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions*
- *Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)*
- *Creating or propagating computer viruses or other harmful files*
- *Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet*
- *On-line gambling and non-educational gaming*
- *On-line shopping / commerce*

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Please see Appendix 2.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have

been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupil sanctions

	Refer to class teacher	Refer to online safety coordinator	CHILD PROTECTION ISSUE – refer to Safeguarding Manager	Refer to headteacher	Refer to Police	Refer to IT Technical support	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓		✓		✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓	✓				✓		✓		
Unauthorised use of mobile phone / digital camera / other handheld device	✓			✓			✓			
Unauthorised use of social networking / instant messaging / personal email	✓	✓				✓				
Unauthorised downloading or uploading of files	✓	✓				✓				
Allowing others to access school network by sharing username and passwords	✓	✓		✓		✓		✓		
Attempting to access the school network, using another pupil's account	✓	✓		✓		✓		✓		
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓		✓				✓		
Corrupting or destroying the data of other users	✓	✓		✓			✓	✓	✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓	✓			✓		✓	
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓	✓		✓	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓		✓			✓		✓	
Using proxy sites or other means to subvert the school's filtering system	✓	✓		✓		✓		✓	✓	
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓		✓		✓	✓			
Deliberately accessing or trying to access offensive, radical, extremist or pornographic material	✓	✓	✓	✓	✓	✓		✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓		✓		✓	✓	✓	✓	

Staff sanctions

	Refer to line manager	Refer to head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓	✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓	✓			✓	✓		
Unauthorised downloading or uploading of files	✓	✓			✓	✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	✓				✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓	✓				✓		
Deliberate actions to breach data protection or network security rules	✓	✓			✓	✓	✓	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓			✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓			✓	✓	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✓	✓	✓			✓		✓
Actions which could compromise the staff member's professional standing	✓	✓				✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓				✓		
Using proxy sites or other means to subvert the school's filtering system	✓	✓			✓	✓	✓	
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓			✓	✓		
Deliberately accessing or trying to access offensive, racist, extremist, radical or pornographic material	✓	✓	✓		✓	✓	✓	
Breaching copyright or licensing regulations	✓	✓				✓		
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓			✓	✓	✓

3.b Reporting of Incidents (Misuse Plan)

The majority of ICT misuse incidents in schools involve a violation of the school's Acceptable Use Agreement rather than illegal activity. All ICT use that violates our rules will be dealt with promptly and fairly through normal disciplinary procedures. (Refer to flowchart on appendix 7 plus agreed forms to complete are in Appendices 8, 9 & 10)

Written procedures **– urgent risk and illegal conduct**

In the case of an ICT incident involving immediate risk to a child, we will inform the Designated Safeguarding Lead and follow school child protection procedures. We will also consult the Herefordshire Safeguarding Children Board (LSCB) or Multi-Agency Safeguarding Hub (MASH) and, in urgent cases, inform the local police.

In cases where a child is not at immediate risk, we will proceed as follows:

If we discover content that is or might be illegal, the LSCB or school's online safety officer will be notified. In cases involving images of child sexual abuse, we will notify the Internet Watch Foundation. Other criminal content will be reported to the local police or CEOP.

If we suspect that a student or member of staff has engaged in illegal activity online, the CSU or online safety officer will be notified. In cases involving possible sexual exploitation of a child online, we will report the incident to CEOP. Other criminal activity will be reported to the relevant law enforcement agency. We will cooperate fully with any investigation by CEOP or the police and will follow the investigation with our own child protection or staff allegation procedures as necessary.

All online safety or ICT misuse incidents will be recorded in the school's incident log. Following an incident, we will review our policies and make any necessary changes.

In addition to the general procedures laid out above, the school will keep in mind the following best practices, especially where deliberate misuse is suspected:

- Involve multiple senior members of staff or governors in the review and monitoring process if possible
- Use a designated and secured computer for the duration of the review. The computer should not be one that is used by students and should be one that police can take off-site if needed
- Keep a careful record of any websites and content visited while investigating a misuse incident, including the url (web link) of the site and a description of the content in question. In some cases, it may be necessary to store screenshots of the content. (Please note that this does **not** include images of child sexual abuse – see below)
- If child abuse images are discovered in the course of a review, internal monitoring should immediately be stopped and the incident should be reported to the police. The police should also be consulted if a review uncovers grooming of a child, obscene material sent to a child, adult material in violation of the Obscene Publications Act, criminally racist material or any other illegal activity.

