High Ham C of E Primary School

Online Safety Policy

2019

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group /committee made up of:

- Headteacher / Senior Leaders
- Online Safety Officer / Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governors / Board
- Parents and Carers
- Community users
- Digital Leaders from across Key Stage 1 and Key Stage 2

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

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body on:	30th September 2019 Chris Palmer
The implementation of this Online Safety policy will be monitored by the:	Rupert Little Kayleigh Drew Jane Rosser
Monitoring will take place at regular intervals:	By Kayleigh Drew as part of Curriculum lead
The Governing Body will receive a report on the	Every FGB

implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	January 2021
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Designated Safeguarding Lead, Head teacher, Police.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology 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 online-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.

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:

Role	Responsibility
Governors	• **Approve and review the effectiveness of the Online Safety Policy** • **Delegate a governor to be part of the Online Safety Group** • **Online Safety Governor works with the Online Safety Leader to carry out regular monitoring and report to Governors** • **Ensure systems are in place that allow monitoring and Safeguarding discussions**
Head Teacher and Senior Leaders	• **Ensure that all staff receive suitable CPD to carry out their Online Safety roles including online risks of extremism and radicalisation** • **Create a culture where staff and learners feel able to report incidents** • **Ensure that there is a progressive Online Safety curriculum in place** • **Ensure that there is a system in place for monitoring Online Safety** • **Follow correct procedure in the event of a serious Online Safety allegation being made against a member of staff or pupil** • **Inform the local authority about any serious Online Safety issues** • **Ensure that the school infrastructure/network is as safe and secure as**

	possible • **Ensure that policies and procedures approved within this policy are implemented** • **Use an audit to annually review Online Safety with the school's technical support**
Online Safety Leader	• **Lead the Online Safety working group** • **Log, manage and inform others of Online Safety incidents and how they have been resolved where this is appropriate** • **Lead the establishment and review of Online Safety policies and documents** • **Lead and monitor a progressive Online Safety curriculum for pupils** • **Ensure all staff are aware of the procedures outlined in policies relating to Online Safety** • **Provide and/or broker training and advice for staff** • **Attend updates and liaise with the LA Online Safety staff and technical staff** • **Meet with Senior Leadership Team and Online Safety Governor to regularly discuss incidents and developments** • **Coordinate work with the school's designated Safeguarding Lead**

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular

information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at termly Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors Committee

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 Online Safety Lead.
- The Headteacher and (at least) another member of the Senior Management 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 Local Authority/other relevant body disciplinary procedures).
- The Headteacher is responsible for ensuring that the Online Safety Lead and other relevant 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 Management Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority/relevant body

- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meeting/committee of Governors
- reports regularly to Senior Leadership Team
- reach out to the community of parents to offer support with online programmes and support

Network Manager/Technical staff

The Technical Staff/Co-ordinator for ICT/Computing is 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 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 online safety role and to inform and update others as relevant
- that the use of the network/internet/Learning Platform/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher
- that monitoring software/systems are implemented and updated as agreed in school policies

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/Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher/Online Safety Officer/Lead
- 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 Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 Lead

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
- online-bullying

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. Depending on the size or structure of the school. This group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body and take part in policy changes.

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

- the production/review/monitoring of the school Online Safety Policy/ documents.
- the production/review/monitoring of requests for filtering
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs
- consulting stakeholders – including parents/carers and the pupils about the online safety provision

- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils:

- are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Agreement
- need to sign the Online Safety page of their Pupil Reading Record with their parent/carer and discuss the meaning of each point.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- 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
- understanding the importance of keeping passwords secure for their G Suite log in details to prepare for the transition to Secondary School
- understanding the information we have on G Suite is owned by the school and not by Google.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters and information about national/local online safety campaigns/literature. 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
- access to parents' sections of the website/Learning Platform and on-line student/pupil records
- their children's personal devices in the school
- their children upholding the signed agreement page of their Pupil Planner

Community Users

Community Users who access school systems as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school.

