Haddenham St Mary's CE School

ONLINE SAFETY POLICY

Scope of the Policy

This policy applies to all members of the Haddenham St Mary's CE school (the school) community (including staff, pupils, volunteers, parents/carers, visitors) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the *school* but is linked to membership of the school. 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 published Behaviour Policy.

The *school* 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.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the School.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of Online Safety Governor. This role has been taken on by Gaynor Bull who is also the Child Protection governor. The role of the Online Safety Governor will include:

- regular meetings with the Designated Safeguarding Leads
- regular monitoring of online safety incident logs
- reporting to relevant Governors

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Deputy Safeguarding Leads in school who are also the Senior Leadership Team (SLT).

- The Headteacher and (at least) another member of the Senior Leadership Team 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 a later section – "Responding to incidents of misuse" and relevant Bucks Council local disciplinary procedures).
- The Headteacher is responsible for ensuring that staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will respond to staff reports and concerns.

Online Safety Officer

The Headteacher has the overall responsibility of the Online Safety Officer role with support from SLT. The Online Safety Officer will:

- have day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority / relevant body
- liaise with school technical staff
- receive reports of online safety incidents and creates a log of incidents to inform future online safety developments if needed
- meet regularly with the Online Safety *Governor* to discuss current issues and review incident logs as needed.

Network Manager / Technical staff:

Our Network is managed by the local Council- SchoolsTST fulfil the role and are paid to do this. RM provide our internet service and filtering.

The ICT Co-ordinator and Headteacher with support from SchoolsTST are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack

- that the school meets required online safety technical requirements and any Local Authority Online Safety Guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with online safety technical information in order to effectively carry out their role and to inform and update others as relevant
- that the use of the network and Microsoft Teams is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / SLT for investigation.
- that monitoring software / systems are implemented and updated.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher or SLT for investigation/action or sanction
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the internet safety rules and acceptable use policies
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Leads

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying.

Pupils

- are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Agreement
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's* Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents and carers will be encouraged to support the *school* in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- Microsoft Teams, both for themselves and their children

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, the school web site, Teams
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

We will do this in the following ways:

- A planned online safety curriculum will be provided as part of Computing and PHSE lessons and should be regularly revisited
- Key online safety messages will be reinforced as part of a planned programme of Collective Worship/assembly
- Pupils will be taught about the dangers that they might face when using the internet and the rules to follow if they feel uncomfortable.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment if they need to talk about this
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff will act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements
- It is expected that some staff will identify online safety as a training need within the performance management process
- The Online Safety Officer will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations

- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings and INSET days
- The Online Safety Officer and SLT will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any committee involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL)
- Participation in school information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

Our managed ICT service – Schoolstst and RM will carry out and support the school with online safety measures.

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School 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 school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- All staff users will be provided with a username and secure password who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. Pupils will not require a username and password for school devices but will receive one for Microsoft Teams
- The "master/administrator" passwords for the school ICT system, used by the ICT Co-ordinator must also be available to the Headteacher and School Business Manager and kept in a secure place

- SchoolsTST is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- 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 by RM
- Internet filtering will ensure that children are safe from terrorist and extremist material when accessing the internet
- The school has provided differentiated user-level filtering for staff and pupils
- An appropriate data breach system is in place for users to report any actual or potential technical incident / security breach to the GDPR Lead in school
- Appropriate 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. The school infrastructure and individual workstations are protected by up to date virus software
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems
- An agreed policy is in place regarding the extent of personal use that users (staff/ pupils/community users) and their family members are allowed on school devices that may be used out of school
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices
- An agreed Data Protection policy is in place regarding the use of removable media by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies

Mobile technology devices may be school owned or personally owned and might include: smartphone, tablet, notebook/ laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Child Protection Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of

mobile technologies should be an integral part of the school's Online Safety education programme.

