HMFA

Herefordshire Marches
Federation of Academies

St Weonard's

Online Safety Policy

March 2017

Next Review Due: January 2018

Co-ordinator – Mrs J Brace

HMFA Online Safety Policy

POLICY DATE: 8 February 2017 REVIEW DATE: January 2018

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.

Communication of the policy

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

- Displayed on the school website, and available in the staffroom and classrooms.
- Included as part of the induction pack for new staff.
- Acceptable use 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 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 school 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 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 head teachers, deputy head teachers and safeguarding manager 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 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. Staff and Governors will be informed of any updates or amendments to it.

The Online Safety Committee is comprised of:-

Jo Brace (Deputy Headteacher - IT Development & Marketing for LSA)

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

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

Phil Clewer (IT Technician at D&D - all HMFA schools apart from Marden Primary Academy)

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

Student online safety curriculum

The school has a clear, progressive online safety education programme primarily as part of the Computing curriculum / PSHE curriculum 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 understands 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 Agreements to all new parents.
- Regular, up to date information in newsletters and on the website and social media, particularly in response to emerging trends.
- 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. 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.

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.

Password Security
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).

Filtering information provided by D&D (applies to HMFA schools apart from Marden Primary Academy)

Filtering is applied at network level. Software isn't required on any devices and applies across mobile and app technologies.

Illegal content online
We use SonicWall firewall who are IWF (Internet Watch Federation) members. Child Abuse Images and Content are blocked

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

Are there other types of content that your system manages?
The SonicWall at LSA 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 your network.
SSL filtering is part of LSA's SonicWall system automatically. All other HMFA schools need to purchase DPI – SSL licensing on an annual or 3 yr basis.

How does your system avoid overblocking?
SonicWall CFS 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 D&D helpdesk or direct to an engineer during an SLA visit for sites/categories to be blocked/allowed.

How the system identifies individual users
The SonicWall 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.

HMFA schools report content to D&D for access or blocking
Via the helpdesk or during an SLA visit.

How D&D's system provides reports on the websites visited by HMFA users
Currently the system does not offer this. It is available as an additional add-in.

- The technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of the school's technical systems.
- All users will have clearly defined access rights to the technical systems and school owned devices.
- All users will be provided with a username and secure password. Users will be responsible for the security of their username and password. Some classes also have a group log-on and password.
- The administrator passwords for the school ICT system, used by D&D IT Technicians) is also available to the Headteacher and kept in a secure place.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.

- HMFA schools allow different filtering levels for different groups of users – staff / students. We are working with our IT support providers on setting up differentiated filtering levels for different ages / stages.
- The current systems do not allow proactive monitoring of devices. We are working with our IT support companies to build this into our networking infrastructure.
- Security measures are in place 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 D&D. 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.

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

The school has a Data Protection Policy that is regularly reviewed and updated. This includes information on the transfer of sensitive data; and the storage and access of data.

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.

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) or ICT Technician, may need to use their mobile phones in the vicinity of children in order to report an IT issue to our IT support (D&D). 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 Early Years Foundation Stage and Kidsclubs (After school care)

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.

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, eg 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 soon to use a mobile device management system (MDM) that will manage and track staff tablets.
- Members of staff are encourage 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
- At St Weonard's primary, 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, Seesaw & ShowBie (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)

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 20 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.

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, 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 using these systems monitor the use of the LP by pupils regularly in all areas, but with particular regard to messaging and communication.

Staff use is monitored by the administrator.

User accounts and access rights can only be created by the school administrators and by LA administrators.

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 access to the learning platform.

When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled (or transferred to their new establishment if possible / appropriate).

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 the site administrator if the user does not comply.

c) Access to the LP for the user may be suspended.

d) The user will need to discuss the issues with a Deputy Headteacher before reinstatement.

e) A pupil’s parent/carer may be informed.

A visitor (e.g. Global Partnership school or teaching student) may be given temporary and/or limited access to the LP by the school administrators following a request from a member of staff.

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 in school via the Outlook Web App accessible via a web browser (internet Explorer) from their desktop and also through the Microsoft Outlook 2010 application installed on their desktop or laptop.

Some staff have access to push email of Microsoft Exchange to their personal mobile phones or their school iPads.

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 person 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 http://schoolname.hmfa.org.uk) and http://hmfa.org.uk) .

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

http://canonpyon.hmfa.org.uk

http://kingscaple.hmfa.org.uk

http://llangrove.hmfa.org.uk

http://lordscudamore.hmfa.org.uk

http://marden.hmfa.org.uk

http://stweonards.hmfa.org.uk

http://sutton.hmfa.org.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 do not allow individuals to be recognised
- 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)

8. Illegal or inappropriate activities and related sanctions (Misuse Plan)

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.