Digital Leaders

The Digital Leaders team is representatives chosen from each class, who bring a pupil voice to decisions linked to policy making and influencing the way we address the delivery of online safety education across the school. The Digital Leaders have a keen interest in ensuring all children become familiar with using their Google Accounts safely within school and using Google Classroom efficiently and safely at home.

A message from the High Ham Digital Leaders:

'Together, we aim to make sure everyone is safe, happy and secure whilst using and learning about technology.'

Policy Statements

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/digital literacy 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.

Keeping Children safe in Education

https://dera.ioe.ac.uk/22567/1/Keeping_children_safe_in_education.pdf

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

- A planned online safety curriculum should be provided as part of Computing lessons and will be regularly revisited as part of circle time and assemblies

- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making, under the Counter Terrorism and Securities Act 2015.
- Pupils should 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.
- Pupils should be reminded of the Pupil Planner page signed in their planners and understanding the importance of upholding this at home and at school.
- Staff should act as good role models in their use of digital technologies, the Internet and mobile devices
- In lessons, where Internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Where pupils are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need.
- Promoting the use and discussion of new technology and how being safe online applies to these technologies.

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 online 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
- Our weekly bulletin
- Parents/Carers evenings
- Parent drop-in sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant websites/publications
  e.g. swgfl.org.uk
  www.saferinternet.org.uk/
  http://www.childnet.com/parents-and-carers
  https://www.somerset.org.uk/sites/highham/SitePages/Safeguarding.aspx

Education – The Wider Community

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

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community

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 will receive regular updates through attendance at external training events (e.g. eLims local meetings) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The Online Safety Lead 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 subcommittee/group 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 training/information sessions for staff or parents
- Being present for assemblies on online safety
- Monitoring sessions with class teachers throughout each term to discuss Computing and Online Safety

Technical – infrastructure / equipment, filtering and monitoring

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below.

The school will be responsible for ensuring that the school infrastructure 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
- All users from KS2 will be provided with a username and secure password by Computing Coordinator. Users are responsible for the security of their username and password and will be required to change their password every term.

- The "administrator" passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe).
- Technicians are 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. Staff check with Online Safety Lead and Finance before downloading to check licence logs.
- 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.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided differentiated user-level filtering and with a further level using Google accounts too.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person. This is reported to their class teacher who reports immediately to the Computing Coordinator. MyConcern is also used for logging Safeguarding incidents. Breach of data is reported to the DPO.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. AUP's are signed if wireless connection is requested. Visitors to the school are prompted to use laptops/iPads within the school to protect from accidental or malicious attempts, which might threaten the security of the school systems and data

Mobile Technologies (including BYOD)

Mobile technology devices may be school owned/provided 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.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. 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	Yes	No	No	No
Internet only	Yes	Yes	Yes	No	Yes	No
No network access	No	No	No	Yes (BYOD days)	No	Yes (Signed AUP at front office when signing in)

Staff devices:

- iPads are allocated to teaching staff and support staff.
- Laptops are allocated to teaching staff.
- iPads and laptops are used in school and outside of school.
- Personal use of technology is not allowed.
- Staff have access to the networks on laptops and internet on iPads/laptops
- Staff to have signed an AUP and read the staff induction pack.
- Staff are able to install apps onto their iPads through their Apple ID.
- If any technical issues arise, staff must log this in the office ready to give to our Technician.
- Filtering of devices take part in
- Staff are told not to have cloud services activated on their school device with their own personal accounts
- Staff are told never to store important log in or passwords details. Reminders are given every 60 days for changing passwords.
- Photographs and videos taken on staff devices can be used for Twitter (if permission granted from parent/carer) but must be deleted as soon as used.
- When a member of staff leaves the school, devices must be handed back over to the school in advance of them leaving the school, to ensure data/photographs/apps are deleted.

- Staff to take part in sessions where devices are monitored for storage of photographs/videos and saved credentials.

Personal devices:

- Technical support is not available for personal devices
- BYOD days – staff member organising ensures that AUP is signed and Internet password is not saved to the device
- Filtering on these devices are linked to the Internet
- Mobile phones cannot be used in the classroom and BYOD can be used in accordance with classroom rules set by that teacher
- Photographs or videos must not be taken on personal devices

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.
- Staff 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 pupil and parents or carers.