- The school Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies

The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*No*	*No*	*No*	*On request*
Internet only	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*On request*
No network access	*Yes*	*Yes*	*No*	*No*	*Yes*	*Yes*

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

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press as part of the documents that parental consent forms completed on a yearly basis.
- 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 pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Pupil's work can only be published with the permission of the parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school has a Data Protection Policy and Data Retention Policy that ensures that all personal data will be fairly obtained in accordance with the relevant GDPR Privacy Notice.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults			Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	x							x
Use of mobile phones in lessons		x						X

Use of mobile phones in social time	x							X
Taking photos on mobile phones / cameras		x						x
Use of other mobile devices e.g. tablets, gaming devices	x							x
Use of personal email addresses in school , or on school network	x							x
Use of school email for personal emails		x						x
Use of messaging apps	x					x		
Use of social media	x							x
Use of blogs	x							x

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, chat, Teams) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Email addresses will be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

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

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
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 –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination					X
	threatening behaviour, including promotion of physical violence or mental harm					X
	Promotion of extremism or terrorism					x
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	

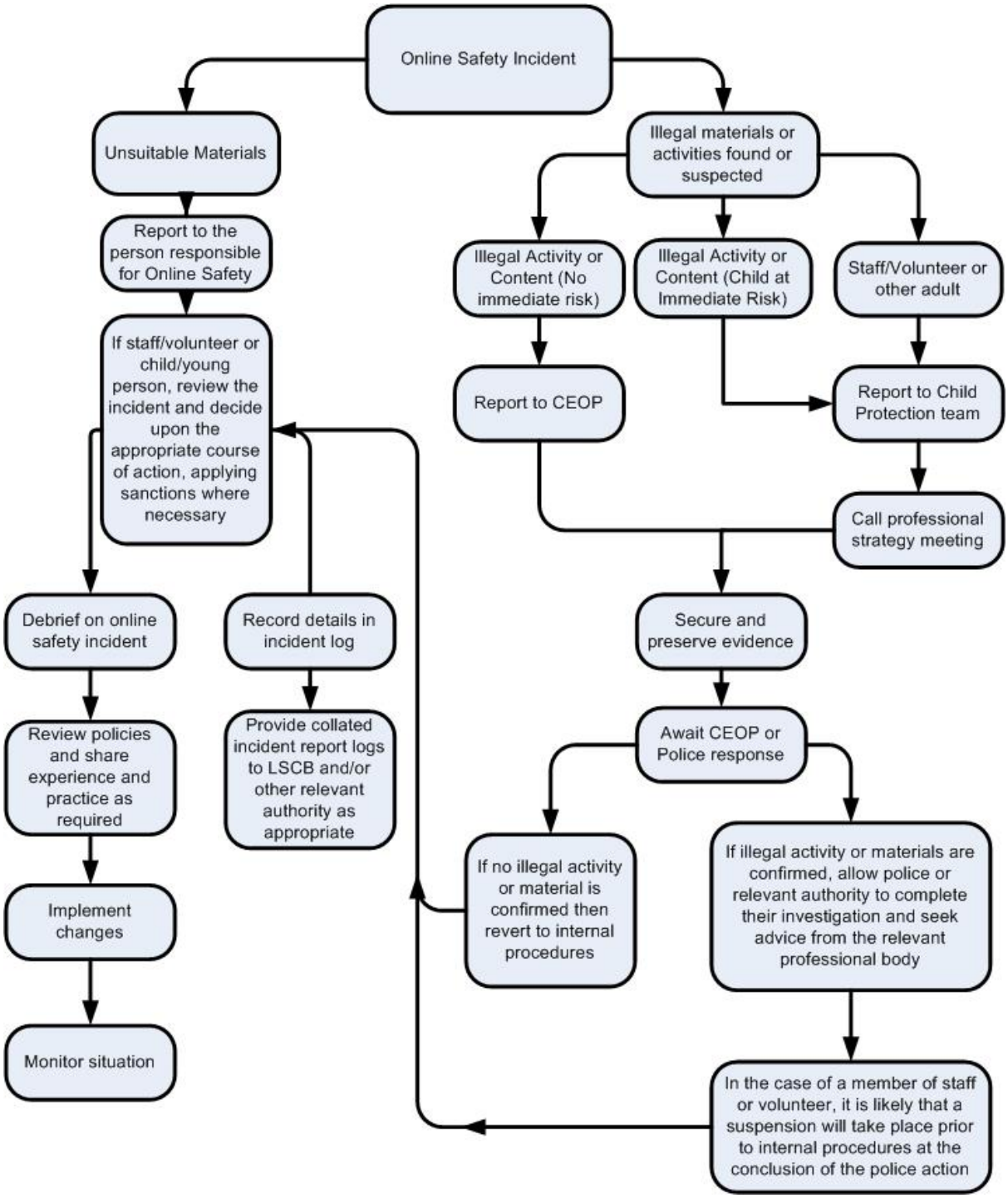
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)				x	
On-line gaming (non-educational)				x	
On-line gambling				x	
On-line shopping / commerce	x				
File sharing		x			
Use of social media	x				
Use of messaging apps	x				
Use of video broadcasting e.g. Youtube	x				

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were

carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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 with pupils and staff will be dealt with through normal behaviour/disciplinary procedures as follows. Staff incidents will always follow the Bucks Council disciplinary procedures and the Headteacher will seek advice in these circumstances when appropriate.

