



HAWKESLEY CHURCH PRIMARY ACADEMY

E-Safety Policy

“Let your light shine” Matthew 5:16

Background and Rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual’s consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive or addictive use which may impact on social and emotional development and learning

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children about the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Section A - Policy and leadership

This section begins with an outline of the **key people responsible** for developing our E-Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school.

It goes on to explain **how we maintain our policy** and then to outline **how we try to remain safe while using different aspects of ICT**.

A.1.1 Responsibilities: e-safety coordinator

Our e-safety coordinator is the person responsible to the Head Teacher and Local Academy Board Members for the day to day issues relating to e-safety. The e-safety coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- provides training and advice for staff
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reviews weekly the output from monitoring software and initiates action where necessary
- attends relevant meetings and committees of Governing Body
- reports regularly to Senior Leadership Team
- receives appropriate training and support to fulfil their role effectively

A.1.2 Responsibilities: Local Academy Board Members

Local Academy Board Members are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the School Improvement Board Members receiving regular information about e-safety incidents and monitoring reports. A member of the School Improvement Board has responsibility for ICT and has also taken on the role of e-safety member which involves:

- *meetings with the E-Safety Co-ordinator when required*

A.1.3 Responsibilities: Head Teacher

- The Head Teacher is responsible for ensuring the safety (including e-safety) of all members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Co-ordinator
- The Head Teacher and another member of the senior management team will be familiar with the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff, including non-teaching staff. (see flow chart on dealing with e-safety incidents (included in section 2.6 below) and other relevant Local Authority HR / disciplinary procedures)

A.1.4 Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:

- they safeguard the welfare of children and refer child protection concerns using the proper channels: **this duty is on the individual, not the organisation or the school.**
- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school's Acceptable Use Agreement for staff
- they report any suspected misuse or problem to the E-Safety Co-ordinator
- they undertake any digital communications with pupils in a fully professional manner and only using official school systems
- they embed e-safety issues in the curriculum and other school activities, also acknowledging the planned e-safety programme (See section C)

A.1.5 Responsibilities: ICT technician

The ICT Technician is responsible for ensuring that:

- the school's ICT infrastructure and data are secure and not open to misuse or malicious attack
- the school meets the e-safety technical requirements outlined in section B.2.2 of this policy (and any relevant Local Authority E-Safety Policy and guidance)
- users may only access the school's networks through a properly enforced password protection policy as outlined in the school's e-security policy
- shortcomings in the infrastructure are reported to the ICT coordinator or head teacher so that appropriate action may be taken.

A.2.1 Policy Scope

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

The Education and Inspections Act 2006 empowers head teachers/head of school, 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 e-safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.

The school will deal with such incidents using guidance within this policy as well as associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

A.2.2 Acceptable Use Agreements

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

Acceptable Use Agreements are needed for:

- Pupils (EYFS/KS1 / KS2)
- Staff (and volunteers)
- Community users of the school's ICT system

Acceptable Use Agreements are introduced at the beginning of each new academic year. Children who join midyear will receive a copy of the agreement with their home school diary.

All employees of the school and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy.

Community users sign when they first request access to the school's ICT system.

A.2.3 Self Evaluation

Evaluation of e-safety is an ongoing process and links to other self evaluation tools used in school in particular to pre Ofsted evaluations along the lines of the Self Evaluation Form (SEF). The views and opinions of all stakeholders (pupils, parent, teachers ...) are taken into account as a part of this process.

A.2.4 Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context (**those in bold are illegal**) and that users should not engage in these activities when using school equipment or systems (**in or out of school**).

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 (illegal - The Protection of Children Act 1978)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- 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

Additionally the following activities are also considered unacceptable on ICT equipment or infrastructure provided by the school:

- *Using school systems to undertake transactions pertaining to a private business*
- *Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Worcestershire County Council Broadband and / or the school*

- *Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions*
- *Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)*
- *Creating or propagating computer viruses or other harmful files*
- *Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files that causes network congestion and hinders others in their use of the internet)*
- *On-line gambling and non educational gaming*
- *On-line shopping / commerce*
- *Use of social networking sites (other than in the school's learning platform or sites otherwise permitted by the school)*

If members of staff suspect that misuse might have taken place – whether or not it is evidently illegal (see above) - it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

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 indicated on the following page.

