Online Safety Policy

Harvington C of E First and Nursery School

Written by Milly Brown. Updated by R Enstone
Updated July 2025
Governors Responsibility: Safeguarding

Policy development, monitoring and review

This Online Safety policy has been developed (from a template provided by Worcestershire School Improvement Service) by a working group made up of:

- *School Online Safety Lead*
- *Headteacher / Senior Leaders*
- *Teachers*
- *ICT Technical staff*
- *Governors*
- *Parents and Carers*
- *Pupils*

Schedule for development / monitoring / review of this policy

This Online Safety policy was approved by the governing body on:	7.23
The implementation of this Online Safety policy will be monitored by the:	*The Online Safety Lead*
Monitoring will take place at regular intervals:	*Annually*
The governing body will receive regular reports on the implementation of the Online Safety policy (which will include anonymous details of Online Safety incidents) as part of a standing agenda item with reference to safeguarding:	*Termly meetings held with the Safeguarding Governor*
The Online Safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technology, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:	*July 2026*
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	*Worcestershire Safeguarding Children Board Online Safety representative or* *Local Authority Designated Officer or* *Worcestershire Senior Adviser for Safeguarding Children in Education or* *West Mercia Police*

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even truer 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.

This Online Safety Policy outlines the commitment of Harvington C of E First and Nursery School to safeguard members of our school community online in accordance with statutory guidance and best practice. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Harvington C of E First and Nursery 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.

While developing technology brings many opportunities, it also brings risks and potential dangers, for example:

- 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.
- Potential for paying for add ons/extras when gaming leading to mismanagement of finances

The purpose of this policy statement is to:

- Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- Provide staff and volunteers with the overarching principles that guide our approach to online safety
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in Harvington C of E First and Nursery School.

Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England.

Summaries of the key legislation and guidance are available::

• Online abuse learning https://www.nspcc.org.uk/keeping-children-safe/online-safety/
• Bullying learning https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/bullying-and-cyberbullying/
• Child protection learning https://learning.nspcc.org.uk/

We believe that:

• Children and young people should never experience abuse of any kind
• Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

• The online world provides everyone with many opportunities; however it can also present risks and challenges
• We have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
• We have a responsibility to help keep children and young people safe online, whether or not they are using Harvington C of E First School's network and devices
• All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
• Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

Policy and leadership

Responsibilities: the Online Safety Lead: DSL: Tom Holdstock

- *Review and monitor this Online Safety policy.*
- *Consider any issues relating to school filtering*
- *Discuss any Online Safety issues that have arisen and how they should be dealt with.*
- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident
- provides training and advice for staff
- liaises with the Local Authority
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments
- attends relevant meetings and committees of Governing Body
- receives appropriate training and support to fulfil their role effectively

Issues that arise are referred to other school bodies as appropriate and, when necessary, to bodies outside the school such as the Worcestershire Safeguarding Children Board.

Responsibilities: Governors

Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors (or a governors' subcommittee) receiving regular information about Online Safety incidents and monitoring reports.

- *Monitoring of Online Safety incident logs*
- *Reporting to relevant Governors committee / meeting*
- *Regular meetings with the Online Safety Co-ordinator (termly) with an agenda based on:*

✓ monitoring adherence to, and effectiveness of Online Safety and Acceptable Use policies
✓ monitoring of mechanisms to support pupils, staff and parents facing online safety issues
✓ regular review of Online Safety training, to ensure it remains relevant and up to date for all stakeholders
✓ monitoring of mechanisms for educating children to build knowledge, skills and confidence around online safety, and assessing their effectiveness
✓ monitoring of mechanisms for the education of parents and the whole school community with online safety, and assessing their effectiveness

Responsibilities: Headteacher

- The Headteacher is responsible for ensuring the safety (including Online Safety) of all members of the school community, though the day to day responsibility for Online Safety is delegated to the Online 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 Online Safety allegation being made against a member of staff, including non-teaching staff (see flow chart on dealing with Online Safety incidents below) and other relevant Local Authority HR / disciplinary procedures)

Responsibilities: Teaching and support staff

School 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 Online Safety matters and of the current school Online Safety policy and practices
- They have read, understood and signed the school's Acceptable Use Agreement for staff (see Appendix 1)

- They report any suspected misuse or problem to the Online Safety Lead
- They undertake any digital communications with others in a fully professional manner and only using official school systems
- They embed Online Safety issues in the curriculum and other school activities, also acknowledging the planned Online Safety programme
- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding they have attended training with The Online Safety Lead
  They immediately report any suspected misuse or problem to DSL or DDSLs for investigation/action, in line with the school safeguarding procedures
- Ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- In lessons where internet use is pre-planned, learners 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 lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource:
  https://swgfl.org.uk/resources/safe-remote-learning/
- Have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Responsibilities: Communication:

When using communication technologies, the school considers the following as good practice:

• When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school

• Any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.

• Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community

• Users should immediately report to the DSL, DDSLs and Headteacher, 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

• Relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

Responsibilities: Technical Staff are responsible for ensuring that:

• They are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy

• The school technical infrastructure is secure and is not open to misuse or malicious attack

• The school meets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body

• There is clear, safe, and managed control of user access to networks and devices

• 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

• The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to DSL or DDSLS and Headteacher for investigation and action

• The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person

• Monitoring software/systems are implemented and regularly updated as agreed in school policies

Responsibilities: Parents and carers

The school will take every opportunity to help parents and carers understand these issues through:

• publishing the school Online Safety Policy on the school website

• providing them with a copy of the learners' acceptable use agreement

• publish information about appropriate use of social media relating to posts concerning the school

• seeking their permissions concerning digital images, cloud services

Parents and carers will be encouraged to support the school in:

• reinforcing the online safety messages provided to learners in school

• monitoring the use of their children's internet use, including on hand held devices

• Logging and reporting concerns outside of school with Class Teacher, DSL, DDSLs or Headteacher

Responsibilities: Learners

• are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy

• should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

• should know what to do if they or someone they know feels vulnerable when using online technology

• 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

The school will protect learners by:

- Appointing an online safety lead who is trained as a DSL
- Providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
- Supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- Supporting and encouraging parents and carers to do what they can to keep their children safe online
- Developing an online safety agreement for use with young people and their parents/carers
- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
- Reviewing and updating the security of our information systems regularly
- Ensuring that user names, logins, email accounts and passwords are used effectively
- Ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- Providing supervision, support and training for staff and volunteers about online safety. Providing a clear and progressive plan to teach online safety as well ensuring staff discuss aspects of learning each time the children use the computers.
- Examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

Online Safety Education Programme

The education of learners in online safety is an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop 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 for all year groups matched against a nationally agreed framework
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; RSE; Computing etc.
- Planning incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Learners should be helped to understand the need for the learner 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

There are eight aspects of Online Education. These are covered in our programme for online safety.

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and security

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
    - ✓ 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 Purple Mash and CEOP's Think U Know site as a basis for our Online Safety education http://www.thinkuknow.co.uk/teachers/resources/*

If online abuse occurs, we will respond to it by:

• Having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)

• Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation

• Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account

• Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Filtering

•The school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours

• The school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering.

• Access to online content and services is managed for all users

• Illegal content (e.g., child sexual abuse images) is filtered by the broadband

• There are established and effective routes for users to report inappropriate content

• There is a clear process in place to deal with requests for filtering changes (see above)

• Filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.

• An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored.

• There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice

• Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

• Physical monitoring (adult supervision in the classroom)

• Internet use is logged, regularly monitored and reviewed

• Filtering logs are regularly analysed and breaches are reported to senior leaders

• Pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.

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 as indicated in the. Monitoring takes place as follows:

- The DSL/DDSL reviews the filtering school system regularly
- "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.

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
- 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
- Personal 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. Please see Appendix 2.

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 pages:

Communicating with parents through online learning platforms

Throughout the school we have learning platforms which allow staff and parents to communicate and share learning. These include:

- Microsoft TEAMS
- Class Dojo
- Emails via school email address
- School App system

Parents sign our acceptable use agreement in the Data Collection Form and when starting to use Class Dojo

If a comment is deemed negative through any communication tool then please follow the correct procedure which is outlined below:

1) Do not respond and if possible take a screen shot of the message

2) Do not delete the messages and turn off commenting if the post is public
3) Report to the Leadership Team

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.
  - ✓ Personal hand held devices can only be used in lesson time in an emergency or extreme circumstances. Staff should speak with teachers/ Key Stage leads if this is the case.
  - ✓ Members of staff are free to use mobile phones and electronic devices outside teaching time.
  - ✓ Members of staff can use mobile phones on offsite visits to liaise with the school and for emergency purposes.
  - ✓ Mobile phones should never be used to take photos of children during trips.
- Pupils are not currently permitted to bring their personal hand held devices into school. Year 5 children who walk home from school may have a mobile phone, this needs to be stored at the office, where phones will be collected from at the end of the day.

