BENTS GREEN SCHOOL

INDIVIDUALS MATTER

Online Safety Policy

Adopted from the Local Authority	
Approved by:	Sacha Schofield
Last reviewed on:	02/2021
Next review due by:	02/2023

Policy Introduction

The Online safety policy is in place to ensure that all staff and students are supported to understand how to keep themselves safe when using the internet and associated technologies. The use of these exciting and innovative technologies in school and at home has been shown to raise educational standards and promote student achievement. However, their use can put users at risk. These risks can be categorised into three main areas:

Content: being exposed to illegal, inappropriate or harmful material

Contact: being subjected to harmful online interaction with other users

Conduct: personal online behaviour that increases the likelihood of, or causes, harm

Bents Green School is committed to ensuring that students have safe access to the internet by putting effective systems in place to stop them accessing inappropriate information. This is reinforced by a curriculum which aims to ensure all students and staff develop a safe and responsible set of behaviours which will enable them to reduce the risks of harm whilst continuing to benefit from using the Internet and new technologies.

Scope of the Policy

- This policy applies to all members of the school community (including staff, students, Governors, volunteers, parents / carers, work placement students, visitors and 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, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This applies to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- The **Education Act 2011** gives the school the power to confiscate and search the contents of any mobile device if the Head Teacher believes it contains any illegal content or material that could be used to bully or harass others
- The school will identify within this policy how incidents will be managed and will, where appropriate, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Communication of the Policy

- The school's senior leadership team will be responsible for ensuring all members of school staff and students are aware of the existence and contents of the school online safety policy and the use of any new technology within school.
- The policy will be provided to and discussed with all members of staff formally.
- An online safety training programme will be established across the school to include a regular review of the online safety policy.
- All amendments will be published and awareness sessions will be held for all members of the school community.

- The students Acceptable User policy will be developed in conjunction with the School Council to ensure the language and vocabulary is appropriate and understandable for the intended audience.
- Online safety modules will be included in the PSHE and computing curriculum covering and detailing content of and amendments to the online safety policy / acceptable user policies.
- Pertinent points from the school online safety policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.
- The key messages contained within the online safety policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed online safety messages across the curriculum whenever the internet or related technologies are used
- The relevant sections of the online safety policy (Acceptable User policy) will be introduced to the students at the start of each school year
- Safeguarding posters will be prominently displayed around the school

Development / Monitoring / Review of this Policy

This policy has been developed through consultation with:

- Senior Leadership Team
- Safeguarding Team
- ICT Technical staff
- Governors

As a school Bents Green will keep abreast of new technologies and consider both the benefits for teaching and learning and also the risks from an online safety point of view. The online safety policy and procedures will be reviewed and amended as necessary.

The school will monitor the impact of the policy using:

- Logs of reported incidents via CPOMs and Smoothwall
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students
  - parents / carers
  - staff

All staff and members of the School community will be informed of any relevant amendments to the policy.

Roles and Responsibilities

We believe that online safety is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for teaching and learning. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Senior Leadership Team:

- The Head Teacher has overall responsibility for online safety for all members of the school community, though the day to day responsibility for online safety will be delegated to the online safety Co-ordinator with the support of technical staff.
- The Head Teacher and senior leadership team are responsible for ensuring that the online safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues when necessary.
- The Head Teacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The Head Teacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious online safety incident.
- The Head Teacher will be responsible for leading any investigations of illegal / inappropriate use of technology by staff in line with behaviour and discipline procedures.
- The Head Teacher is responsible for ensuring that data held in school complies with the Data Protection Act (2018). This includes understanding and informing:

  - What information is held, and for what purposes
  - How information will be amended or added to over time
  - Who has access to the data and why
  - How information is retained and disposed of

Responsibilities of the online safety Coordinators- Safeguarding Co-ordinator and Teaching Staff Co-ordinator.