3.c Electronic Devices - Searching & Deletion (June 2012)

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 school will not face legal challenge but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

Responsibilities

The Executive Headteacher has authorised the Head of Schools and any member of the school's senior leadership team (SLT) to carry out searches for and of electronic devices and the deletion of data / files on those devices.

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

The school 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.

This online safety Policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

The school's policy on the use of mobile devices is set out in section A.3.1 of this policy and the sanctions relating to breaches of these rules in section A.2.6

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 school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so.

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff 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.

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

A record should be kept of the reasons for the deletion of data / files. This should be recorded in the IT & Esecurity/Online Safety/School name/Schoolname online Safety Logs folder

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 head teacher on a termly basis.

The Behaviour Policy refers to our Search and Deletion policy.

4. Managing the ICT infrastructure

The school is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that related policies and procedures are implemented. It will also ensure that the relevant people will be effective in carrying out their online safety responsibilities with regards to the ICT infrastructure.

There are regular reviews and audits of the safety and security of the school's technical systems.

All users have clearly defined access rights to the technical systems and school owned devices.

Security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly by IBS Schools. The HMFA schools' infrastructure and individual workstations are protected by up to date virus software.

Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

All users will be provided with a username and password by the school'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 school owned iPads must have strong passwords. The passwords must not be shared and staff are required to change their password twice a year (currently).

Temporary passwords can be issued by Sherry Morris-Davies, 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.

A multi-user account is available for visitors to the school (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 to determine school-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 school shared drives or their HMFA One Drive instead of using USB storage devices.

The administrator passwords for the school ICT system, used by IBS Peritech Technicians) is also available to the Executive Headteacher and kept in a secure place.

Filtering

Filtering information provided by IBS School (applies to HMFA schools apart from Marden Primary Academy, Clehonger CE Primary School & Pencombe CE Primary School)
Filtering is applied at network level. Software isn't required on any devices and applies across mobile and app technologies. Internet access is filtered for all users. There is a clear process in place to deal with requests for filtering changes.

Illegal content online
We use Smoothwall firewall who are IWF (Internet Watch Federation) members. Illegal content (child sexual abuse images and Content are blocked by actively employing the Internet Watch Foundation CAIC list and also Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'. Content lists are regularly updated and internet use is logged and regularly monitored.

Inappropriate online content
These are listed the categories that are blocked at HMFA schools:
• Violence/Hate/Racism
• Intimate Apparel/Swimsuit
• Nudism
• Pornography
• Weapons
• Adult/Mature Content
• Cult/Occult
• Drugs/Illegal Drugs
• Illegal/Questionable Skills
• Sex Education
• Gambling
• Alcohol/Tobacco
• Chat/Instant Messaging
• Abortion/Advocacy Groups
• Online Banking
• Online Brokerage and Trading
• Games
• Hacking/Proxy Avoidance Systems
• E-mail (Web based)
• Web Communications
• Personals and Dating
• Shopping
• Internet Auctions
• Freeware/Software Downloads
• Pay to Surf Sites
• Social Networking
• Malware

Other types of content managed by the system
The Smoothwall is licensed with Comprehensive Gateway security suite (CGSS) which provides you with a single integrated package of security technologies. It helps stop threats such as intrusions, viruses, spyware, worms, Trojans, adware, key loggers, malicious mobile code (MMC), and other dangerous applications entering our network.
SSL filtering is part of Smoothwall's filtering system as standard.

How the system avoids overblocking
Smoothwall has categorized over 20 million URLs, IP addresses and domains in a database, with thousands more added daily. Because the ratings are determined both by artificial intelligence and human observation, the database is highly accurate and the instance of false positives is minimized.