Use of communication technologies

Email

Access to email 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 on school systems (e.g. by remote access)
- Users need to be aware that email communications may be monitored
- A structured education program is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email
- 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 the Online Safety lead 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 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 must only be captured using school equipment; **the personal equipment of staff should not usually be used for such purposes. However, where staff judge their own equipment is better suited or is more quickly available then they may ask permission from the Headteacher. They may then use it, provided that all images taken are uploaded to school equipment and deleted from personal equipment the same day, or within two working days of returning to school if used off site.**
- 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

Use of web-based publication tools

Website (and other public facing communications)

Our school uses the public facing website 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.
- Detailed calendars will not be published on the school website.
- 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
    - ✓ where possible, photographs will not allow individuals to be recognised
    - ✓ written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see section A.2.3 and Appendix 1)
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Learning Platform

Class teachers monitor the use of the learning platform by pupils regularly during all supervised sessions, but with particular regard to messaging and communication.
Staff use is monitored by the super-user/administrator.
User accounts and access rights can only be created by the school administrator
Pupils are advised on acceptable conduct and use when using the learning platform.
Only members of the current pupil, parent/carers and staff community will have access to the learning platform.
When staff, pupils, etc. leave the school their account or rights to specific school areas will be disabled (or transferred to their new establishment if possible / appropriate).
Any concerns with content may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.
c) Access to the learning platform may be suspended for the user.
d) The user will need to discuss the issues with a member of SLT before reinstatement.
e) A pupil's parent/carer may be informed.

A visitor may be invited onto the learning platform by the administrator following a request from a member of staff. In this instance there may be an agreed focus or a limited time slot / access.

Staff training

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

- A planned programme of formal Online Safety training will be made available to staff. An audit of the Online Safety training needs of all staff will be carried out regularly.
- It is expected that some staff will identify Online Safety as a training need within the performance management process.
- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and acceptable use policies which are signed as part of their induction

- The Online Safety Lead will receive regular updates through attendance at local authority or other training sessions and by reviewing guidance documents released by the DfE, the local authority, the WSCB and others.
- The Online Safety Lead will provide advice, guidance and training as required to individuals as required on an ongoing basis.
- External support for training, including input to parents, is sought from Worcestershire School Improvement Learning Technologies Team when appropriate

If staff had an Online Safety concern they have many sources of support:

- Log concern on CPOMs safeguarding
- Discuss with DSL or DDSLs as Safeguarding lead
- Discuss with the Safeguarding Governor
- Visit the CEOP website https://ceop.police.uk/safety-centre/
- For more information visit the https://www.saferinternet.org.uk/professionals-online-safety-helpline.

Governor training

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

- Attendance at training provided by the school, Local Authority (Governor Services or School Improvement Service), National Governors Association or other bodies.
- Participation in school training / information sessions for staff or parents

Parent and carer awareness raising

Parents and carers may have 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 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, website,*
- *Online Safety articles via the newsletter*
- *Relevant information on key issues in the news*
- *Reference to the parents materials on the National Online Safety Website https://nationalcollege.com/categories/online-safety?phases[0]=2&roles[0]=2&roles[1]=4*

Related policies and procedures. This policy statement should be read alongside our organisational policies and procedures, including:

- Safeguarding Child protection
- Child on child abuse policy
- Code of conduct for staff and volunteers
- Anti-bullying policy and procedures (in the Behaviour Policy)
- Photography and image sharing guidance

Related national policies should also be read alongside this policy:

Teaching Online Safety in school - https://www.gov.uk/government/publications/teaching-online-safety-in-schools

Education for a connected world - https://www.gov.uk/government/publications/education-for-a-connected-world

KCSIE – the most up to date version (new versions are published annually in September https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Relationships and sex education guidance - https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education

UK Council for Internet Safety
https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Appendix 1 – Acceptable Use Agreement templates

Appendix 1a – Acceptable use policy agreement – pupil (KS1)

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer
- I will only use activities if an adult says it is OK.
- I will take care of the computer and other equipment
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will turn off the monitor and tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

I understand these computer rules and will do my best to keep them

My name:	
Signed (child):	
OR Parent's signature:	
Date:	

Appendix 1b – Acceptable use policy agreement – pupil (KS2)

I understand that while I am a member of Harvington CE First School I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology (especially when I use the internet) will be supervised and monitored.
- I will keep my password safe and will not use anyone else's (even with their permission)
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.