	Refer to:				Inform:	Action:			
	Class teacher	E-safety coordinator	Refer to head teacher/head of school	Refer to Police	Refer to designated safeguarding lead or deputy	Parents / carers	Remove of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Pupil sanctions <i>The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.</i>									
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓								
Unauthorised use of mobile phone / digital camera / other handheld device	✓				✓	✓	✓		
Unauthorised use of social networking / instant messaging / personal email	✓	✓				✓		✓	
Unauthorised downloading or uploading of files	✓						✓	✓	

Allowing others to access school network by sharing username	✓	✓	✓					✓	
Attempting to access the school network, using another pupil's account	✓							✓	
Attempting to access or accessing the school network, using the account of a member of staff	✓		✓		✓	✓		✓	
Corrupting or destroying the data of other users	✓		✓			✓	✓	✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓		✓	✓	✓	✓	
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓		✓	✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓		✓		✓			✓	
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓			✓	✓	✓	
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓		✓	✓			
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓		✓	✓	✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓		✓		✓		✓		

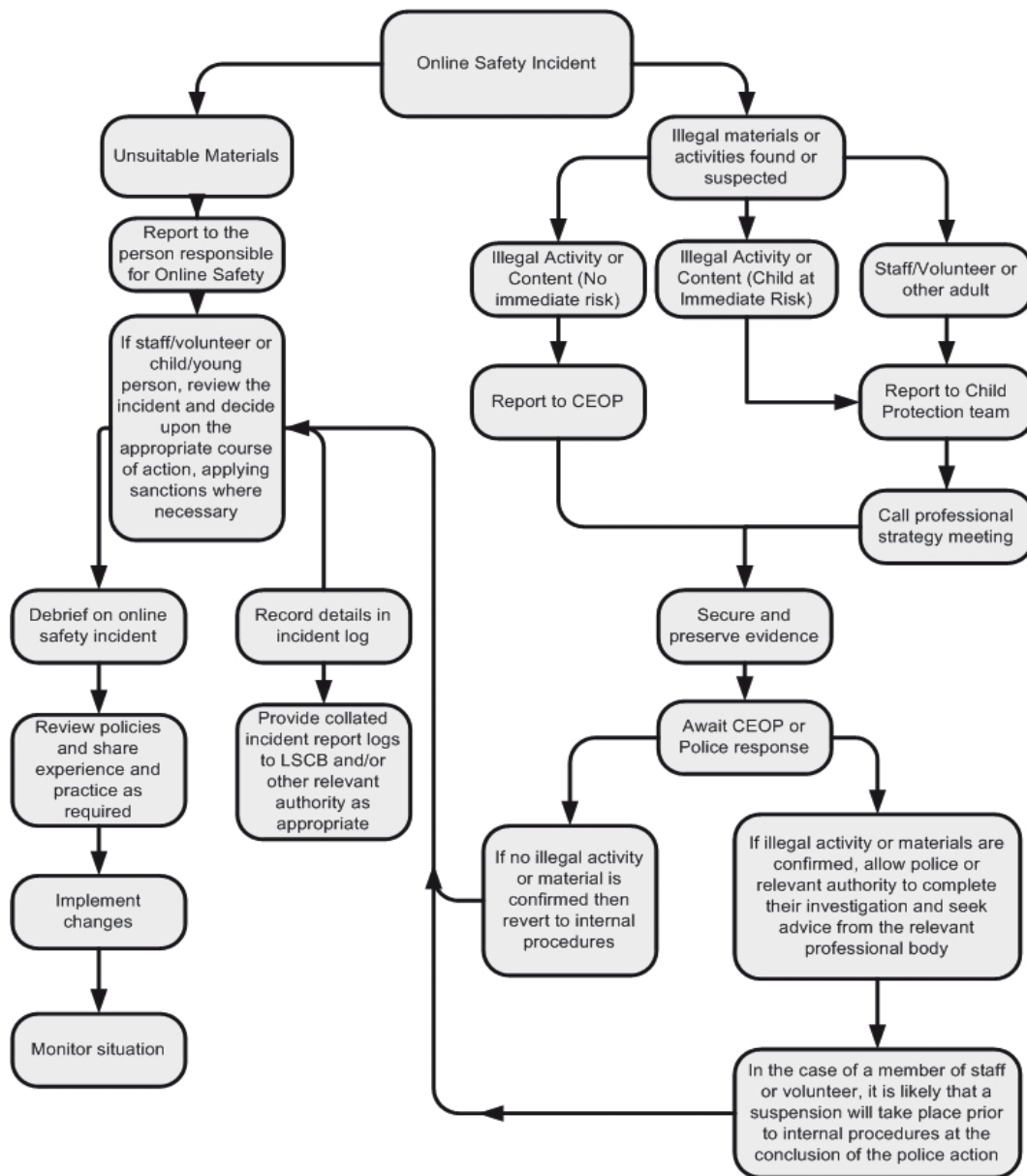
	Refer to:					Action:			
	Line manager	Head teacher/Head of School	Local Authority / HR	Police	Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action	
Staff sanctions <i>The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.</i>									
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓	✓	✓	
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓	✓				✓		✓	
Unauthorised downloading or uploading of files	✓				✓	✓			
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	✓	✓			✓	✓	✓		