Filtering for different age groups and roles
The policy-based system allows the blocking of pre-defined categories in any combination and to apply these policies on a granular level. For example, if one group of users requires access to sites typically found within one category, this level of access can be granted while still denying access to other users.

How HMFA controls the filter to allow or block specific content or sites
Currently the school makes a request via the IBS Schools helpdesk via email, the online Peritech logbook or to a IT Technician during an SLA visit for sites/categories to be blocked/allowed.

How the system identifies individual users
The Smoothwall integrates with Active Directory to determine who is logged onto domain joined devices. The groups the user is a member of determines the filtering policy they receive. IPads are identified via IP address. Staff iPads share the base level of filtering, if they require access to higher level content they are prompted for their Active Directory credentials (username & password).

HMFA schools report content to IBS Schools for access or blocking
Via the IBS Peritech Logbook, emailing support helpdesk or during an SLA visit.

How IBS Schools' system provides reports on the websites visited by HMFA users
Smoothwall generates instant reports and weekly that are sent via email to Jo Brace, Jan McColl, and the Headteacher.

Monitoring
Smoothwall Safeguarding suite actively monitors internet & webs access of users and devices and generates alerts for the school to act upon.

Teachers can also use Apple Classroom to actively monitor ‘real time’ iPad use of pupils in their class.

Social Media
The HMFA has a Social Media Policy that covers the management of school accounts and set out guidelines for staff personal use of social media.

5. Data Protection

The school has a Data Protection Policy that is regularly reviewed and updated by our Data Protection Officer (DPO) HY Professional Services. The Privacy Notice and Data Protection Policy can be found on the Polices & Statements section of our school websites. All HMFA schools are registered with the ICO.

6. Equipment and Digital Content

6.a Use of Mobile Technologies (iPads, laptops & phones etc)

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

Pupil Use of Mobile Phones

The school strongly advises that pupil mobile phones should not be brought into school.
Where pupils bring mobile phones to school by prior agreement these are stored in the school office during the school day. They should be clearly labelled with the child's name and passcode protected. Pupil mobile phones must be turned off or placed on silent.

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 school rules. Any search will be carried out in line with the school's Search Policy – Electronic Devices (p10 of this document).

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 school trips. School cameras are available and should be used in conjunction with the Mobile Phone/Acceptable Use Policy.

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

Occasionally, the online safety lead (Jo Brace) and the ICT Co-ordinator at LSA (Sherry Morris-Davies, 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 Cameras in EYFS and After School Care

Appropriate use of mobile phones is essential at Breakfast and Kidsclubs. 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 school 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 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 dialling 141 first).

iPads and Laptops – School Owned

Staff Use

- Unique IDs (provide by the school) are used on staff tablets (to avoid accidental data transfer to colleague's tablets). Necessary passwords are given to member of staff.
- Personal IDs (often with associated personal media collections, e.g. music from iTunes) are not to be used on school 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.
- Cloud storage (other than officially endorsed systems) is not used for sensitive data.
- Specific training on tablet security issues is provided for staff using tablets.
- 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 pubic Wi-Fi

Pupil Use of School Owned iPads

- A growing number of iPads are available for children to use in school
- Lord Scudamore Academy, Kings Caple, Sutton, Llangrove, Canon Pyon, St Weonards and Pencombe schools and academies iPads are managed via a Mobile Device Management (MDM) system.
- At all other HMFA schools, the iPads are managed locally using Apple Configurator on an HMFA owned MacBook. All HMFA schools are to move to an MDM solution as part of the IT Development Plan.
- Age appropriate apps are purchased via Apple's VPP store and deployed with due regard to licensing and copyright.

- Files are transferred to from and between iPads using a variety of methods. All schools have Microsoft's One Drive. The One Drive app is installed on all iPads and the school's one drive account is logged into on all iPads. Children are not given the password. Schools are trialling the use of Online Portfolios services (Tapestry EYFS and Seesaw (KS1 & 2).
- We make use of cloud services in other carefully chosen apps.
- Parents give their permission for this via the parents' AUP agreement and permissions form (see appendix 3). There is the option to withdraw consent at any time.