For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will only use my own personal device if I have permission and use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school safe.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on the devices belonging to the school without permission.
- I will only use social networking, gaming and chat through the sites the school allows

KS2 Pupil Acceptable Use Agreement Form

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

Name:	
Signed:	
Date:	

Appendix 1c - Acceptable Use Agreement – staff & volunteer

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, learning platform) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the Online Safety policy.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident of which I become aware, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- Mobile phones will be stored away in bags within the school cupboard and not be used in front of the chn unless on a trip in an emergency
- Any other form of technology with access to social media and messages should be not looked at or used in the presence of children and notifications should be switched off. If mobile phone or other system needs to be near, this should be discussed and agreed with leads.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital images. I will not use my personal equipment to record these images.
- Where images are published (e.g. on the school website / learning platform) I will ensure that it will not be possible to identify by name, or other personal information, those who are featured. (see section A.3.3 of the Online Safety policy)
- I will only use chat and social networking sites in school in accordance with the school's policies. (see section A.3.2 of the Online Safety policy)
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (see sections A.3.1 and A.3.2 of the Online Safety policy)

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will only use my personal mobile ICT devices as agreed in the Online Safety policy (see section A.3.1) and then with the same care as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems except in an emergency (A.3.2).
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up in accordance with relevant school policies (see **IBS Schools Systems and Data Security advice**).
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (see e-security policy). Where personal data is transferred outside the secure school network, it must be encrypted.
- I will not take or access pupil data, or other sensitive school data, off-site without specific approval. If approved to do so, I will take every precaution to ensure the security of the data,
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and to my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police (see section A.2.6).

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

Staff / volunteer Name:	
Signed:	
Date:	

Appendix 1d - Acceptable use policy agreement and permission forms – parent / carer

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure that:

- Young people will be responsible users and stay safe while using ICT (especially the internet).
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect them to agree to be responsible users.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Child's name	
Parent's name	
Parent's signature:	
Date:	

Permission for my child to use the internet and electronic communication

As the parent / carer of the above pupil(s), I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, Online Safety education to help them understand the importance of safe and responsible use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's Online Safety.

Parent's signature:	
Date:	

Permission to use digital images (still and video) of my child

The use of digital images (still and video) plays an important part in learning activities. Pupils and members of staff may use the school's digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. The school will also ensure that when images are published, the young people cannot be identified by name.

As the parent / carer of the above pupil, I agree to the school taking and using digital images of my child(ren). I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at school events which include images of children, I will abide by these guidelines in my use of these images.

Parent's signature:	
Date:	

Permission to publish my child's work (including on the internet)

It is our school's policy, from time to time, to publish the work of pupils by way of celebration. This includes on the internet; via the school website and in the school's learning platform.

As the parent / carer of the above child I give my permission for this activity.

Parent's signature:	
Date:	

Permission to for my child to participate in video-conferencing

Videoconferencing technology is used by the school in a range of ways to enhance learning – for example, by linking to an external "expert", or to an overseas partner school. Video conferencing only takes place under teacher-supervision. Independent pupil use of video-conferencing is not allowed.

As the parent / carer of the above child I give my permission for this activity.

Parent's signature:	
Date:	

The school's Online Safety Policy, which contains this Acceptable Use Agreement, and the one signed by your child (to which this agreement refers), is available on the school website.

Appendix 1e - Acceptable use policy agreement – community user

You have asked to make use of our school's ICT facilities. Before we can give you a log-in to our system we need you to formally agree to use the equipment and infrastructure responsibly.

For my professional and/or personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, of which I become aware, to a member of the school's staff.

I will be responsible in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files or data, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials described above.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, except with the specific approval of the school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines. I understand that failure to comply with this agreement will result in my access to the school's ICT systems being withdrawn, that further actions will be taken in the event illegal activity, and that I may be held liable for any damage, loss or cost to the school as a direct result of my actions.

Community user Name:	
Signed:	
Date:	

Appendix 2 - 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 Online Safety policy (pages 36-38): http://www.swgfl.org.uk/Files/Documents/esp_template_pdf

Appendix 3 – 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.