Actions/sanctions

Pupils Incidents	Refer to class teacher	Refer to Headteacher /SLT	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X			x	x		
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		x			x	x		
Unauthorised / inappropriate use of social media / messaging apps / personal email		x			x	x		
Allowing others to access school network by sharing username and passwords		x		x	x	x		

Attempting to access or accessing the school network, using another student's / pupil's account		x		x	x	x		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x		x	x	x		
Continued infringements of the above, following previous warnings or sanctions								x
Deliberately accessing or trying to access offensive or pornographic material		x		x	x	x		

Staff Incidents	Refer to Local Authority /	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X				
Inappropriate personal use of the internet / social media / personal email				x		x
Unauthorised downloading or uploading of files			x	x		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x				x	x
Careless use of personal data e.g. holding or transferring data in an insecure manner				x		
Deliberate actions to breach data protection or network security rules	x					x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x					x

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x					x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	x					x
Actions which could compromise the staff member's professional standing	x				x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x				x	x
Using proxy sites or other means to subvert the school's / academy's filtering system			x	x		
Accidentally accessing offensive or pornographic material and failing to report the incident			x	x		
Deliberately accessing or trying to access offensive or pornographic material	x				x	x
Breaching copyright or licensing regulations			x	x		
Continued infringements of the above, following previous warnings or sanctions	x				x	x

Links to other policies:

This policy should be read and links with the following policies:

- HSM Remote Learning Policy
- HSM Child Protection Policy
- HSM Behaviour Policy
- HSM Staff conduct agreement

Legislation

This Online Safety Policy has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

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

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to

imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

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

Regulation of Investigatory Powers Act 2000

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

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

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

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is

intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

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

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

Racial and Religious Hatred Act 2006

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

Protection from Harrassment Act 1997

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

Protection of Children Act 1978

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

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers,

health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

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

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

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

The Education and Inspections Act 2006

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

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

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

The School Information Regulations 2012
Requires schools to publish certain information on its website:

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

Serious Crime Act 2015
Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Links to other organisations or documents

Safer Internet Centre – http://saferinternet.org.uk/
South West Grid for Learning - http://swgfl.org.uk/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/
CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others
INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

Tools for Schools
Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

Bullying / Cyberbullying
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) - http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Social Networking
Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Connectsafely Parents Guide to Facebook
Facebook Guide for Educators

Curriculum
Glow - http://www.educationscotland.gov.uk/usingglowandict/
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Mobile Devices / BYOD
Cloudlearn Report Effective practice for schools moving to end locking and blocking
NEN - Guidance Note - BYOD

Data Protection

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO
Guide to Data Protection Act - Information Commissioners Office
Guide to the Freedom of Information Act - Information Commissioners Office
ICO guidance on the Freedom of Information Model Publication Scheme
ICO Freedom of Information Model Publication Scheme Template for schools (England)
ICO - Guidance we gave to schools - September 2012 (England)
ICO Guidance on Bring Your Own Device
ICO Guidance on Cloud Hosted Services
Information Commissioners Office good practice note on taking photos in schools
ICO Guidance Data Protection Practical Guide to IT Security
ICO – Think Privacy Toolkit
ICO – Personal Information Online – Code of Practice
ICO Subject Access Code of Practice
ICO – Guidance on Data Security Breach Management
LGfL - Data Handling Compliance Check List
NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

NEN - Guidance Note - esecurity

Working with parents and carers

Online Safety BOOST Presentations - parent's presentation
Connectsafely Parents Guide to Facebook
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media
The Cybersmile Foundation (cyberbullying) - advice for parents

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
Futurelab - "Digital participation - its not chalk and talk any more!"
Ofcom – Children & Parents – media use and attitudes report - 2015

Glossary of Terms

AUP / AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW

TUK Think U Know – educational online safety programmes for schools, young people and parents.

VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP Wireless Application Protocol

UKSIC UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

Appendix 1: Staff acceptable User Policy

- Staff closely monitor and scrutinise what their pupils are accessing on the Internet including checking the history of pages
- Computer monitor and iPad screens are readily visible for the teacher, so they can monitor what the pupils are accessing
- Pupils have clear guidelines for the content of e-mail messages, sending and receiving procedures
- Pupils only use the Internet when supervised by a teacher or adult
- Pupils are taught skills and techniques to enable efficient and effective use of the Internet
- Pupils have a clearly defined focus for using the Internet and e-mail
- If offensive materials are found (despite using professional filters) the monitor or screen should be switched off, materials confiscated and offensive URLs should be given to the ICT Co-ordinator who will report it to our IT support provider
- Virus protections are essential and will be used
- The recommended ISP (Bucks Council) will check sites visited by schools
- Participating in newsgroups/discussion groups – these groups are open to all therefore be careful! It is recommended that pupils don't use these forums

I have read the NetSmart Code of Practice for staff

I agree to abide by the Staff Code of Practice.

Name: _____

Signed: _____

Date: _____

Appendix 2: Staff code of conduct (extracted)

10 GUIDANCE ON USING IMAGES OF CHILDREN

The following is an amalgamation of general advice from the DfE Publicity Division and advice offered from the teams responsible for child protection and for safe use of images on the net and in other media.

10.1 Providing the name and photograph of a pupil either written, website or video format allows for the possibility that people outside the school might identify and then contact or attempt to contact pupils directly. The measures described below can help to reduce the risk of inappropriate and/or unsolicited attention:

10.2 When considering the use of photographs of children, avoid close-up pictures of individual children where possible and instead, use general shots of classroom or group activities. Decide whether there is a need for the school and/or the pupils to be identified at all. If there is such a need, avoid captions that give the children's full names or include personal details such as e-mail addresses, home addresses and telephone numbers.

10.3 It is acceptable practice, in normal conditions, to give the first name of a pupil and their school name as this should not give any information that is not easily accessible from other sources. Of course, in some cases, a pupil/pupils may wish to be associated with the image (i.e if the subject matter is such that it reflects well on them or their school). In such cases, it may be harder to only include a first name. In such circumstances, other issues such as whether the image is to be publicly available or only to a 'closed' audience should also be considered. There may also be some circumstances in which the use of false names is justified.

10.4 Only use images of pupils in suitable dress e.g. school uniform, remember that children can be identified through logos or emblems on sweatshirts etc. Sometimes it may be necessary to airbrush or 'fuzz' out the relevant part of the image. It may also be inappropriate to use images or footage of pupils doing PE even if the school and/or pupils are not identified.

10.5 If you are still undecided on the best approach, a broad rule of thumb to remember is: **If the pupil is named, avoid using their photograph. If the photograph is used, avoid naming the pupil.**

10.6 In all circumstances, always ask for parental permission to use an image of a pupil and explain the purpose for which the image will be used and whether it will be retained for further use (and if necessary, offer assurances that the images will be securely stored and used only by those authorised to do so). Use this opportunity to reassure parents who may have concerns. This ensures that parents are fully aware of the way that the image of their child is being used.

10.7 Using photographs of items designed and made in technology lessons together with excerpts from written work and scanned images of artwork allows pupils' work to be exhibited to a wider audience without increasing the risk of inappropriate use of images of pupils.

11. ACCEPTABLE USE OF TECHNOLOGY

- Staff will not use technology in school to view material that is illegal, inappropriate or likely to be deemed offensive. This includes, but is not limited to, sending obscene emails, gambling and viewing pornography or other inappropriate content.

- Staff will not use personal mobile phones and laptops, or school equipment for personal use, in school hours or in front of pupils. They will also not use personal mobile phones or cameras to take pictures of pupils.

- We have the right to monitor emails and internet use on the school IT system.

12. USE OF SOCIAL MEDIA

- Staff are not permitted to be 'friends' with parents on social media unless they have known the parent previously to their child starting the school.

- Staff are not permitted to make any derogatory comments about the school or any comments that do not promote the schools values in terms of their own personal life.

- If staff are parents and linked to class social media groups, they are not permitted to make any derogatory comments about the school or cast any opinions on any subjects discussed relating to the school.

- School staff's social media profiles should not be available to pupils. If they have a personal profile on social media sites, they should not use their full name, as pupils may be able to find them. Staff should consider using a first and middle name instead, and set public profiles to private.

- Staff should not attempt to contact pupils or their parents via social media, or any other means outside school, in order to develop any sort of relationship.

- Staff will ensure that they do not post any images online that identify children who are pupils at the school without their consent.

- Staff should be aware of the school's e-safety policy

  If in doubt, don't post it!