6.b - Digital images and video

We believe that photographs validate children's experiences and achievements and are a valuable way of recording milestones in a child's life. Parental permission for the different ways in which we use photographs is gained as part of the initial registration on admission. We take a mixture of photos that reflect the school environment, sometimes this will be when children are engrossed in an activity either on their own or with their peers.

Children are encouraged to use the class camera/iPad to take photos of their peers. 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 school 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 school may have to ask that photographs are not taken at all. This is for confidential reasons when we need to protect individual children.

We seek permission from parents and carers for the use of digital photographs or video involving their child as part of the Use of Digital and Video Images Agreement when their child joins the school. Parents are able to withdraw their consent at any time.

We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video.

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

Students are taught to think carefully about placing any personal photos on social media sites. The importance of privacy settings as a tool to safeguard their personal information is included in internet safety education. They are also taught that they should not post images or videos of others without their permission.

Students understand the risks associated with sharing images that reveal the identity of others and their location, such as house number, street name or school.

6.c - Teaching of Website Creation to Pupils

The Computing Curriculum requires that pupils in KS2 are taught how to create websites.

Parents should be informed by letter explaining the sites to be used before the children embark on the project. They should sign an agreement giving permission for their websites to be made public or whether they prefer they should be private sites.

Teachers who set up the websites must only use pupil first names when setting up the sites and use a teacher created account using a teacher email address as part of the sign up.

Teachers must use this as an opportunity to teach pupils online safety e.g. digital footprint, what is suitable to share (privacy), how to ignore and be resilient to advertising etc.

6.d - Cloud Based Learning Platforms

The HMFA schools are currently trialling cloud based Learning platforms that can also provide an online portfolio of their work. These Learning Platforms (LPs) are Tapestry, Office365, Google Apps for Education, ShowBie & Seesaw. All cloud based systems used have been designed specifically for education purposes. They have Privacy Statements that comply with our Data Protection Policy.

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 school their account or rights to specific school 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.

7. Communication

Professional standards for staff communication

In all aspects of their work in our school teachers abide by the Teachers' Standards as described by the DfE (http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf. Teachers translate these standards appropriately for all matters relating to online safety.

Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems.

- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.
- It is not recommended that staff members have pupils, parents or ex-pupils as friends when personally using social networking sites (e.g. Facebook, Twitter, Instagram or Snapchat etc.).

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of pupils are used to inform this process also.

7.a - Email

Access to email is provided for all staff via Office 365.

Year 3 pupils have temporary access to the email system during the term when they are receiving Email lessons.

These official school email services may be regarded as safe and secure and are monitored.

- Pupils can only use the school email services in school using school systems
- Staff should use only the school email services to communicate with others on a professional basis for school related issues
- Users need to be aware that email communications may be monitored
- Pupils normally use only a class email account to communicate with people outside school and with the permission / guidance of their class teacher.
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email (see section C of this policy)
- Staff may only access personal email accounts outside of lesson times on school systems for emergency or extraordinary purposes. Staff may use personal email accounts outside of the teaching day. (Be aware that some online email accounts may be blocked by filtering).
- Users must immediately report, to their class teacher / Designated Safeguarding Lead – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

7.b - Social networking (including chat, instant messaging, blogging etc)

- Teachers are encouraged to use educationally sound social networking tools, especially blogging, with children
- Only approved tools are used
- The use of non-educational and age inappropriate social networking by children is forbidden.
- See the HMFA Social Media Policy for further guidance.

7.c - Skype for education

Skype is used in school for small group video conferences. The following safeguards are in place:

- The Skype client software is installed only on selected computers
- The use of Skype with children is at all times monitored by staff
- Where the client software is installed, the default “Start Skype when I start Windows” tick is removed (Options – General Settings)
- The Skype shortcut in the Programs menu is removed and a shortcut to launch the software exists only in Common.Staff
- The school uses a single account created in the name of the school
- The client software is closed when not in use
- Skype is only used for appropriate education purposes and is fully supervised by staff.