- To promote an awareness and commitment to online safety throughout the school.
- To take day-to-day responsibility for online safety within school and to have a leading role in establishing and reviewing the school online safety policies and procedures, ensuring that they remain current and pertinent
- To make appropriate resources, training and support available to members of the school community to ensure that all staff are able to carry out their roles with regard to online safety effectively and that online safety is embedded within the curriculum.
- To ensure that all members of staff and students are made aware of the school's online safety policy and procedures and of any subsequent changes made.
- To work with members of SLT to monitor teaching and learning to ensure that online safety is embedded within the curriculum
- To be a point of contact in school on online safety matters (see attached protocols) – receive and regularly review online safety incident logs and be aware of the procedures to be followed should an online safety incident happen in school.
- To ensure online safety incidents of a safeguarding nature are passed immediately to the safeguarding team in line with the schools protocols
- To lead the school online safety team
- To liaise with the local authority (Online safety support manager), the Local Safeguarding Children's board and other relevant agencies as appropriate.
- To communicate regularly with school technical staff, the Safeguarding governor, the Senior Leadership Team and the schools Designated safeguarding lead.
- To maintain an up to date understanding of current online safety issues, guidance and appropriate legislation.
- To monitor and report on online safety issues to the online safety group and the senior leadership team and governors.
- To ensure that an online safety incident log is developed and kept up to date.

- To ensure that school Acceptable Use Policies are appropriate for the intended audience.
- To understand the issues surrounding the sharing of personal or sensitive information.
- To understand the dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving grooming of young children.
- To be aware of and understand cyberbullying and the use of social media for this purpose.
- To ensure that systems are in place to make sure that photographs of children and their names do not appear together at any time on any publication and that the use of photos and images are in line with parental consent.
- To provide regular online safety training for all staff and to ensure it is delivered as part of an induction package to all new staff.
- To provide regular safety training for all parents through workshops and through online presentations / information and to ensure that online safety is regularly promoted to parents / carers
- To ensure support is available to parents regarding safety / internet and safety settings as needed.
- To provide additional training and support to individual staff as needed.
- To audit the online safety knowledge and needs of the staff team at regular intervals.
- To maintain up to date knowledge of current online safety issues and ensure that teaching staff receive guidance on what to teach / how to keep children safe online.
- Provide schemes of work and reference to useful websites / activities / resources to support the teaching and learning relating to online safety
- Ensure that visual online safety information is clearly in place around school and that students are taught how to report a concern or problem.
- To support the head teacher to ensure use and storage of data complies with the data protection act (1998), that clear guidance is in place and that all staff are aware of and adhere to the given guidance.
- To work with the Senior Leadership Team, computing lead and technical staff to develop safe and effective ICT systems and protocols across school.
- To attend Sheffield City Council Online Safety Training.

Responsibilities of the Designated Safeguarding Lead/Deputies

- To support the online safety coordinator in promoting an awareness and commitment to online safety throughout the school.
- To be a point of contact in school on online safety matters (see attached protocols) – receive and regularly review online safety incident logs and be aware of the procedures to be followed should an online safety incident happen in school.
- To lead the safeguarding team
- To liaise with the local authority, the Sheffield Safeguarding Children's Board and other relevant agencies as appropriate.
- To communicate regularly with school technical staff, the Safeguarding governor, Senior Leadership Team, PSHCE and computing leads.
- To maintain an up to date understanding of current online safety issues, guidance and appropriate legislation.
- To ensure that online safety is promoted to parents and carers.
- To understand the issues surrounding the sharing of personal or sensitive information.
- To understand the dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving grooming of young children.
- To be aware of and understand cyberbullying and the use of social media for this purpose.

- To lead any investigations of illegal / inappropriate use of technology by students in line with behaviour and discipline procedures, reporting to and consulting with wider professionals in line with the schools responses to an Incident of Concern (see page 19)
- To attend Safeguarding Refresher yearly with Sheffield City Council.

Responsibility of the school's PSD AND PSHE (including online safety) and computing Leads

- To promote to all members of the school community the safe use of the internet and any technologies deployed within school.
- To work with the Senior Leadership Team and the school's online safety coordinator to develop, implement and monitor a school wide online safety curriculum and protocols in line with current requirements and advice from the Safeguarding Sheffield Children's board and other relevant establishments.
- To support the online safety coordinator and Senior Leadership Team to monitor the implementation of the online safety Acceptable Use Policies for students within school
- To work with the Senior Leadership Team and online safety coordinator to monitor the teaching and learning of online safety across school.
- To maintain up to date knowledge of current online safety issues and support the online safety coordinator to ensure that teaching staff receive guidance on what to teach / how to keep children safe online.
- Work with the online safety coordinator to provide schemes of work and reference to useful websites / activities / resources to support the teaching and learning relating to online safety
- Ensure that visual online safety information is clearly in place around school and that students are taught how to report a concern or problem.
- The computing lead to work with the SLT, the online safety coordinator and technical staff to develop safe and effective ICT systems and protocols across school.