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.

Pupil sanctions	Refer to class teacher	Refer to online safety coordinator	CHILD PROTECTION ISSUE – refer to Safeguarding Manager	Refer to Deputy head teacher	Refer to Police	Refer to ICT Network manager	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	✓	✓	✓			✓	✓	✓

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.

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 Local 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:

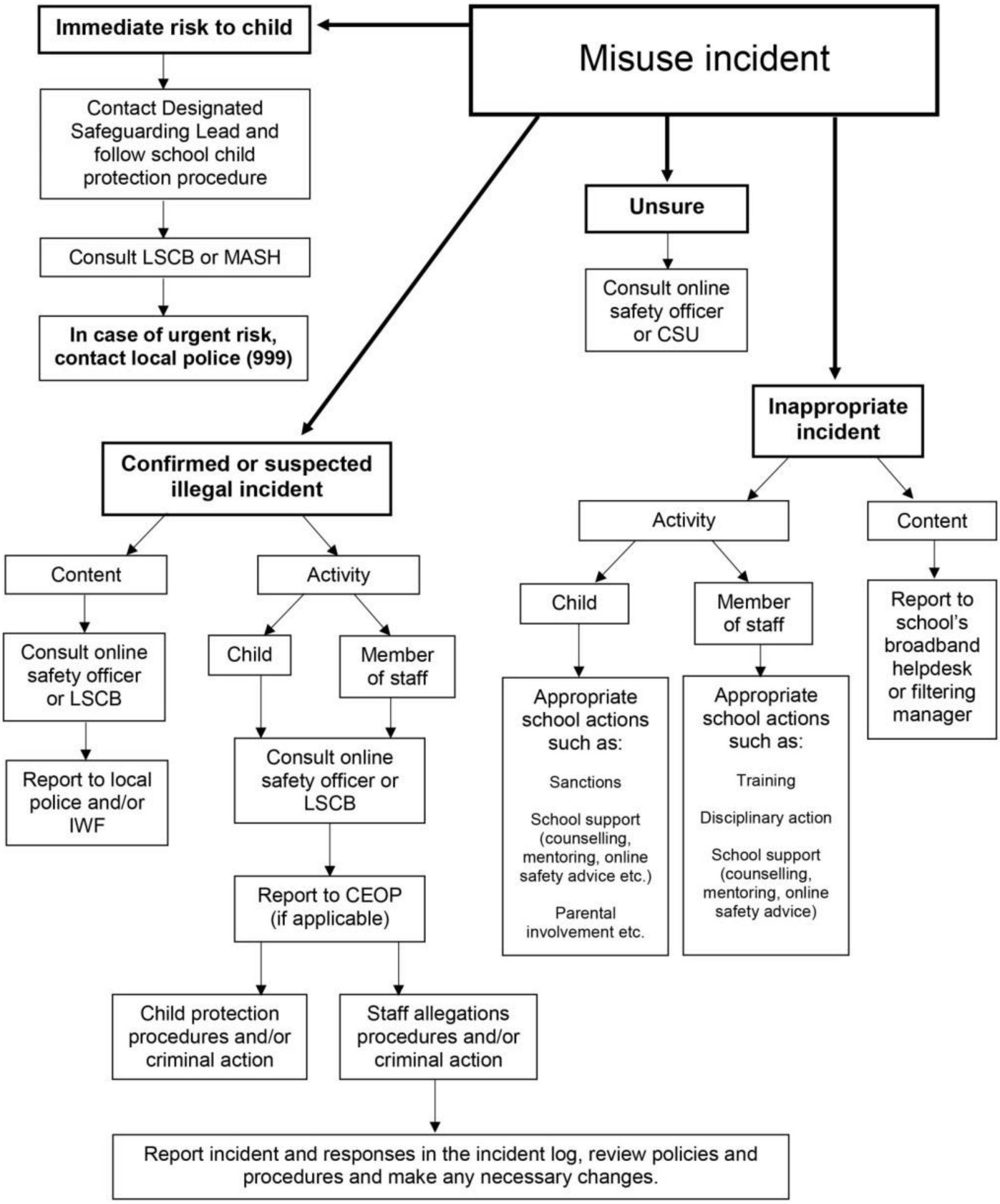
If we discover content that is or might be illegal, the LSCB or school's online safety officer will be notified. In cases involving images of child sexual abuse, we will notify the Internet Watch Foundation. Other criminal content will be reported to the local police or CEOP.

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 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 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.