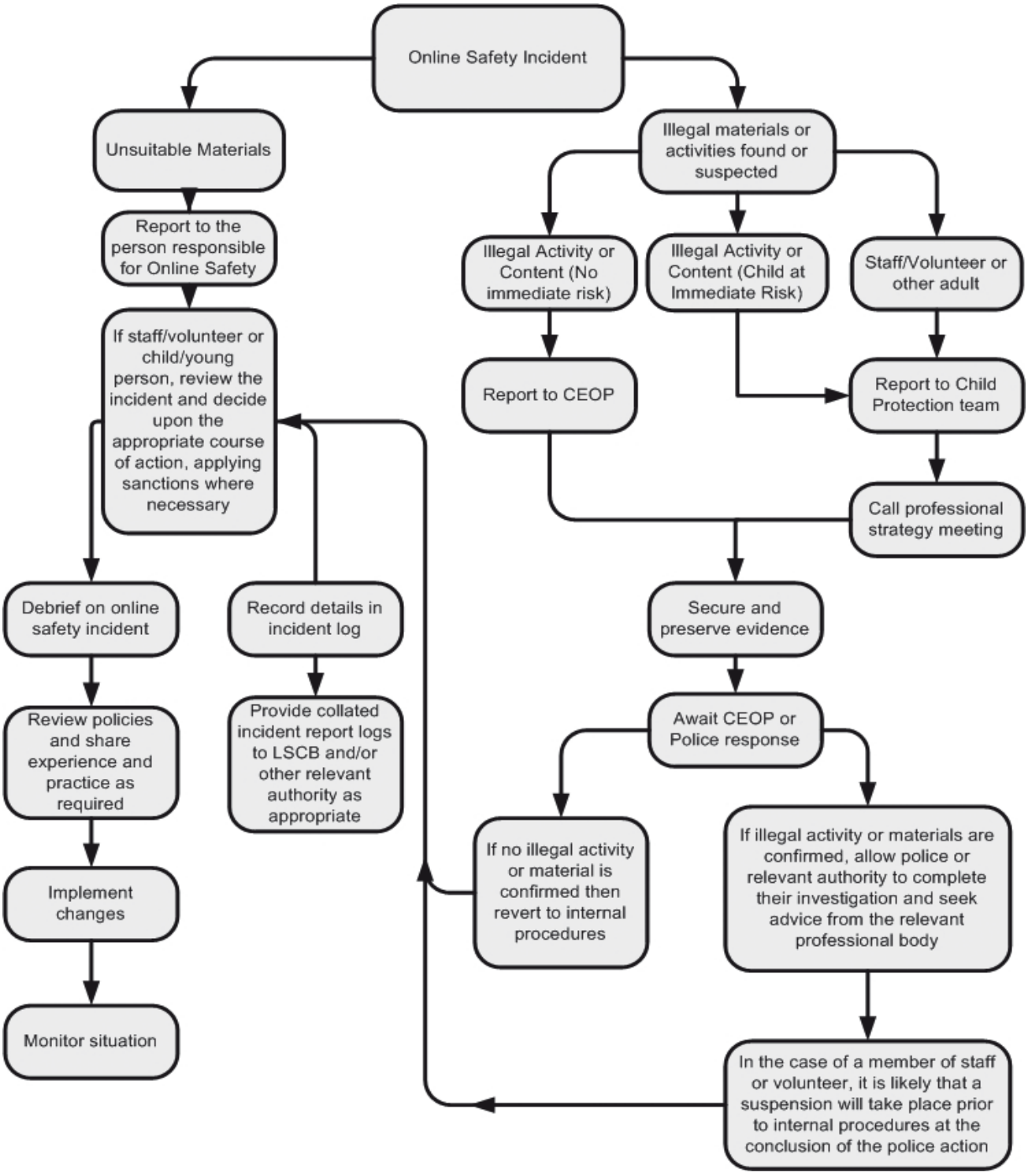
C. DESIGN - Is the website well designed? Is it / does it:

- Appealing to its intended audience (colours, graphics, and 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?

Flow chart on dealing with Online Safety incidents



The following links may help those who are developing or reviewing a school Online 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/Online Safety

National Education Network NEN Online Safety Audit Tool - http://www.nen.gov.uk/hot_topic/13/nen-Online Safety-audit-tool.html

WMNet – http://www.wmnet.org.uk

WES Worcestershire Online Safety Site – http://www.wes.networcs.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.dundeecity.gov.uk/dundeecity/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