Responsibilities of the Teaching and Support Staff

- To read, understand and help promote the school's online safety policies and guidance.
- To read the online safety bulletins sent out regularly via email
- To attend / complete any required training
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To ensure students are made aware of and understand the school's Student Acceptable Use policy
- To report any suspected misuse or problem to the online safety coordinator / technical lead / safeguarding team following the schools safeguarding procedures.
- To develop and maintain an awareness of current online safety issues and guidance.
- To model safe and responsible behaviours in their own use of technology and maintain a professional level of conduct in personal use of technology at all times.
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones etc.
- To ensure that only school equipment is used to take photographs of children and that photographs are deleted once uploaded.
- To embed online safety messages in learning activities across all areas of the curriculum.

- To supervise and guide pupils carefully when engaged in learning activities involving technology.
- To ensure that pupils are made aware of research skills and of legal issues relating to electronic content such as copyright laws (where appropriate).
- Ensure that sensitive and personal data is kept secure at all times by using the schools cloud data storage / schools network as directed and by transferring data through secure communication systems.
- To incorporate current online safety issues into teaching and learning, adapting resources and activities to reflect current issues and groups learning needs.
- To ensure that photographs of children and their name do not appear together at any time on any publication.
- To ensure that images and videos of students are only used with appropriate parental consents.
- To read, understand, contribute to and help promote the school's online safety policies, procedures and guidance.

Responsibilities of Technical Lead

- To work with SLT and the computing lead to ensure appropriate filtering is in place for all students and that this is monitored and reviewed regularly and adapted as needed in line with new developments and the safeguarding log.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school ICT system, specifically
    - All externally facing devices shall be hardened and patched to ensure no high-risk vulnerable are present
    - All desktops shall have up to date anti-malware software installed
    - All incoming email shall be scanned for malware and filtered for spam
    - All anti-malware software shall be configured to alert the ICT technicians when any malware is detected
    - All malware definitions should be updated daily
    - All students access to the internet should be filtered for inappropriate use
    - All hard discs and other media containing school information (including backup media) should be securely deleted, either by specialist detection utilities or physical destruction prior to disposal
    - Data backups should be automated, taken at regular intervals (daily) and backup media should be kept offsite
    - Use a log consolidation tool in conjunction with a network time protocol server to enable accurate analysis of logs
    - All internet-facing systems shall be placed onto a separate network segment, a demilitarised zone (DMZ) with access to applicable services, controlled by a firewall
    - All wireless implementations shall be a minimum of WPA2 encryption, and shall require authentication prior to connection
- To support the school in providing a safe technical infrastructure to support teaching and learning
- To liaise with the local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.

- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted.
- Where any external network traffic is allowed from the internet to the school, a local firewall will be deployed to restrict traffic into only necessary ports and IP.

Responsibilities of Students / pupils

To the best of their abilities:

- Read, understand and adhere to the school student Acceptable Use Policy
- Help and support the school in the creation of online safety policies and practices and to adhere to any policies and practices the school creates.
- Know and understand school policies on the use of mobile phones, digital cameras and handheld devices.
- Know and understand school policies regarding cyberbullying.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- Demonstrate awareness (where appropriate) of research skills and of legal issues relating to electronic content such as copyright laws.
- Take responsibility for your own and each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school.
- Accept responsibility for your comments made on social networking sites and/or text messages sent.
- Ensure you respect the feelings, rights and values of others in your use of technology in school and at home.
- Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if you know of someone who this is happening to.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exist within school.
- Discuss online safety issues with family and friends in an open and honest way.

Responsibilities of Parents / Carers

- To help and support your school in promoting online safety.
- To read, understand and promote the school student Acceptable Use Policy with your children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that your children use in school and at home.
- To participate in online safety training events, either by attending workshops or by undertaking the online training provided on line.
- To support school in identifying parental training needs by completing online safety training audits when requested.

- To take responsibility for your own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss online safety concerns with your children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- To model safe and responsible behaviours in your own use of technology
- To consult with the school if you have any concerns about your children's use of technology.
- Ensure that you monitor your son / daughter's use of the internet at home.