7.d - Use of web-based publication tools

Website (and other public facing communications)

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

Here is a list of all of the HMFA school, websites:-

https://canonpyon.hmfa.org.uk

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://www.pencombe.hereford.sch.uk

https://www.clehongerschool.co.uk/

Our websites are for sharing information with the community beyond our school. 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 school 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).

Only pupil’s first names are used on the website, and only then when necessary.

Detailed calendars of Off-site events are not published on the school website.

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:

- 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 these show respect & dignity for the pupils
- images are not able to be copied or downloaded from the websites

Written permission from parents or carers is obtained before photographs of pupils are published on the school website (Appendix 3)

Pupil's work can only be published with the permission of the pupil and parents or carers. (Appendix 3)

Appendices

Appendix 1 – EYFS/KS1 – Acceptable Use Policy Agreement (signed by Pupils annually)

Appendix 2 – KS2 - Acceptable Use Policy Agreement (signed by Pupils annually)

Appendix 3 – Parent Permissions Form

Appendix 4 – Staff Acceptable Use Policy Agreement (signed by Staff annually)

Appendix 5 – Visitor/Community user Acceptable Use Policy Agreement (signed annually)

Appendix 6 – Training Audit Log

Appendix 7 – Incident Response Tool

Appendix 8 - Record of Reviewing Devices / Internet Sites (responding to incidents of misuse)

Appendix 9 - Online Safety Incident Report Form

Appendix 10 - Online Safety Incident Reporting Log

Credits

Elements of this policy has been taken from SWGfL and Digital School Member templates.

Monitoring, Evaluation and Review

We will review this policy annually and assess its implementation and effectiveness. The policy will be promoted and implemented throughout the Academy.

Appendix 1 – Acceptable use policy agreement EYFS/KS1

Three Cs for Online Safety (EYFS & KS1 AUP)

I agree to keep these computer rules:

Content

- ✓ 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.

Contact

- ✓ 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.

Conduct

- ✓ 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 understand these computer rules and always do my best to keep them.

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

Artwork is from: http://www.saferinternet.org/esafety-kit

Appendix 2 – Acceptable use policy agreement – pupil (KS2)

Our School's Three Cs of Online Responsibility (KS2 AUP)

I agree to be responsible online with:

CONTENT

- ✓ If I find anything online that makes me uncomfortable or that I think we shouldn't have on a school computer I tell an adult so they can sort it out for us
- ✓ I know that it's best if I check with an adult before downloading anything in school

CONTACT

- ✓ I make sure I keep personal information private and help others to do the same
- ✓ I keep all my passwords safe and never use anyone else's (even with their permission)
- ✓ I only use social networking (chat, blogs etc) through the sites the school lets me use
- ✓ If anyone I don't know tries to make contact with me online I ask an adult to give me advice

CONDUCT

- ✓ I show great respect for what others do online and I only post positive comments
- ✓ I make sure that my online image and the way I behave online reflects what a great person I am
- ✓ I make sure that I never share other people's personal information and photographs online unless I check with them first

I am a good, responsible person and proud that I take responsibility for my online behaviour.

I think these are great rules to keep us all safe and I agree to keep them. I promise to do my best to help others to keep these rules too.

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

Artwork is from: http://www.saferinternet

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 3 C's of Online Safety 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 a virtual learning environment (VLE).

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

Parent's signature:			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 Microsoft's O365 or Google Apps for Education (Y2-Y6) 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 **Microsoft O365 and Google Apps for Education**

Parent's signature:		Date:	

Our pupils also save work to a cloud based online portfolios (VLE) called Seesaw (Y1-Y6). 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**.

Parent's signature:		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.