Careless use of personal data e.g. holding or transferring data in an insecure manner	✓	✓	✓		✓	✓		✓
Deliberate actions to breach data protection or network security rules	✓	✓	✓		✓	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓				✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓			✓	✓	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✓	✓			✓	✓	✓	✓
Actions which could compromise the staff member's professional standing	✓	✓				✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓			✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓			✓	✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓		✓	✓		
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓	✓	✓
Breaching copyright or licensing regulations	✓					✓		
Continued infringements of the above, following previous warnings or sanctions	✓	✓			✓	✓		✓

A.2.5 Reporting of e-safety breaches

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

Particular care should be taken if any apparent or actual misuse appears to involve illegal activity listed in section A.2.4 of this policy.



A.3.1 Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- *Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:*
 - ✓ *Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances*
 - ✓ *Members of staff are free to use these devices outside teaching time and away from the vicinity of children e.g. school office or staffroom*
- *Pupils are not currently permitted to bring their personal hand held devices into school.*

Personal hand held technology	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time		✓						✓
Taking photos on personal phones or other camera devices				✓				✓
Use of hand held devices e.g. PDAs	✓							✓

A.3.2 Use of communication technologies

A.3.2a - Email

Access to school emails is provided for all users in school.

These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the school email services to communicate with others when in school, or for work related purposes only outside of school
- Users need to be aware that email communications may be monitored
- *Staff may only access personal email accounts on school systems for emergency or extraordinary purposes (if they are not blocked by filtering)*

- Users must immediately report to their class teacher / e-safety coordinator – in accordance with the school policy - the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and they must not respond to any such email

Use of Email	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Use of personal email accounts in school / on school network				✗				✗
Use of school email for personal emails				✗				✗

A.3.2b - Social networking (including chat, instant messaging, blogging etc)

Use of social networking tools	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
<i>It is important that schools review this table in the light of principles agreed within their own establishment.</i>								
Use of non educational chat rooms etc				✗				✗
Use of non educational instant messaging				✗				✗
Use of non educational social networking sites				✗				✗
Use of non educational blogs				✗				✗

A.3.2c - Videoconferencing

External IP addresses should not be made available to other sites.

Only web based conferencing products that are authorised by the school (and are not blocked by internet filtering) are permitted for classroom use.

