Malmesbury C of E Primary School

Company Number 08483768

Online Safety Policy

To be read in conjunction with

Code of conduct for Staff

Data Policy Incorporating General Data Protection Regulation and Freedom of Information

Policy on Personal Use of Social Media by Teaching and Support Staff

Version: 1.2

Issue date: July 2018

Review date: July 2023

Date of next policy review: July 2024

Malmesbury C of E Primary School
Tetbury Hill
Malmesbury
Wiltshire
SN16 9JR
Tel: 01666 823514

Head teacher: Stephen Heal

E-mail: admin@malmesbury-pri.wilts.sch.uk
Website: www.malmesburyprimaryschool.co.uk

Contents

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by the Head teacher (DSL), ICT subject leader and governors of the curriculum committee.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Board of Directors	
The implementation of this Online Safety policy will be monitored by the:	*Senior Leadership Team*
Monitoring will take place at regular intervals:	*Every year*
Curriculum Governors Sub Committee will receive a report on the implementation of the Online Safety Policy.	*Every year*
The Online Safety Policy will be reviewed every year. An annual child-protection audit is done in school and online safety is part of this; if this highlights any dangers then a review of the whole policy should be undertaken. The next anticipated review date will be:	*July 2023*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*Designated Officer for Allegations (formerly LADO) if an employee has behaved in a way which could have harmed a child.* *Social Services and/or* *Police as appropriate.*

The school will monitor the impact of the policy using:

- Logs of reported incidents using CPOMS
- Monitoring logs of internet activity (including sites visited) / filtering (Oaford)
- Systematically checking the schools filtering system (yearly)
- Annual Child Protection Audit

Scope of the Policy

This policy applies to all members of the *school* community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) 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 Head teachers to such extent as is reasonable, to regulate the behaviour when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This would include 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. 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 (Directors):

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 / Board* has taken on the role of *Online Safety Governor*. This person is Paula Muir-McLeod. The role of the Online Safety *Governor* will include:

- Receiving reports on online safety incident log
- reporting to the Governors as part of our year safeguarding audit

Head teacher and Senior Leaders:

- The *Head teacher* has a duty of care for ensuring the safety (including online safety) of members of the school community. The Online safety officer (Head Teacher) will be taken by the Designated Safeguarding Lead (DSL) and supported by the Deputy Designated Safeguarding lead (The Deputy Head).
- The Head teacher and Deputy Head 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 HR / other relevant body* disciplinary procedures).
- *The Head teacher and Deputy are responsible for ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.*
- *The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the Online Safety Co-ordinator / Officer.*

Online Safety Coordinator / Officer:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- 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 which are logged on CPOMS and will be reviewed annually
- Establish a Filtering and Monitoring staff group who will complete a monitoring checklist of the filtering system annually (see Appendix 2)

Network Manager / Technical staff:

Oakford are Network managers and Technical support. Further technical support for apple products is provided by Computers. They 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 / School Group / other relevant body* Online Safety Policy / 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.
- *the filtering policy (Oakford have own policy in place), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.*
- 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 / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Head teacher or Deputy Head.*
- *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 Code of Conduct and Social Media policies.
- they report any suspected misuse or problem to the Head teacher or Deputy head for investigation
- all digital communications with students / 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
- 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 students / 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/ Deputy 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
- cyber-bullying

Students / Pupils:

- are responsible for using *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
- 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 cyber-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

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, website and information about national safety campaigns. 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
- their children's personal devices in school (Yr 6 phones to be handed in to teachers and placed in drawer)

Policy Statements

Education – Students / 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 is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing and PHSRE and is regularly revisted
- Key online safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities (online safety week)
- Students / pupils will be helped to understand the need for the pupil Acceptable Use Agreement and are encouraged to adopt safe and responsible use both within and outside school.
- In lessons where internet use is pre-planned, it is best practice that students / 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 students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

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

- *Regular letters, newsletters, web site,*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Parents evenings and online videos*

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:

- Online safety training will be given to staff yearly as part of safeguarding training.
- Further online training updates will be given when updates are needed

Training – Governors / Directors

The lead governor for safeguarding will take part in online awareness sessions. This will be in the form of participation in school / training / information sessions for staff or parents.

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 academy 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. It is also important that the managed service provider is fully aware of the *School* Online Safety Policy / Acceptable Use Agreements.