Parent's signature:		Date:	

HMFA PHOTO & 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 name_____ Class_____

Signed parent/carer_____ Date_____

Appendix 4 - Staff AUP

Staff, teaching student & volunteer

Acceptable Use Policy Agreement - 10.07.19

Background

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while 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.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, iPads, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of our schools and academies.
- I understand that the school digital technology systems are primarily intended for educational use.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

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

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

- I will not use my personal mobile device e.g. laptops, tablets, USB devices or mobile phones during lessons (unless I have been given express permission to do so). If permission has been granted then I will follow the rules set out in this agreement, in the same way as if I was using *school / academy* equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school / academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any pc or laptop, or store programmes on a computer, nor will I try to alter computer settings (unless permission has been granted to do so).
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted and/or password protected. Passwords must not be emailed but telephoned to the recipient. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school / academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of HMFA IT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school / HMFA.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/ Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff / Volunteer Name:	
Signed:	
Date:	

Copy 1: to be kept by staff member
Copy 2: will be kept with staff member's personnel file.

Appendix 5 - Visitor/Community user Acceptable Use Policy Agreement

You have asked to make use of our school's ICT facilities. Before we can give you a log-in to our system we need you to agree to this acceptable use policy.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, of which I become aware, to a member of the school's staff.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

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

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, except with the specific approval of the school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines. I understand that failure to comply with this agreement will result in my access to the school's ICT system being withdrawn.

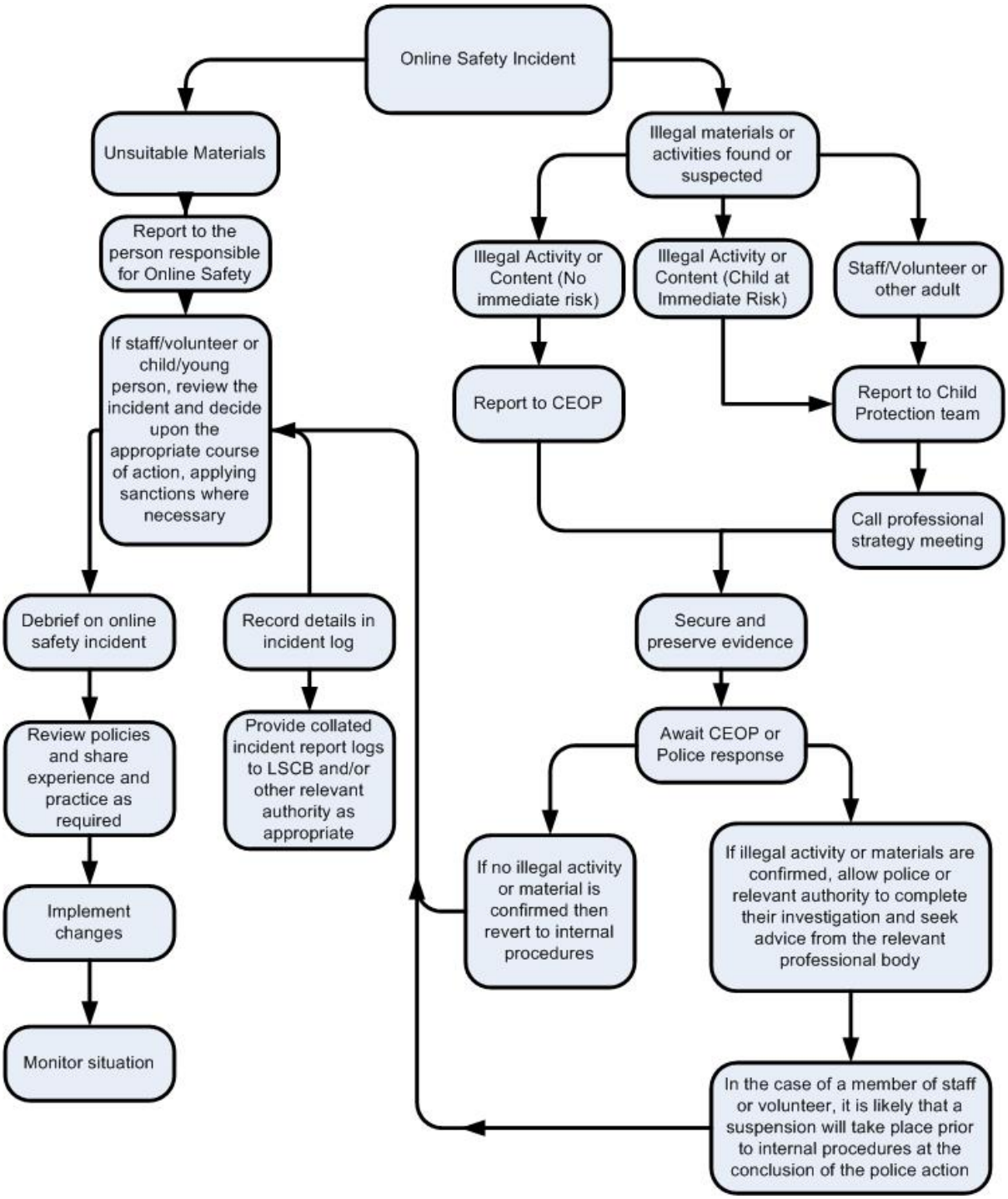
Community user Name:	
Signed:	
Date:	