Videoconferencing is normally supervised directly by a teacher. In the event of this not being the case pupils must ask permission from the class teacher before making or answering a videoconference call.

Permission for children to take part in video conferences is sought from parents / carers at the beginning of the pupil's time in school. Only where permission is granted may children participate.

Only key administrators have access to videoconferencing administration areas.

Unique log on and password details for the educational videoconferencing services are only issued to members of staff.

A.3.3 Use of digital and video images

- 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.
- Members of staff are allowed to take digital still and 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 captured using 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

A.3.4 Use of web-based publication tools

A.3.4a - Website (and other public facing communications)

Our school uses the public facing website www.heronswoodprimary.worcs.sch.uk only for sharing information with the community beyond our school. This includes, from time-to-time, celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information will not be posted on the school website and only official email addresses will be used to identify members of staff (never pupils).
- Only pupil's first names will be used on the website, and only then when necessary.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
 - ✓ pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
 - ✓ written permission from parents or carers will be obtained before photographs of pupils are

A.3.5 Professional standards for staff communication

In all aspects of their work in our school, teachers abide by the broad **Professional Standards for Teachers** laid down by the DfE (2011):

www.gov.uk/government/uploads/system/uploads/attachment_data/file/301107/Teachers_Standards.pdf

Teachers translate these standards appropriately for all matters relating to e-safety.

Any digital communication between staff and pupils or parents / carers (email, chat, learning platform etc) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of pupils are used to inform this process also.

Section B. Infrastructure

B.1 Password security

The school's e-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of school.

B.2.1 Filtering

B.2.1a - Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

B.2.1b - Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the **e-safety coordinator** (with ultimate responsibility resting with the **head of school and School Improvement Board Members**). They manage the school filtering in line with this policy and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks to protect those responsible, changes to the school filtering service must:

- be logged in change-control logs
- be reported to a second responsible person (*the head of school / ICT coordinator [if they are not also the e-safety coordinator] / e-safety governor*) within a timely manner

All users have a responsibility to report immediately to class teachers / e-safety coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

B.2.1c - Education / training / awareness

Pupils are made aware of the importance of filtering systems through the school's e-safety education programme.

Staff users will be made aware of the filtering systems through:

- signing the Acceptable Use Agreement (as part of their induction process)
- briefing in staff meetings, training days, memos etc. (timely and ongoing).

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions.

B.2.1d - Changes to the filtering system

Where a member of staff requires access to a website that is blocked for use at school, the process to unblock is as follows:

- The teacher makes the request to the school e-safety coordinator
- The e-safety coordinator checks the website content to ensure that it is appropriate for use in school

THEN (if the school is not controlling its own filtering)

- If agreement is reached, the e-safety coordinator makes a request to DandD.
- The Support helpdesk will endeavour to unblock the site within 24 hours. This process can still take a number of hours so teaching staff are required to check websites in advance of teaching sessions

B.2.1e - Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment. Monitoring takes place as follows:

- Identified member(s) of staff reviews the Policy Central console captures weekly
- "False positives" are identified and deleted
- Potential issues are referred to an appropriate person depending on the nature of the capture
- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g. 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught

Section C. Education

C.1.1 E-safety education

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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of ICT, PHSE and other lessons. This is regularly revisited, covering the use of ICT and new technologies both in school and outside school
- *We use the resources through Digital Literacy and Citizenship organisation(e.g. Hector's World at KS1 and Cyber Café and SAFE social networking at KS2)*
- Key e-safety messages will be reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT both within and outside school
- 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, encouraging children to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary
- Pupils will be made aware of what to do should they experience anything, while on the Internet, which makes them feel uncomfortable

C.1.2 Information literacy

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
 - ✓ Checking the likely validity of the URL (web address)
 - ✓ Cross checking references (Can they find the same information on other sites?)
 - ✓ Checking the pedigree of the compilers / owners of the website
 - ✓ See lesson 5 of the Cyber Café Think U Know materials below
 - ✓ Referring to other (including non-digital) sources
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils are taught how to make best use of internet search engines to arrive at the information they require
- *We use the resources on CEOP's Think U Know site as a basis for our e-safety education <http://www.thinkuknow.co.uk/teachers/resources/>*

C.1.3 The contribution of the children to e-learning strategy

It is our general school policy to encourage children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology (especially rapidly developing technology such as mobile devices) could be helpful in their learning.