Responsibilities of the Governing Body

- To read, understand, contribute to and help promote and monitor the school's online safety policies, procedures and guidance.
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- To develop an overview of how the school ICT infrastructure provides safe access to the internet.
- To develop an overview of how the school encourages students to adopt safe and responsible behaviours in their use of technology in and out of school.
- To support the work of the online safety group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in online safety activities.
- To ensure appropriate funding and resources are available for the school to implement its online safety strategy.
- To identify an online safety governor to meet regularly with the online safety co-ordinator to review safeguarding processes in school: including monitoring of the online safety logs, monitoring of the teaching and learning relating to safeguarding / online safety across the curriculum and the provision of monitoring reports to the rest of the governing body.
- To be aware of safety issues and guidance by undertaking regular reading / training.

Protecting the professional identity of all staff, work placement students and volunteers

Please also see "Guidance for Safer Working Practice for Adults who work with Children and Young People"

Communication between adults and between children / young people and adults, by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums and blogs.

When using digital communications, staff and volunteers should:

- Only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of the school.
- Not share any personal information with a child or young person e.g. should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.
- Not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.

- Not send or accept a friend request from the child/young person on social networks.
- Pass on to the safeguarding lead in school any occasions where students attempt to make contact with them personally (i.e. through a social networking site)
- Be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- Ensure that all communications are transparent and open to scrutiny.
- Be careful in their communications with children so as to avoid any possible misinterpretation.
- Ensure that if they have a personal social networking profile, details are not shared with children and young people in their care (making every effort to keep personal and professional online lives separate).
- Not post information online that could bring the school into disrepute.
- Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Education

At Bents Green School we believe that the key to developing safe and responsible behaviours online, not only for students but for everyone within the school community, lies in a progressive and age appropriate online safety curriculum. We know that the Internet and other technologies are embedded in our students' lives not just in school but outside as well, and we believe we have a duty to help prepare our students to safely benefit from the opportunities that the Internet brings.

Online safety education will be provided in the following ways:

- We will provide a series of specific online safety-related lessons in every year group as part of the PSD AND PSHE, computing curriculum and other lessons as appropriate.
- We will celebrate and promote online safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant online safety messages with students routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- We will remind students about their responsibilities through an Acceptable Use Policy which every student will sign and which will be displayed throughout the school.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- When searching the internet for information, students will be guided to use age-appropriate search engines. All use will be monitored and students will be reminded of what to do if they come across unsuitable content.
- Where appropriate students will be taught in an age / ability appropriate way about copyright in relation to online resources.
- Students will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Students will be made aware of where / how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button

Parents/Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way and in promoting the positive use of the internet and social media. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through

- parents' evenings and Online safety workshops
- letters, parent texts
- information and parent online safety training on the school website
- information about national / local online safety campaigns / literature
- auditing parents online safety training needs / knowledge to guide training / support
- Providing support for parents regarding safety settings for Wi-Fi and devices.

Use of digital images, video and sound

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

Bents Green School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Staff will inform and educate students about the risks associated with the taking, use of, sharing, publication and distribution of images. Students will be taught to understand the risks attached to inappropriate use of images / videos online. Staff will support students to develop safe and responsible online behaviours.

- Staff and students will follow the school policies on creating, using and storing digital resources – in particular:

    - Digital images, videos and sound will not be taken without the permission of participants (where possible)
    - Images and videos will be of appropriate activities and participants will be in appropriate dress
    - Full names of participants will not be used either with the resource itself, within the file name or in accompanying text online
    - Digital images and videos will not be published online without the permission of the staff / students involved.
    - Digital images will be uploaded to the media drive on the school's network or the 'Assessment for Learning App' as soon as possible and deleted from the device.

- Digital images, video and sound should only be taken on school equipment.

- Student's work can only be published with the permission of the student and parents or carers.

Managing ICT systems and access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- All laptops, computers, tablets and mobile phones accessing school networks will be locked down when not in use by the user, including the users own equipment if used to access school networks / email systems, whether the user is at home or in school.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- All students will have an individual user account with an appropriate password which will be kept secure, in line with the student Acceptable Use Policy. They will (with staff support as needed) ensure they log out after each session.
- All student internet access will be monitored by staff and any concerns will be reported following the school's policies and protocols.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the school Acceptable User Policies at all times.
- Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff, e.g. Lead Technician and Computing Lead Teacher
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However, it is not possible to guarantee that access to unsuitable material will never occur. All incidents of inappropriate access will be reported, investigated and acted upon appropriately.
- The school will regularly audit ICT use to establish if the online safety policy is adequate and that it is appropriately implemented across school. The policies will be reviewed and amended to minimise risks.