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
- 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.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other persons) must also be available to the on-site IT technician (Judith Brown) nominated senior leader and kept in a secure place.
- On site technician is responsible for ensuring the license and dispatching of software for iTunes apps across the school site.
- Oakford is responsible for ensuring that the number of licences purchased do not exceed the number of software installations on window machines.
- 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 – see flow diagram in appendices
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.

- The school has provided enhanced / differentiated user-level filtering allowing staff and pupils to have different levels of filtering.
- An appropriate system is in place (See GDPR policy) for users to report any actual security breach.
- 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. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.
- Staff are allowed to download programs to support the teaching of lessons as long as these are legally obtained. If staff are unsure of programs they should always ask, Support Tech, Deputy Head or the school computer support as to the validity of the program
- Guests who have had the necessary checks in line with our child protection policy can be given access to the school wifi via the guest login
- An agreed policy is in place (See data protection and GDPR policy) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices and the use of personal data.

Mobile Technologies (including BYOD/BYOT)

All mobile devices that have access to the school network are owned by the school and have the necessary passwords and firewalls installed. No privately owned mobile device with the exception of the Head, Deputy and School IT coordinator will have access to the school Wi-Fi and these devices do not have access to the Network. Personal devices can only be used in certain locations within the school (with the exception of the above) and all staff must adhere to the Social Media and Acceptable Use Polices.

School owned / provided devices:

- iPads and iPods are allocated to year groups or centrally stored in the Media suit and not allocated individuals with the exception of year 6. In year 6 each child is allocated an iPad, which is for school based work only (see appendix for Year 6 agreement). Use is monitored and network firewalls are in place.
- All pupil mobile devices are to be used as an educational tool and will be used as part of a lesson or research based activity. The pupils will be monitored and supervised when using these mobile devices.
- All devices are firewalled. Pupil machines only have access to the pupil share. Staff can access the staff shares.
- Staff can install apps on individual machines using the school account. Only the administrator or technical support can install apps across the site.
- Technical support is given by Oakford for all devices across the school. Western Computers provides technical support for apple products. School I.T support is provided by Judith Brown who liaises with the above companies.
- Filtering of devices is provided by Oakford.
- Data Protection is outlined in our GDPR and Data Protection Polices.
- All parents /carers are asked for permission to have pictures taken, stored and/or shared. This is outlined in GDPR and Data Protection Polices.

- All computers are cleared of data including passwords and sensitive information and restored to original settings. When a device reaches the end of its working life it is recycled at an authorised ADISA Certified company.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / 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 students / 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 students / pupils are published on the school website / social media / local press. This is done on entry to the school.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims using school, 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 students / 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 student / pupil and parents or carers.

Data Protection (Please see Data Protection Policy for more detail)

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.

As a school we commit to:

- Holding 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.
- Every effort being made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data being fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”. (see data protection policy)
- Having a Data Protection Policy
- Being registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

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.
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications (see Code of Conduct for staff - points 39 -42)

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	Students / 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 /	✓						✓	
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		✓						✓
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 – 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 students / pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.
- Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use if needed within the curriculum.
- Students / 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 (See Social Media Policy for more detail)

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 13minimize 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 students / 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 /academy 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 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
- As a general rule, we do not engage with postings about the school on social media unless they are perceived to be a personal data breech, involve bullying of a member of staff or a child protection issue.

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:

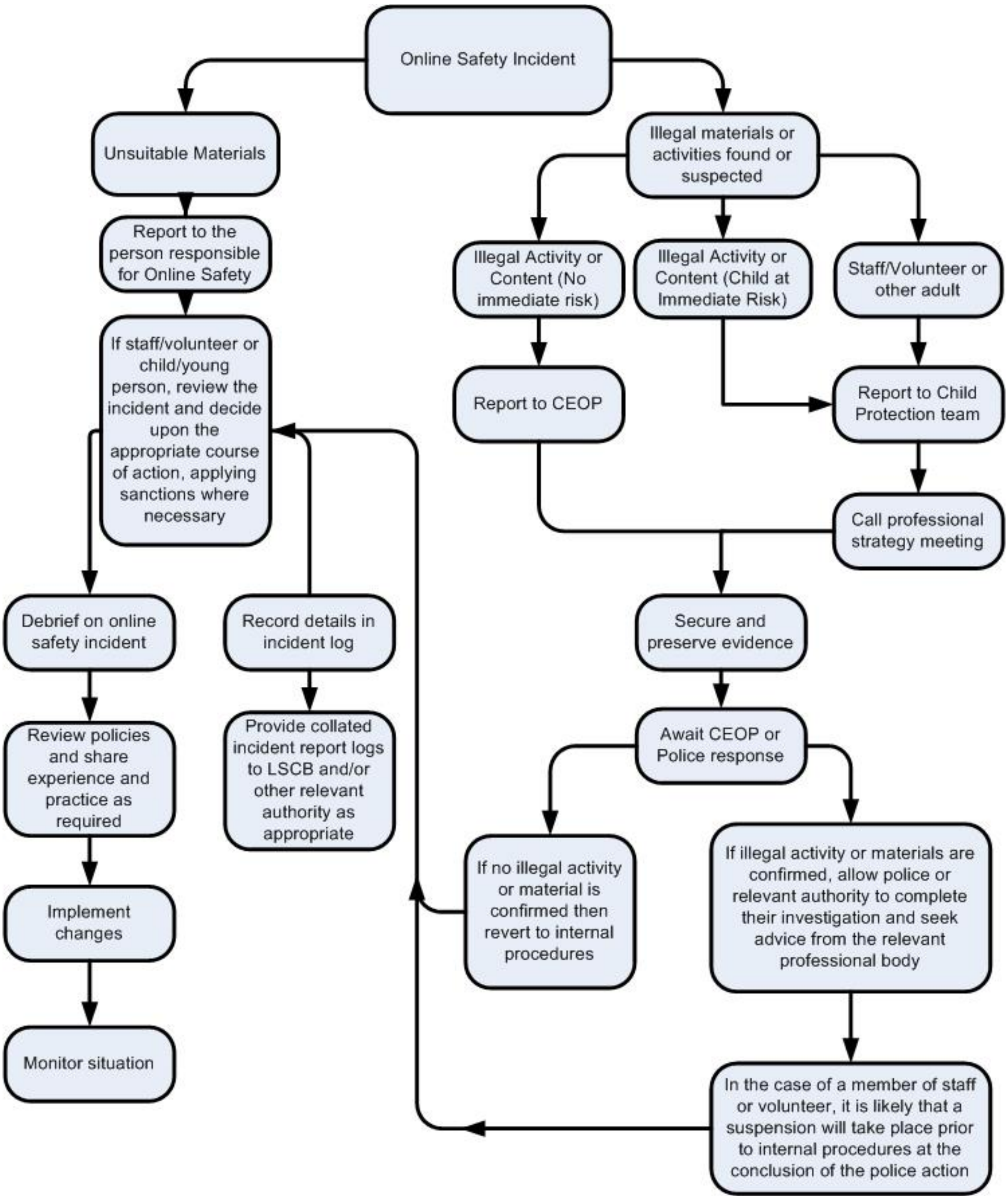
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child 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					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).

Online 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.



Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

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.
- 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 Group or national / local organisation (as relevant).
    - 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 will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils Incidents	Refer to class teacher	Refer to member of SLT	Refer to Head teacher /DSL/DDSL	Refer to Police	Refer to technical support staff for action re filtering / security etc.	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	X	X
Unauthorised use of non-educational sites during lessons	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	X
Unauthorised downloading or uploading of files	X	X			X	
Attempting to access or accessing the school network, using the account of a member of staff			X			X
Corrupting or destroying the data of other users	X					X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X?	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident			X			
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X

Staff Incidents	Refer to line manager	Refer to Head teacher	Refer to HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	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	X
Breach of the social media and code of conduct policies		X	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			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	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		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			
Actions which could bring the school 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 ’s filtering system	X	X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X			X
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X
Breaching copyright or licensing regulations		X			X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X

Logging of incidents in reference to Internet Safety

Logging of incidents with children

All incidents that involve children and internet safety will be logged via CPOMs. These should be logged by the member of staff dealing with the incident, DSL or DDSL. These incidents are anything to do with the internet either at home or in school. The cyber incident button should be checked when reporting. If any member of staff feels a child is at immediate risk, then you should report the incident in person.

Logging of incidents with staff

Any incident involving staff should be reported to the DSL or DDSL. These will then be assessed against the flow chart. These may be held on file as a low-level concern. Low level concerns are not place on any member of staffs permanent record.

Appendices

1. Meeting Digital Standards in Schools. Filtering+and+Monitoring+Standards+

2. Malmesbury CE Primary School Filtering Test Internet filtering test 120623.docx

3. Student / Pupil Acceptable Use Agreement Template – for Year 5 and 6

4. Student / Pupil Acceptable Use Policy Agreement Template – for Year 3 and 4 (Foundation / KS1)

5. Student / Pupil Acceptable Use Policy Agreement Template – for Year 3 and 4

6. Responding to incidents of misuse – flow chart

7. Record of reviewing devices / internet sites (responding to incidents of misuse)

8. System for requests for filtering changes

9. Legislation

10. Links to other organisations or documents

11. Glossary of Terms

Pupil Acceptable Use Agreement Template

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users.

Acceptable Use Policy Agreement Yr 5 and 6

I understand that I must use computing technologies in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will check how I use my devices in school.
- I will be aware of "stranger danger", when I am on-line.
- I will not share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, where I go to school).
- I will immediately report anything that makes me feel uncomfortable when I see it on-line to my teachers if in school or parents outside of school.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the *school's devices* are intended for educational use and that I will not use them for games, sharing files, broadcasting or watching videos (e.g. YouTube) unless I have permission.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or hurtful language.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

- I will not **try to** access any materials which may cause distress to others.
- I will immediately report any damage or faults to the computers/tablets; however this may have happened.
- I will not try to alter any settings on computers and tablets including downloading programmes.
- I will not use social media sites in school at any time.
- Personal mobile devices are not allowed to be used in school at any time.
- **Year 6 only –** If bringing a mobile phone into school it must be handed to the teacher at the start day.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- When I am using the internet to find information, I should take care to check that the information that I access is accurate.

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

- I understand that the *school* also has the right to take appropriate action against me if I am involved in incidents of misbehaviour, that affect people in school (examples would be cyber-bullying, use of images or personal information).
- I understand that if I do not keep to this Acceptable Use Policy Agreement, I may lose the right to use the school internet, and my school might contact my parents.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the *school* devices;
- I use my own equipment out of the school in a way that is related to me being a member of this *school such as* communicating with other members of the school via mobile devices and accessing the school website.

Name of Student / Pupil: ....

Group / Class: ....

Signed: ....

Date: ....

Parent / Carer Countersignature ....

Acceptable Use Policy Agreement Yr 3 and 4

I understand that I must use computers in a sensible way, so that there is no risk to my safety or to the safety of others.

For my own personal safety:

- I understand that the school will check how I use the computers and tablets in school.
- I will be aware of "stranger danger", when I am on-line.
- I will not share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, where I go to school).
- I will tell someone (parent or teacher) if I see something that makes me feel uncomfortable.

I understand that everyone has equal rights to use technology (computers and tablets):

- I understand that the *school's devices* are intended for educational use and that I will not use them for games, video broadcasting or watching (e.g YouTube) unless I have permission.

I will act as I expect others to act toward me:

- I will not deliberately (on purpose) change or delete someone else's work without their permission.
- I will be polite when I communicate with others.
- I will not take or share pictures or videos of anyone without their permission.

I recognise that the school has a responsibility to keep the school's computers working and to keep everyone safe.

- I will not **try to** go on any websites which may upset others.
- I will report any damage or faults to the computers/tablets; however this may have happened.
- I will not try to alter any settings on computers and tablets.
- I will not use social media sites (e.g facebook) in school at any time.
- Personal mobile devices are not allowed to be used in school at any time.

When using the internet for research or recreation, I recognise that:

- When I am using the internet to find information, I should take care to check that the information is accurate.

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

- I understand that the *school* also has the right to take appropriate action against me if I am involved in incidents of misbehaviour, that affect people in school (examples would be cyber-bullying, use of images or personal information).
- I understand that if I do not keep to this Acceptable Use Policy Agreement, I may lose the right to use the school internet, and my school might contact my parents.

Please complete the sections below to show that you have read, understood and agree to these rules If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student / Pupil Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the *school* devices;
- I use my own equipment out of the school in a way that is related to me being a member of this *school such as* communicating with other members of the school via mobile devices and accessing the school website.

Name of Student / Pupil: ....

Group / Class: ....

Signed: ....

Date: ....

Parent / Carer Countersignature ....

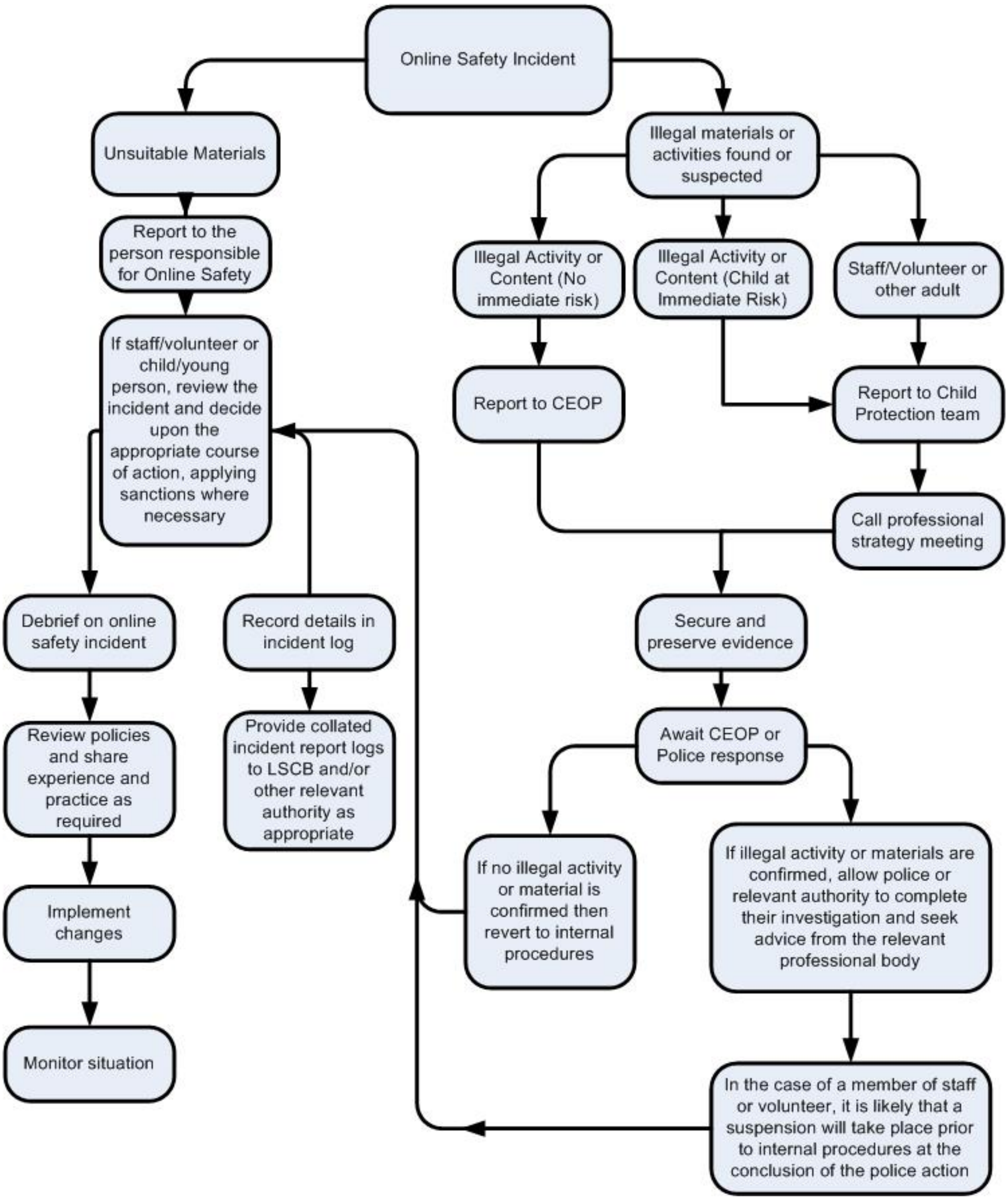
Pupil Acceptable Use Policy for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or teaching assistant if I want to use the computers / tablets.
- I will only use activities that a teacher or teaching assistant has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or teaching assistant if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or teaching assistant if I see something that upsets me on the screen.
- I know that if I break the rules, I might not be allowed to use a computer / tablet.
- I will not share personal information about myself with people I don't know on line.