Data Protection

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

The school ensures that:

- We have a Data Protection Policy.
- We have paid the appropriate fee to the Information Commissioner's Office (ICO).
- We have appointed a Data Protection Officer (DPO).
- We will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.

- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools must have a Freedom of Information Policy, which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Memory sticks or other removable media must not be used in school as they cannot be password protected.

G Suites

Google Accounts are now a integral part of our learning infrastructure at school and help children prepare for their transition to Secondary School.

- Children in KS1 have their own username, but have a shared and monitored password to their accounts
- Children in KS2 have their own username and password, which is monitored by staff and is accessible at home.

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	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	*				*				
Use of mobile phones in lessons				*	*				
Use of mobile phones in social time		*			*				
Taking photos on mobile phones / cameras		*			*				
Use of other mobile devices e.g. tablets, gaming devices				*			*		
Use of personal email addresses in school or on school network		*			*				
Use of school email for personal emails				*	*				
Use of messaging apps		*			*				
Use of social media		*			*				
Use of blogs		*					*		

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.
- Users must immediately report, to the nominated person (class teacher, Online Safety Lead/Computing Coordinator/Designated Safeguarding Lead) 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 (email, social media, chat, blogs) 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.
- KS2 password and log in details will apply for Google Accounts.
- 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 and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, 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 / academy 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 associate 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

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
- As Twitter is used by all classes in the school, monitoring of Tweets takes place by the Headteacher
- Twitter is used daily as part of our monitoring. Each subject coordinator monitors Tweets and this is manageable through using specific 'hash tags'.
- The Headteacher will speak to those involved with any comments on social media sites.

The school's use of social media for professional purposes will be checked regularly by the Online Safety Group to ensure compliance with the school policies. Digital Leaders also look at Tweets across the school as part of their monitoring.

Dealing with 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 users	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 / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (e.g. 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.