13. STAFF PRIVACY

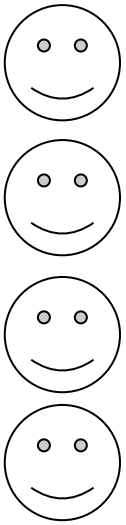
- Staff should not give out their personal details or any other members of staff personal details (eg. telephone numbers) to parents

Appendix 3: Pupil Acceptable Use Policy Agreement

Pupils' NetSmart Code of Practice

I'm NetSmart because (please colour in the faces):

- I only use the Internet when supervised by a teacher or adult
- I never tell anyone I meet on the Internet my home address, my telephone number or my school's name
- I never send anyone my picture
- I always tell my teacher if I see anything that upsets me



Pupil's Name: .....

I have read the pupil's NetSmart Code of Practice and I have discussed it with my child. We agree to support the school's policy on the use of the Internet.

Signed(Parent/Carer): _____

Date: _____

Appendix 4: Haddenham St Mary's CE Digital devices loan form

This is the detail of the device that will loaned to you:

Description:

Model:

IPad/laptop number:

The school has provided iPads and computers with Internet access to help your child's learning. These rules will keep your child safe and help us be fair to others.

- I will keep my iPad in its protective case at all times
- I will only access the systems and my device with my own login and password
- I will use the iPad for school work and homework as needed
- I will not behave in a way that can cause damage to iPads or to ICT equipment
- The messages I send will be polite and responsible
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent, Carer or teacher has given permission
- I will report any unpleasant material or messages sent to me
- I understand that use of the iPad is subject to the schools social media and pupil's Netsmart code of practice (reattached and signed on school entry previously)
- I understand that the iPad remains the property of the school all times during the loan period and that I will return the iPad to the school when my child no longer requires it or leaves the school
- I know I cannot buy the device

By signing this form I am agreeing to the terms above and will monitor and support my child to adhere to the rules. Please return this page to the School Office.

Parent's signature: _____ Date: ___/___/___

Pupil's name: _____ Class:_____

Appendix 5: HSM Covid-19 home-school remote learning agreement

Our school will:

- Provide remote learning that allows your child to access as much of the curriculum as possible
- Continue to nurture your child through regular contact to ensure that they are happy, safe and well
- Endeavour to support you with any technical difficulties that you may be experiencing
- Respond to any concerns you may have in a timely manner, within school hours
- Make alternative arrangements if your child can't access remote learning

I, as a parent/carer will:

- Do my best to support my child to complete any remote learning work set for them, and get in touch with the school if this won't be possible for any reason
- Ensure that any document uploaded by the teacher does not get moved to another location or edited
- Ensure that any queries I have regarding my child's academic tasks are directed to the class teacher within school hours
- Offer understanding and support to teachers who, as key workers, are continuing to provide care and routine for my child in these difficult circumstances
- Not utilise parent WhatsApp groups to provide a negative commentary of the school
- Only use the agreed channels to communicate with staff and ensure that my child does the same
- Monitor my child's use of Teams and what they are posting onto it
- Not compare HSM with other schools. All schools are operating under different circumstances.

I, as a Pupil of Haddenham St Mary's will:

- Do my best to complete the activities set for me by my teacher
- Listen to my teacher or the member of staff when they are on the screen and follow their instructions.

Social media

Nationally social media websites are being increasingly used to fuel complaints and campaigns against schools, school staff, headteachers and in some cases parents and children. Haddenham St Mary's CE School considers the use of social media in this way as

unacceptable and not in the best interests of the children or the school community. Any concerns parents may have should be addressed using the appropriate channels by speaking initially to the class teacher, then the Headteacher, or eventually to the Chair of Governors, so that they can be dealt with fairly, appropriately and effectively for all concerned.

In the event that any child, or parent of a child being educated at our school, is found to be posting libellous or defamatory comments on Facebook or other social media sites which are personal or would bring the school into disrepute, they will be reported to the 'report abuse' section of the network site. All social media networks have clear rules about the content that can be posted and provide robust mechanisms to report activity which breaches these. The school will also expect that the child or parent removes such comments immediately.

Should any member of the school community use *any* social media site to publically humiliate another this will be taken very seriously, and will be treated as an incidence of bullying behaviour which is not tolerated in our school.

In serious cases the school will consider its legal options to deal with any mis-use of social networking sites.

Possible sanction for failure to comply with this agreement:

- Removal of access to Microsoft Teams for your child/children

Appendix 6: HSM Record of reviewing devices / internet sites (responding to incidents of misuse)

Class/pupil: .....
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 web sites)

.....

.....

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Appendix 7: HSM record of online safety incidents

Reporting Log Group:						
Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By whom?		