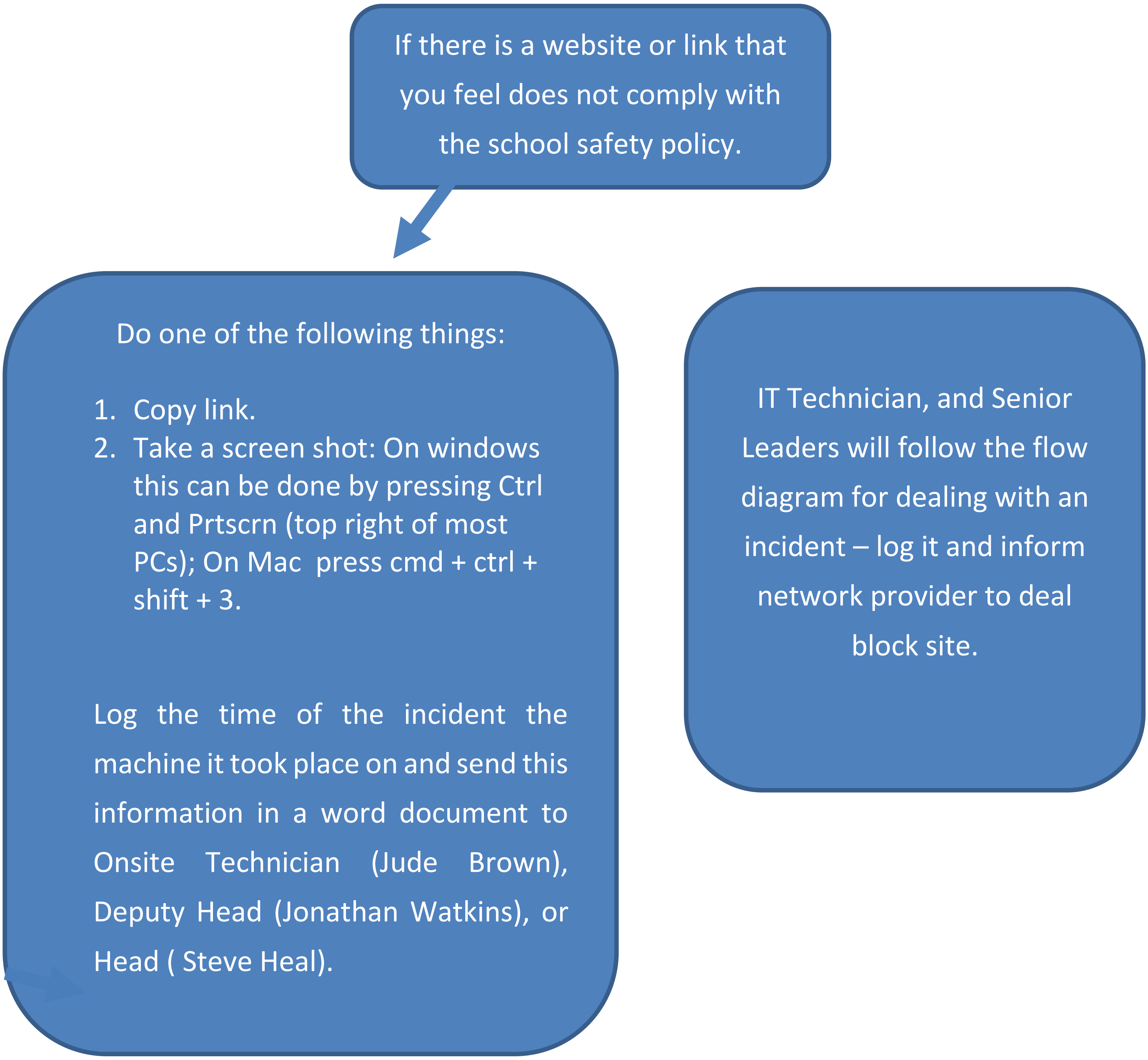
Signed (child): ………………………………………………………

Responding to incidents of misuse – flow chart


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

System for requests for filtering changes

to be used in conjunction with Responding to incidents of misuse – flow chart



If there is a website or link that you feel does not comply with the school safety policy.

Do one of the following things:

1. Copy link.
2. Take a screen shot: On windows this can be done by pressing Ctrl and Prtscrn (top right of most PCs); On Mac press cmd + ctrl + shift + 3.

Log the time of the incident the machine it took place on and send this information in a word document to Onsite Technician (Jude Brown), Deputy Head (Jonathan Watkins), or Head (Steve Heal).

IT Technician, and Senior Leaders will follow the flow diagram for dealing with an incident – log it and inform network provider to deal block site.

Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance 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 Head teachers, to such extent as is reasonable, to regulate the behaviour of students / 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 Head teachers (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

The following links may help those who are developing or reviewing a school online safety policy:

UK Safer Internet Centre

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

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

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
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
SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
Connectsafely Parents Guide to Facebook
Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship 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
SWGfL - Guidance for Schools on Cloud Hosted Services
LGfL - Data Handling Compliance Check List
Somerset - Flowchart on Storage of Personal Data
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

Somerset - Questions for Technical Support
NEN - Guidance Note - esecurity

Working with parents and carers

SWGfL Digital Literacy & Citizenship curriculum
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.