Prevent

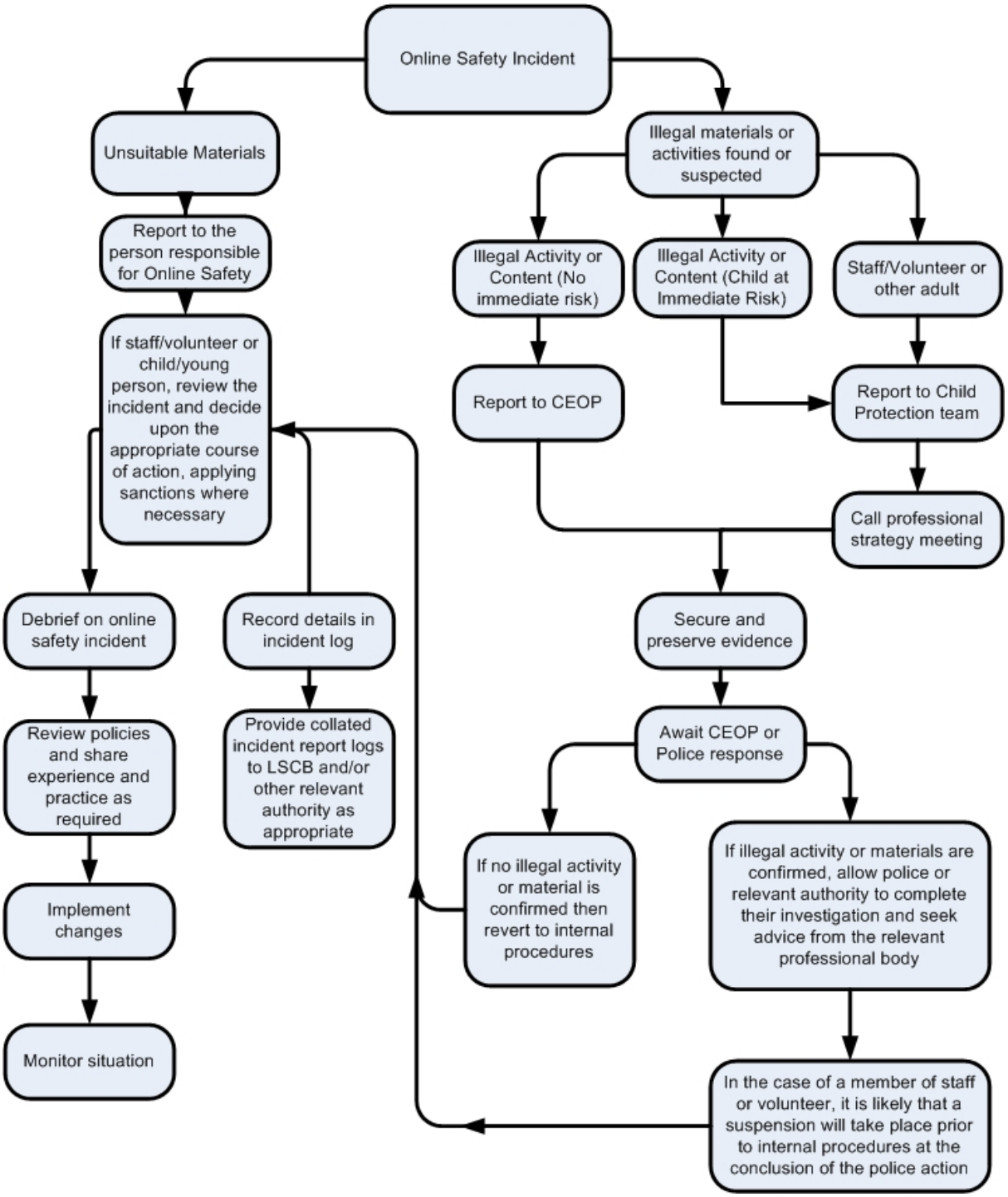
Our school works to ensure that children are safe from terrorist and extremist material when accessing the Internet. We ensure there are levels of filtering and a filtering service, which includes terms related to terrorism. Monitoring of the Internet will identify attempts to accessing this material. Children are educated of how to report any concerns to a trusted adult, at home and at school.

The Prevent Duty - 2015

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

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) 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 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
    - 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.

Our flowchart, which is displayed in every classroom and office space within the school, demonstrates the actions we would take when dealing with any incidents and who we would contact. Please see flowchart attached:

Online Safety Advisory Incident flowchart

Online Incident

Illegal Activity or Material found or suspected

Reported by broadband/filter provider

Reported by user at school

If possible, turn off screen/ isolate device

Inform Safeguarding Officer → Headteacher Chair of Governors

Inform Police/CEOP

Illegal means something against the UK Criminal Law such as:

Creating, downloading or distributing child sexual abuse images (Further advice http://bit.ly/SICSXTA4S)

Inciting race , homophobic, religious hatred or other hate crime

Content

Inform www.iwf.org.uk

Activity

Secure Evidence

Disable access

Child(ren)

Instigator

Disciplinary sanctions according to school policy

Victim

Contact ESA for child; legal advice for staff; and identify outside support including appropriate counselling

Staff

Instigator

Contact LADO / HR Disciplinary sanctions according to school policy

eLIM Support Services for Education SSE

Further support and training can be obtained by contacting: elimadmin@somerset.gov.uk

Local Contact Details

Schools Designated Safeguarding Lead:	Mrs Ann Edwards (DSL) Mrs Joanne Stewart (DDSL) Mrs Jane Rosser (HT & DDSL)
School Online Safety Coordinator:	Mrs Kayleigh Drew
Safeguarding / Online Safety Governor:	Mrs Rupert Little
LADO and Education Safeguarding Advisor (ESA):	Somerset Direct 0300 1232224

Professional Online Safety Helpdesk
0344 381 4772
helpline@saferinternet.org.uk

Harmful/Inappropriate activity or material found or suspected

Incident could be:

- Upsetting or bullying through technology
- Accessing websites against school policy
- Using personal device in class without permission

Child(ren)

Victim

Cyberbullying

- Always listen, record and report
- Capture evidence
- Record and act according to anti-bullying policy

Inappropriate Content

- Turn off/minimise screen, isolate device
- Ask another adult to review with you
- Ensure site/images are added to school filtering system and report to reportharmfulcontent.online
- Review incident with child(ren) if appropriate
- Record and inform parents

Inappropriate Gaming

- Record impact on child
- Discuss with parents

Radicalisation and Extremism

- Assess nature and extent of risk
- Record and report http://www.somerset.gov.uk/health-and-wellbeing/prevent-in-somerset
- Develop appropriate support for child(ren)

Instigator

Cyberbullying including unacceptable contribution to a webpage, blog, social network, app or text

- Capture screen shot as evidence including the name of the contributor
- Delete, or ask child (ren) to delete the contribution
- Discuss contribution with child(ren) involved as appropriate
- Take action according to school's anti-bullying policy including discussing contribution with child(ren) involved and informing parents as appropriate
- In serious incidents consider informing the Child Protection Officer

Deliberate searching for and sharing of inappropriate content

- Identify child(ren) involved, with support from technician, if school device
- Confiscate and use right to search if personal device
- Record and take action according to school's behaviour policy
- Inform parents

Staff

Victim

Adult(s) as Instigator

- Contact the person involved and administrator where a closed group, invite into school to discuss
- Request the offending material be removed
- Inform governors and consider written communication
- Provide support
- Report to website/ social network

If there is no resolution, or you need help, contact the **Professional Online Safety Helpline**

Child(ren) as Instigator

- Contact the child(ren) involved
- Request the offending material be removed
- Inform the parents
- Establish appropriate restorative action
- Provide support
- Report to website/ social network

If there is no resolution, or you need help, contact the **Professional Online Safety Helpline**

Instigator

Child as Victim

If a member of staff has:

- *Behaved in a way that has, or may have harmed a child*
- *Possibly committed a criminal offence*
- *Behaved towards a child in a way which indicates s/he is unsuitable to work with children*

Review evidence and **Contact LADO**

- Follow school disciplinary procedures and contact HR officer
- Where Head teacher is involved immediately contact Chair of Governors

Instigator

Staff as Victim

- Refer to the signed, Acceptable Use Agreement/ Professional Code of conduct
- Follow school disciplinary procedures and contact HR officer
- Contact Chair of Governors

Record as a **child protection concern** and/or separate online safety incident according to school policy

Debrief: What do we need to change for the future? Staff training, Online safety teaching, Parental Engagement, Review procedures and policies, Review of the filtering provision

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 will be dealt with through normal behaviour / disciplinary procedures as follows:

	Actions / Sanctions								
Pupil Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer to Headteacher / Principal	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 detention / 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 use of non-educational sites during lessons						X	X		
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X		X			X			X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X		X			X	X		X
Unauthorised downloading or uploading of files									
Allowing others to access school / academy network by sharing username and passwords					X	X	X	X	
Attempting to access or accessing the school / academy network, using another student's / pupil's account					X	X	X	X	
Attempting to access or accessing the school / academy network, using the account of a member of staff			X		X	X	X	X	

Corrupting or destroying the data of other users	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						X	X	X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school	X						X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system	X						X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X						X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X						X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X						X	X	X

Actions / Sanctions

Staff Incidents

	Refer to line managerr	Refer to Headteacher	Refer to Local Authority / HR	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	X				X
Inappropriate personal use of the internet / social media / personal email	X					X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X				X		
Careless use of personal data e.g. holding or transferring data in an insecure manner		X				X		

Deliberate actions to breach data protection or network security rules		X				X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		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
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X				X	X	X
Actions which could compromise the staff member's professional standing		X				X	X	X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X				X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system		X				X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X	X	X
Deliberately accessing or trying to access offensive or pornographic material		X		X		X	X	X
Breaching copyright or licensing regulations		X	X			X	X	X
Continued infringements of the above, following previous warnings or sanctions		X				X	X	X

NB from Headteacher: Each incident is classed as unique and will be assessed against these sanctions above.