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 Incident Report Form

Name of School:		
Your details		
Your name:	Position:	Data & Time of report:
Details of the Online Safety Incident		
Date & time of incident:		
Where did the incident occur? i.e. at school or at home:		
Who was involved in the incident?		
Child ☐ Name of Child:	Staff/visitor ☐ Name of Staff/volunteer:	
Description of incident (including IP address, relevant user names, devices and programs or apps used)		
Action taken: ☐ Incident reported to head teacher ☐ Advice sought from Safeguarding and Social Care ☐ Referral made to Safeguarding and Social Care ☐ Incident reported to police ☐ Incident reported to Internet Watch Foundation ☐ Incident reported to IT ☐ Disciplinary action to be taken ☐ Online Safety action to be taken ☐ Other (please specify)		
Outcome of investigation:		

Appendix 10 – Online Safety Reporting Log

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

HMFA Online Safety & Data Protection Group
Terms of Reference

HMFA Online Safety & Data Protection Group Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from the HMFA federation community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

2. Membership

2.1 The online safety group will seek to include representation from all stakeholders.

The composition of the group should include:

- Heads of School (DSL) - Kings Caple Primary Academy
- Head of School (DSL) – Sutton Primary Academy
- Head of School (DSL) – St Weonards Primary Academy
- Head of School (DSL) – Llangrove CE Academy
- Head of School (DSL) – Canon Pyon CE Academy
- Head of School (DSL) – Pencombe CE Academy
- Head of School (DSL) – Clehonger CE Academy
- Deputy Headteacher (DSL) - Marden Primary Academy
- HMFA Child Protection/Safeguarding officer (DSL for Lord Scudamore Academy & Director of Safeguarding
- Director of IT & DPO/Online Safety Lead
- IT Technical Support staff (where possible)
- Digital Leaders for advice and feedback. *Pupil voice is essential in the make-up of the online safety group, but pupils are only expected to take part in committee meetings where deemed relevant.*

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of Meetings

Meetings shall be held half termly for a period of 1 hour. These will take place during a scheduled designated Safeguarding Lead meeting. A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

These are to assist the Online Safety Lead (or other relevant person) with the following:

- To keep up to date with new developments in the area of Online Safety & Data Protection Team m
- To annually review and develop the HMFA Online Safety policy in line with new technologies and incidents

- To annually review and develop the Data Protection policy in line with new legislation, development & incidents
- To monitor the delivery and impact of the HMFA Online Safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole HMFA federation community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through]:
    - Staff meetings
    - Pupil Council (for advice and feedback)
    - Parents workshops
    - Directors meetings
    - Local advisory Board meetings
    - Surveys/questionnaires for students / pupils, parents / carers and staff
    - Parents afternoons/evenings
    - HMFA and school websites
    - Newsletters
    - Online safety events
    - Safer Internet Day (annually held on the second Tuesday in February)
    - Other methods
- To ensure that monitoring is carried out of Internet sites used across the school and across the HMFA federation
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the schools and across the Trust
- To monitor incidents involving online-bullying for staff and pupils

6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for HMFA have been agreed

Signed by Executive Headteacher:

Date:

Signed by Executive Headteacher:

Date:

Date for review: