Harbury CE Primary School

Online Safety Policy

Monitoring of this Policy

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

- Headteacher
- Online Safety Coordinator
- Governors
- Pupil representatives from Key Stage 2

Schedule for Monitoring

This Online Safety policy was approved by the Governing Body on:	
The implementation of this Online Safety policy will be monitored by the:	*Online safety subject leader and the Senior Leadership Team*
Monitoring will take place at regular intervals:	*At least once a year*
Governing Body will receive a report on the implementation of the Online Safety Policy as part of the Headteacher's report to governors which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
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:	*March 2021*
Should serious online safety incidents take place, the following external people/agencies should be informed:	*Adrian Over* *Jane Key* *LADO (if appropriate)* *Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Surveys of
    - pupils
    - parents / carers
    - staff (audit of skills and knowledge)

Scope of the Policy

This policy applies to all members of the school (including staff, 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 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 involved in the writing of, and responsible for the approval of, the Online Safety Policy. They are also involved in reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Subject Leader – Helen Bunce
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- communicating and reporting to Governors at a FGB meeting, ensuring Online Safety is placed on the agenda

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Leader.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The Headteacher/Senior Leaders are responsible for ensuring that the Online Safety 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 Senior Leadership Team will receive regular monitoring reports from the Online Safety Leader.

Online Safety Leader

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Technical staff

The school's network infrastructure is maintained by ICT Development Service. This covers all network management, maintenance, filtering and monitoring. Technical Staff at the school are responsible for ensuring:

- 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
- to communicate with support service employed by school (ICT Development Service) to monitor and filter the school's network and technical infrastructure
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher or Online Safety Coordinator for investigation
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- teach online safety issues in all aspects of the curriculum as part of the long term planned overview

Designated Safeguarding Lead

The Designated Safeguarding Leads are trained in Online Safety issues and are aware of the potential for serious safeguarding issues to arise from:

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

Online Safety Group

The school has an Online Safety Group made up of:

- Online Safety Coordinator
- Headteacher
- Pupil representatives from Key Stage 2
- Online Safety Governor

The Online Safety Group meets formally every term. Each term, there will be fortnightly meetings with the pupil representatives. The members of this group will assist the Online Safety Coordinator with:

- regular reporting to the Governing Body
- the review and monitoring of the school's online safety documents, including the Parent and Pupil Acceptable Use Policy
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting parents / carers and the pupils about the online safety provision

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
- are expected to know, understand, and adhere to, policies on the use of mobile devices and digital cameras. They should also know and understand the law on the taking / use of images and on cyber-bullying.
- 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 outside 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. They are expected to sign an Acceptable Use Policy annually and attend the Online Safety events carried out at school. Parents and carers are encouraged to support the school in promoting good online safety practice. Parents and carers are expected to sign an acceptable use policy annually and abide by its content.

Community Users

Members of the wider community will sometimes be using the infrastructure of the school's network. This includes volunteer workers and external community groups. They will be made aware of the Acceptable Use Policy when signing in to the school. They will not be granted internet access through the school's Wi-Fi on their own personal devices. On occasions where Wi-Fi access is necessary, it will be under the supervision of the Headteacher or Senior Leadership Team.

Policy Statements

Education – Pupils

The education of pupils in online safety is 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 across all areas of the curriculum and is the responsibility of all staff. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- The planned online safety curriculum is discretely provided as part of Computing / PSHE lessons and should be regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies throughout the year, including Safer Internet Day
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils are 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 act as good role models in their use of digital technologies, the internet and mobile devices

Education – Parents / Carers

Parents and carers have a key role to play in their children's online safety education. The school provides information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters and the school website's Online Safety section
- Parents / Carers information evenings
- Safer Internet Day
- Reference to these websites and social media accounts – www.internetmatters.org, www.facebook.com/stayingsafeonline

Training – Staff

The school ensures that all staff receive online safety training and understand their responsibilities as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety training is available to all staff
- an audit of the online safety training needs of new staff on arrival
- all new staff receive online safety training as part of their induction programme. This ensures that they fully understand the school's Online Safety documents
- the Online Safety Coordinator receives regular updates at external training events, including termly attendance at the Subject Leaders' Meetings
- the Online Safety Coordinator provides advice, guidance and training to individuals as required

Training – Governors

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

- Attendance at training provided by the Local Authority
- Participation in school training / information sessions for staff or parents
- Participation and monitoring of assemblies / lessons centred on Online Safety

Technical – infrastructure / equipment, filtering and monitoring

The school is 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. All of the school's infrastructure is externally maintained by ICT Development Service. The systems will follow these guidelines:

- Servers, wireless systems and cabling are securely located and physical access is restricted
- All users have clearly defined access rights to school technical systems and devices
- All users are provided with a username and secure password by welearn365.com who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be encouraged to change their password every year.

- The administrator passwords for the school ICT system, used by the Technical Staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place (One Drive)
- Internet access is filtered for all users through Smoothwall and Digital Safeguarding
- Local Authority technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. The school receives a monthly report on usage that is shared with the online safety Leader and technical support.
- 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.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Staff may only use USB memory sticks if safely encrypted. Communication via email is only through the school’s welearn365 account and use of OneDrive is encouraged.

Mobile Technologies

Mobile technology devices are school owned and include: tablet, laptops or other technology that usually has the capability of utilising the school’s wireless network. These devices then have access to the wider internet which includes the school’s learning platform and other cloud based services such as email and data storage. All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school’s Online Safety education programme.

- The school allows:

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

Use of digital and video images

Staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Digital images may remain on the internet forever and can cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

See Use of Images Guidance for children and young people in Warwickshire (2014). Further information on all aspects of child protection or safeguarding is available from:

Adrian Over, Warwickshire Education Safeguarding Children Manager
Tel: 01926 742525 Mobile: 07771 552315

Communications

The following table shows how the school currently considers the benefit of using technologies for education:

	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				✓				✓
Use of other mobile devices e.g. tablets, gaming devices		✓					✓	
Use of personal email addresses in school or on school network		✓						✓
Use of school email for personal emails		✓						✓

Use of messaging apps		✓						✓
Use of social media		✓						✓
Use of blogs		✓					✓	

When using communication technologies we consider the following as good practice:

- The official school email service is used for all professional email communication. Users are aware that email communications are monitored.
- Class Dojo is used as a communication tool between parents and teachers and must always be done so appropriately
- 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.
- Users must report any suspicious / unexpected email and check the sender before opening or clicking on a link

Social Media - Protecting Professional Identity

The school has a Social Media Use Agreement in place for all staff. This includes the following:

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

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer.
- 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

Unsuitable / inappropriate activities

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	

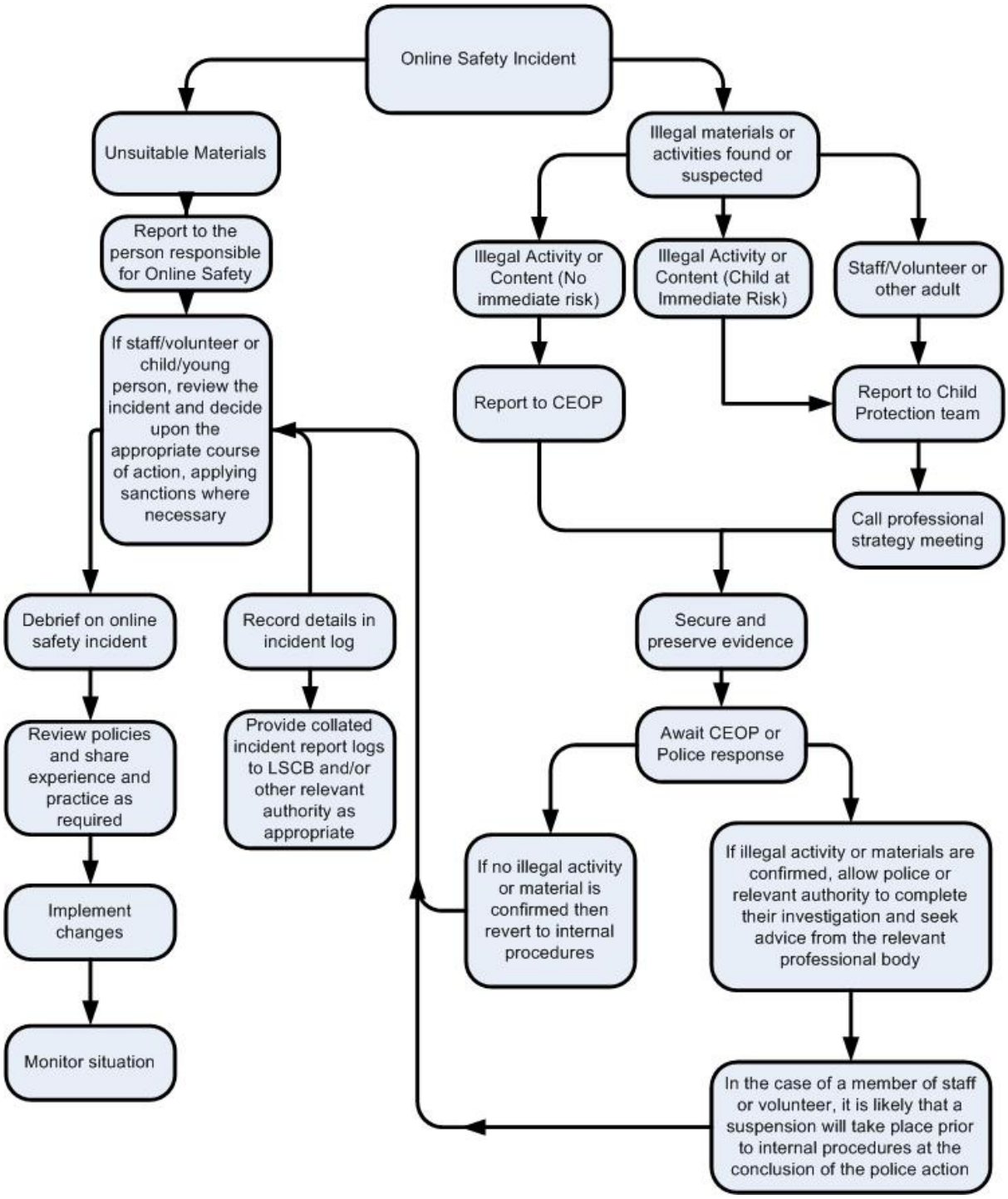
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others 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

The flowchart below explains the process of dealing with any reports of misuse.

Illegal Incidents

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


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
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
Monitor situation
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

School Actions & Sanctions

See behaviour policy for pupil incidents.

Actions / Sanctions

Staff Incidents	Refer to line managerr	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal		X	X	X				
Inappropriate personal use of the internet / social media / personal email		X						
Unauthorised downloading or uploading of files		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						
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						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X						
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students / pupils		X	X					
Actions which could compromise the staff member's professional standing		X						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school / academy		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
Breaching copyright or licensing regulations		X						
Continued infringements of the above, following previous warnings or sanctions		X						