C.2 Staff training

It is essential that all staff – including non-teaching staff - receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction
- The E-safety Co-ordinator will be CEOP trained
- *The E-Safety Coordinator will receive regular updates by reviewing guidance documents released by the DfE, the local authority, the WSCB and others*
- *All teaching staff and non-teaching staff have a responsibility to read and understand this e-safety policy and are therefore aware of its content*
- *The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required on an ongoing basis*

C.3 Governor training

School Improvement Board Members should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee or group involved in ICT, e-safety, health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by The Rivers MAT, National Governors Association or other bodies.
- Participation in school training / information sessions for staff or parents

The e-safety governor works closely with the e-safety coordinator and reports back to the full governing body

C.4 Parent and carer awareness raising

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- *Letters, newsletters, web site, leaflets*
- *Parents evenings*
- *Workshops*

C.5 Wider school community understanding

The school will offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e-safety should also be targeted towards grandparents and other family members. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Policy Updated: September 2022

Agreed by Local Academy Board Members: September 2021

Review Date: September 2023

Appendix 1 - Guidance for Reviewing Internet Sites

This guidance is intended for use when the school needs 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 typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police. Please follow all steps in this procedure:

- 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. *This will automatically be done for you if you are using Policy Central from Forensic Software or other monitoring software.* It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority or national / local organisation (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
 - Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.
- It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Sample documents for recording the review of and action arriving from the review of potentially harmful websites can be found in the PDF version of the SWGfL template e-safety policy (pages 36-38): http://www.swgfl.org.uk/Files/Documents/esp_template.pdf

Appendix 2 – Criteria for website filtering

A. ORIGIN - What is the website's origin?

- The organisation providing the site is clearly indicated.
- There is information about the site's authors ("about us", "our objectives", etc.)
- There are contact details for further information and questions concerning the site's information and content.
- The site contains appropriate endorsements by external bodies and/or links to/from well-trusted sources

B. CONTENT - Is the website's content meaningful in terms of its educational value?

- The content is age-appropriate
- The content is broadly balanced in nature, and does not appear unduly biased, partisan or unreliable
- The site is free of spelling mistakes, grammatical errors, syntax errors, or typos.
- **The site promotes equal and just representations of racial, gender, and religious issues.**
- **The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.**
- **The site does not link to other sites which may be harmful / unsuitable for the pupils**
- The content of the website is current.

C. DESIGN - Is the website well designed? Is it / does it:

- appealing to its intended audience (colours, graphics, layout)?
- easy to navigate through the site - links are clearly marked etc?
- have working links?
- have inappropriate adverts?

D. ACCESSIBILITY - Is the website accessible?

- Does it load quickly?
- Does the site require registration or passwords to access it?
- Is the site free from subscription charges or usage fees?

Appendix 3 - Supporting resources and links

The following links may help those who are developing or reviewing a school e-safety policy.

General

South West Grid for Learning “SWGfL Safe” - <http://www.swgfl.org.uk/Staying-Safe>

Child Exploitation and Online Protection Centre (CEOP) <http://www.ceop.gov.uk/>

ThinkUKnow <http://www.thinkuknow.co.uk/>

ChildNet <http://www.childnet-int.org/>

InSafe <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

Byron Reviews (“Safer Children in a Digital World”) -

<http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews>

Becta – various useful resources now archived

<http://webarchive.nationalarchives.gov.uk/20101102103654/http://www.becta.org.uk>

London Grid for Learning - <http://www.lgfl.net/esafety/Pages/education.aspx?click-source=nav-esafety>

Kent NGfL <http://www.kented.org.uk/ngfl/ict/safety.htm>

Northern Grid - <http://www.northerngrid.org/index.php/resources/e-safety>

National Education Network NEN E-Safety Audit Tool -

http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html

WMNet – <http://www.wmnet.org.uk>

WES Worcestershire E-Safety Site – <http://www.wes.networks.net>

EU kids Online <http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx>

Cyber Bullying

Teachernet “Safe to Learn – embedding anti-bullying work in schools” (Archived resources)

<http://tna.europarchive.org/20080108001302/http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/>

Anti-Bullying Network - <http://www.antibullying.net/cyberbullying1.htm>

Cyberbullying.org - <http://www.cyberbullying.org/>

East Sussex Council - Cyberbullying - A Guide for Schools:

<https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying/Pages/eastsussexandnationalguidance.aspx>

CyberMentors: young people helping and supporting each other online -

<http://www.cybermentors.org.uk/>

Social networking

Digizen – “Young People and Social Networking Services”:

<http://www.digizen.org.uk/socialnetworking/>

Ofcom Report: Engaging with Social Networking sites (Executive Summary)

http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/

Connect Safely - Smart socialising: <http://www.blogsafety.com>

Mobile technologies

“How mobile phones help learning in secondary schools”:

http://archive.teachfind.com/becta/research.becta.org.uk/upload-dir/downloads/page_documents/research/lsri_report.pdf

“Guidelines on misuse of camera and video phones in schools”

http://www.dundee.gov.uk/dundee/uploaded_publications/publication_1201.pdf

Data protection and information handling

Information Commissioners Office - Data Protection:

http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

See also Becta (archived) resources above

Parents' guide to new technologies and social networking

<http://www.iab.ie/>

Links to other resource providers

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and school staff. A comprehensive list of these resources (and those available from other organisations) is available on the “SWGfL Safe” website:

<http://www.swgfl.org.uk/staying-safe>

BBC Webwise: <http://www.bbc.co.uk/webwise/>

Kidsmart: <http://www.kidsmart.org.uk/default.aspx>

Know It All - <http://www.childnet-int.org/kia/>

Cybersmart - <http://www.cybersmartcurriculum.org/home/>

NCH - <http://www.stoptextbully.com/>

Chatdanger - <http://www.chatdanger.com/>

Internet Watch Foundation: <http://www.iwf.org.uk/media/literature.htm>

Digizen – cyber-bullying films: <http://www.digizen.org/cyberbullying/film.aspx>

London Grid for Learning: <http://www.lgfl.net/esafety/Pages/safeguarding.aspx?click-source=nav-toplevel>

Appendix 4 - Glossary of terms

AUA	Acceptable Use Agreement – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (former government agency which promoted the use of information and communications technology – materials and resources are archived and still relevant)
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.
DfE	Department for Education
FOSI	Family Online Safety Institute
ICT	Information and Communications Technology
ICT Mark	Quality standard for schools provided by NAACE for DfE
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
IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network and Regional Broadband Consortia
KS1; KS2	KS1 = years 1 and 2 (ages 5 to 7) KS2 = years 2 to 6 (age 7 to 11)
LA	Local Authority
LAN	Local Area Network
Learning platform	An online system designed to support teaching and learning in an educational setting
LSCB	Local Safeguarding Children Board
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (eg WMNet) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children’s Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education

- SRF** Self Review Framework – a tool maintained by Naace used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark
- SWGfL** South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities and recognised authority on all matters relating to e-safety (on whose policy this one is based)
- URL** Universal Resource Locator – a web address
- WMNet** The Regional Broadband Consortium of West Midland Local Authorities – provides support for all schools in the region and connects them all to the National Education Network (Internet)
- WSCB** Worcestershire Safeguarding Children Board (the local safeguarding board)