Cabot Primary School

Learn together, respect each other, achieve forever

Online Safety Policy

Adopted: November 2017

Review Date	Details	Owned by/linked to
November 2017	New Policy	School (SIC)
November 2019		

Contents

Development, Monitoring and Review of this Policy

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

- Tom Burton - Headteacher
- Freya Heeley – ICT Lead
- Staff – including Teachers, Support Staff, Technical staff
- Governors / Board
- Parents and Carers
- Community users

Consultation with the whole school community has taken place.

Schedule for Development, Monitoring and Review

This Online Safety policy was approved by the Board of Directors / Governing Body / Governors Sub Committee on:	*November 2017*
The implementation of this Online Safety policy will be monitored by the:	*ICT Lead/ Officer / Senior Leadership Team*
Monitoring will take place at regular intervals:	*End of Term 4*
The Resources Committee of the Board of Governors will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*End of term 5*
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:	*November 2018*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*As appropriate - LA Safeguarding Officer, Academy Group Officials, LADO, 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

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated Behaviour and Anti-Bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. The monitoring of the implementation of the Online Safety Policy will be included in the role of the named governor for Child Protection and Safeguarding.

- monitoring of online safety incident logs
- reporting to Resources 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 ICT Leader.

- The Headteacher and Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR disciplinary procedures).
- The Headteacher and Senior Leaders are responsible for ensuring that the ICT Leader 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 and Senior Leaders 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. TWSIT provides school with a fully managed Internet Services the details of which can be found here: http://ict.tradingwithschools.org/internet-services-service-detail/

- The Senior Leadership Team will receive regular monitoring reports from the ICT Leader.

ICT Leader:

- leads the Online Safety issues within the Safeguarding Team
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and 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 school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

TWS IT are employed to manage the technical service provided to the school. TWS IT provide technical staff who are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety 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 is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (This is done through TWS IT services)
- 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 and remote access is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher or ICT Leader for investigation.
- 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
- they report any suspected misuse or problem to the Headteacher, Senior Leadership Team or ICT Leader for investigation and action
- 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, where possible, 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 aware of Online Safety issues and be aware of the potential for serious child protection or safeguarding issues to arise from:

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

Online Safety Group (incorporated into the responsibility of the school Safeguarding Team)

The Safeguarding Team provides a consultative group with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Board of Governors

Members of the Safeguarding Team will assist the ICT Leader with:

- the production, review and monitoring of the school Online Safety Policy and documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and 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 digital technology systems in accordance with the Pupil Acceptable Use Agreement
- 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
- 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 parent sessions, newsletters and information about national or local online safety campaign. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate usedigital and video images taken in school.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 is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum should be provided as part of Computing lessons
- Displays, in and around the school, supporting good online safety practice
- Key online safety messages should be reinforced as part of a planned programme of lessons and activities
- Pupils should be taught in all lessons to be critically aware of the materials and 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, at an age appropriate level, at 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.

  Nb. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- 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.
- 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.

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:

- Letters, newsletters, website,
- Parents / Carers coffee morning 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 (see appendix for further links / resources)

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:

- All new staff should ensure that they fully understand the school Online Safety Policy and The Code of Conduct.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- This Online Safety Policy and its updates will be presented to and discussed by staff via email and in staff meetings.
- The ICT Leader Safety Coordinator will offer guidance or training to individuals as required. Online Safety BOOST includes an array of presentation resources that the Online Safety coordinator can access to deliver to staff (https://boost.swgfl.org.uk/) It includes presenter notes to make it easy to confidently cascade to all staff

Training – Governors / Directors

Governors should take part in online safety training and awareness sessions, with particular importance for those who are members of any subcommittee involved with online safety, health and safety or 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

Technical – infrastructure / equipment, filtering and monitoring

TWSIT provides school with a fully managed Internet Services the details of which can be found here: http://ict.tradingwithschools.org/internet-services-service-detail/

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

- The TWSIT Internet Services include Specialist educational filtering systems meeting 360 Degree e-safety standard level 3 prevent access to illegal and inappropriate material.
- There will be regular reviews and audits of the safety and security of school technical systems
- TWS will be the “master / administrator”
- Servers, wireless systems and cabling must be securely located and physical access restricted
- The School and TWS IT is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content 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. All filtering changes are done by TWSIT following a support request. TWSIT will review the site before making any changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- School technical staff regularly monitors and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. TWS IT can provide a large array of web filter reporting tools available including ability to report to staff on a daily/weekly or monthly basis when a certain search criteria has been searched for (can be used to highlight welfare issues or as part of the PREVENT strategy)
- 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. The systems are all protected by Defender Anti-Virus Software.

- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems. A range of Guest and Supply staff accounts have been created on the network for temporary use. The relevant levels of network access and filtering are applied to these accounts. i.e Guest accounts would allow users access to (filtered) internet use but not school network drives or material stored on them.

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.

- 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 via the school registration forms before photographs of pupils are published on the school website / social media / local press
- 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 or made publicly available on social networking sites. Parents / carers are routinely reminded, (eg at celebration assemblies) not take photographs of children other than their own.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Pupil's work can only be published with the permission of the pupil and parents or carers, obtained via the copyright permission section of the pupil registration form.

Social Media

Personal Use of Social Media

Staff should not befriend former pupils *under the age of 18* on any social media site. Connecting with pupils on any form of social media which would allow unmonitored 1to1 contact is strictly prohibited.

Using Social Media on Behalf of ……

There must be a strong pedagogical or business reason for creating official School sites to communicate with pupils or others. Staff must not create sites for trivial reasons which could expose the School to unwelcome publicity or cause reputational damage.

Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

Using Social Media with Children and Young People

When creating social media sites for children and young people and communicating with them using such sites, staff members must at all times be conscious of their responsibilities; staff must always act in the best interests of children and young people.

Staff members must be alert to the risks to which young people can be exposed. Young people's technical knowledge may far exceed their social skills and awareness - they may post sensitive personal information about themselves, treat online 'friends' as real friends, be targets for 'grooming' or become victims of cyberbullying.

If children and young people disclose information or display behaviour or are exposed to information or behaviour on these sites that raises safeguarding or other concerns, appropriate authorities must be informed immediately. Failure to do so could expose vulnerable young people to risk of harm.

Staff members must also ensure that the webspace they create on third party sites comply with the site owner's minimum age requirements (this is often set at 13 years). Staff members must also consider the ramifications and possibilities of children under the minimum age gaining access to the site.

Care must be taken to ensure that content is suitable for the target age group.

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	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			

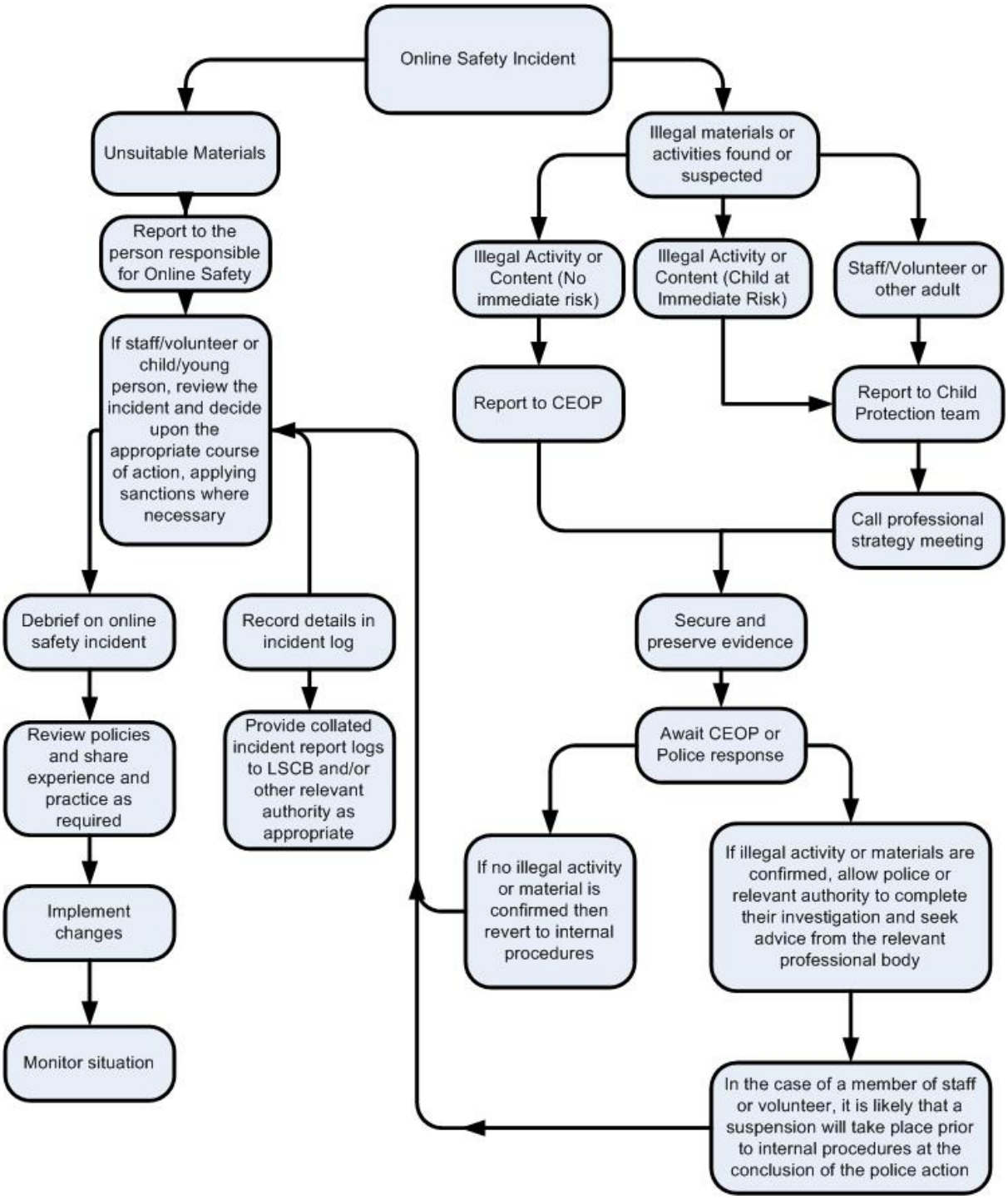
Are ‘Promotion of extremism or terrorism and Infringing copyright’ not illegal?

Responding to incidents of misuse

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

Illegal Incidents

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



Other Incidents

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

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority Group or national / local organisation (as relevant).
    - Police involvement and/or action if relevant
- **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

In the case this event, 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:

	Actions / Sanctions						
Students / Pupils Incidents	Refer to class teacher / tutor	Refer to Headteacher	Refer to Police		Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	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	x					
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	x	x					
Unauthorised / inappropriate use of social media / messaging apps / personal email	x	x				x	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x				x	
Continued infringements of the above, following	x	x				x	x

previous warnings or sanctions							
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	x				x	
Deliberately accessing or trying to access offensive or pornographic material	x	x				x	x
=							

Staff Incidents	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Refer to Headteacher, possible 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
Careless use of personal data e.g. holding or transferring data in an insecure manner				x
Deliberate actions to breach data protection or network security rules				x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x			x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x		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

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x			x
Using proxy sites or other means to subvert the school's filtering system	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
Continued infringements of the above, following previous warnings or sanctions				

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360 degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Appendices

Pupil Acceptable Use Policy Agreement Template – for younger pupils

Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will use only my class network login and password, which is secret.
- I will only open or delete my own files.
- I must not bring into school and use software or files without permission.
- I will only e-mail and open attachments from people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

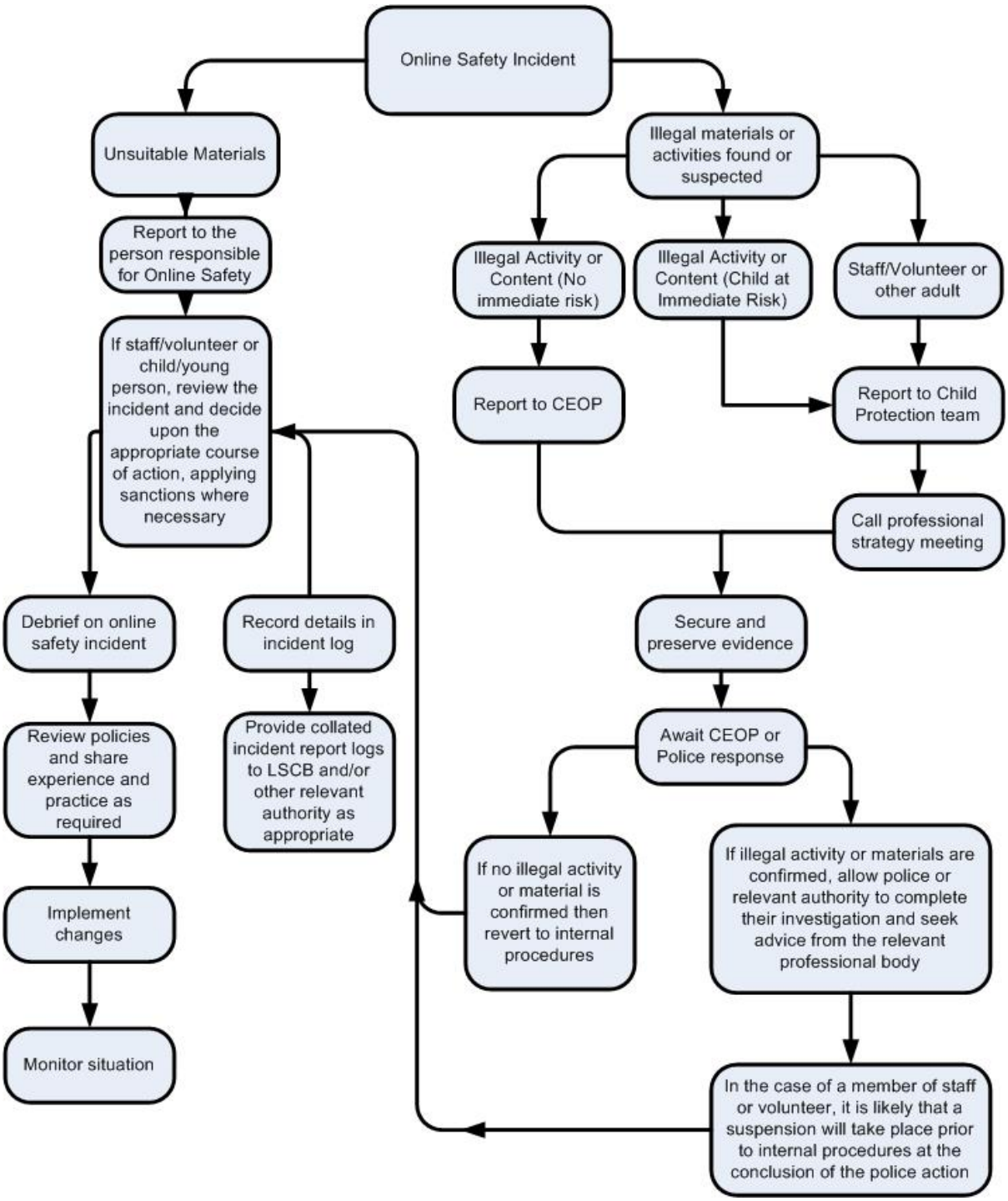
Cabot Primary School

Acceptable Use of the Internet Agreement

Please sign and return the form below:

Pupil:	Class:
Pupil's Agreement I have read and I understand the school rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and follow these rules at all times.	
Signed:	Date:
Parent's Consent for Internet Access I have read and understood the school rules for responsible Internet use and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.	
Signed:	Date:

Responding to incidents of misuse – flow chart



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

Group: .....
Date: .....
Reason for investigation: .....

.....

.....

.....

Details of first reviewing person

Name: .....
Position: .....
Signature: .....

Details of second reviewing person

Name: .....
Position: .....
Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		