Misuse incident
Immediate risk to child
Contact Designated Safeguarding Lead and follow school child protection procedure
Consult LSCB or MASH
In case of urgent risk, contact local police (999)
Unsure
Consult online safety officer or CSU
Inappropriate incident
Activity
Content
Child
Member of staff
Appropriate school actions such as:
Sanctions
School support (counselling, mentoring, online safety advice etc.)
Parental involvement etc.
Appropriate school actions such as:
Training
Disciplinary action
School support (counselling, mentoring, online safety advice)
Report to school's broadband helpdesk or filtering manager
Confirmed or suspected illegal incident
Content
Activity
Consult online safety officer or LSCB
Report to local police and/or IWF
Child
Member of staff
Consult online safety officer or LSCB
Report to CEOP (if applicable)
Child protection procedures and/or criminal action
Staff allegations procedures and/or criminal action
Report incident and responses in the incident log, review policies and procedures and make any necessary changes.

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 – Online Safety Incident Reporting Log

Credits

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

Monitoring, Evaluation and Review

The Governing Body will review this policy annually and assess its implementation and effectiveness. The policy will be promoted and implemented throughout the school.

Approved by HMFA: February 2017

Appendix 1 – Acceptable use policy agreement EYFS/KS1

Three Cs for Computers (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.

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.org/esafety-kit

Appendix 3 - Acceptable use policy agreement and permission forms – parent / carer

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users 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 ICT (especially the internet).
- that school ICT 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 ICT to enhance their learning and will, in return, expect them to agree to be responsible users.

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.

Child's name			
Parent's name			
Parent's signature:		Date:	

Permission for my child to use the internet and electronic communication

As the parent / carer of the above pupil(s), I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of ICT – both in and out of school.

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

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

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

Parent's signature:		Date:	

E-mail alerts and correspondence

I would like to receive e-mails of newsletters, trip reminders and other information from my child's class.

Parent's signature:		Date:	
Preferred e-mail address:			

Permission to use digital images (still and video) of my child

The use of digital images (still and video) plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website *and in school controlled social media.* The school will comply with the Data Protection Act and we will ensure that, when images are published, young people cannot be identified by name.

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

I agree to the school taking and using digital images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school. 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:	

Newspaper, TV, Radio- permissions form

I agree to images / video of my child being taken and used by approved 3rd party organisations (e.g. local newspapers, TV, radio) and I understand that these organisations may not adhere to our school code of practice (e.g. with respect to not printing names etc. alongside pictures)

Parent's signature:		Date:	

Use of cloud based systems – permission form

Many of the apps we use (apps which are used across the world in schools) make use of cloud storage. The school strives for compliance with the data protection act in all respects here (for example we use Microsoft's One Drive, Seesaw & ShowBie for storing some pupil work via Online Portfolios,

We ask for your consent to your child making use of this technology.

Parent's signature:		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, ClassDoJo 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:	

Our school's Online safety Policy, which contains this Acceptable Use Policy Agreement, and the one signed by your child (to which this agreement refers), is available on the school website.

Appendix 4 - Acceptable use policy agreement – staff, teaching student & volunteer

Background

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT 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 ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE, iPads etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the Online Safety policy.
- 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, 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 images. I will not use my personal equipment to record these images. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured. (see pages 7, 8, 9 & 10 of the Online Safety policy).
- I will not use chat or social networking sites in school (unless I have responsibility for website development, have permission to check a cyber-bullying issue or using them for professional reasons e.g. Linkedin outside of lesson time) in accordance with the school's policies. (see page 11 of the Online Safety policy).
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (see page 10 of the Online Safety policy).
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- Staff members are not permitted to have pupils, parents or ex-pupils as friends when personally using social networking sites (e.g. Facebook). They must also not post comments / images that relate to school life.

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 devices e.g. tablets or mobile phones during lessons (unless I have been given express permission to do so). If permission has been granted then 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 except in an emergency.
- 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 ensure that my data is regularly backed up, in accordance with relevant school policies (see e-security policy).
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, radical or extremist or 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, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others using encrypted USB drives, AnyComms, (as outlined in the School e-security policy). Where personal data is transferred outside the secure school network, it must be encrypted or password protected (The password must not be emailed but telephoned to the recipient).
- I understand that the data protection policy requires that any staff or 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 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 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 ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police (see page 13 – 17 of the Online Safety Policy).

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

Staff / volunteer Name:	
Signed:	
Date:	

Appendix 5 - Acceptable use policy agreement – Visitor/community user

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:	

Training Audit Log - Online Safety, Parental Engagement and Digital Safeguarding (Appendix 6)

Group:

Date:

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

HMFA
Herefordshire Marches
Federation of Academies

Online Safety Incident Reporting Log (Appendix 7)

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