Filtering internet access

- The school uses a filtered internet service. The filtering system is provided by Virgin Media and Smoothwall.
- The school's internet provision will include filtering appropriate to the age and maturity of pupils. The online safety coordinator, head teacher and computing leads will meet to discuss steps to manage / develop the levels of filtering for different groups of students within school.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school has a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable User Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the online safety Coordinator. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the Designated safeguarding Lead who will ensure that that the head teacher, online safety

coordinator and lead technician are also informed. In the DSL's absence incidents should be reported directly to the Head Teacher. The school will report such incidents to appropriate agencies including the local authority, (safeguarding advisory and/ or LADO {Local Authority Designated Officer}) police, CEOP (the Child Exploitation and Online Protection Centre) or the IWF(Internet Watch Foundation)

- The school will regularly review the filtering product for its effectiveness.
- The school filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked. A record will be kept of requests and any changes to filtering.
- Pupils will be taught to assess content safely as their internet usage skills develop.
- Pupils will use age-appropriate tools to research internet content.

Passwords

- A secure and robust username and password convention exists for all system access. (Email, network access, school management information system).
- All students have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All staff have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All information systems require end users to change their password at first log on.
- All users are prompted to change their passwords at prearranged intervals.
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.
- All staff will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords, including:
    - Do not write down system passwords.
    - Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
    - Always use your own personal passwords to access computer based services, never share these with other users.
    - Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
    - Never save system-based usernames and passwords within an internet browser.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.
- The school maintains a log of all accesses by users and of their activities while using the system.
- Passwords must contain a minimum of eight characters and be difficult to guess.
- Users should create different passwords for different accounts and applications.
- Users should use numbers, letters and special characters in their passwords (! @ # $ % * ( ) - + = , < > : : " '): the more randomly they are placed, the more secure they are.

- All users accessing school based information on personal devices must have those devices password protected. All devices should be set to request passwords if unused by the user after a 2 minute interval.

Management of assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

Data Protection

- We will ensure that all personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Users should ensure that they log off at the end of any session in which they are using personal data or that their computer is locked when left unattended.
- All sensitive information and personal data will be transferred using encryption and secure password protected devices. No personal information will be contained within the email body itself for any emails being sent to any external email accounts (not 'bentsgreen .sheffield.sch.uk' accounts)
- Personal or sensitive data will not be removed from the school site without permission of the headteacher and without ensuring that such data is kept secure.
- Personal data should never be stored on any portable computer system, USB stick or any other removable media.
- Staff should only save and use data using the onedrive system taking care to remove data once it is no longer needed.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.
- Staff accessing data using their own devices will ensure that they are not left unsupervised, that they are password protected and that settings are timed to require a password after 2 minutes of inactivity.

Using Email

- All students will use approved email accounts allocated to them by the school and be aware that their use of the school email system could be monitored and checked

- All staff should use approved email accounts for school business.
- Students will be reminded when using email about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening email from an unknown sender, or viewing / opening attachments.
- Communication between staff, students, parents / carers and members of the wider school community should be professional and related to school matters only
- Any inappropriate use of the schools email system, or the receipt of any inappropriate messages by a user should be reported using the schools reporting procedures.
- Any correspondence containing sensitive information / data will be sent through secure systems (encryption / secure password protected devices) via an attachment. No sensitive information will be contained within the email itself.
- The official school email service may be regarded as safe and secure and is monitored.
- Users must immediately report to the headteacher the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, VLE etc.) must be professional in tone and content.

Using Fax machines

- All fax machines are situated within controlled areas of the school and any sensitive information or personal data sent fax is transferred using a secure method.

Using blogs, Wikis, podcasts and other ways for students to publish content online

- As we continue to develop and enhance our curriculum opportunities media such as blogs, wikis and podcasts (ways to publish content online) are used to enhance the curriculum by allowing students to publish their own content. However, we will always ensure that staff and students take part in these activities in a safe and responsible manner.
- Content will only be published within the school learning platform (or on recommended blog sites which require passwords, such as wordpress). Students will not be allowed to post or create content on sites where members of the public have access such that they can add content, make comments.
- Students will be reminded about safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, not to reveal personal information which may allow someone to identify and locate them. Students will not use their real names when creating such resources and will be supported to use appropriate nicknames.
- Parental permission will be obtained before any material is published online
- Staff and students will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking and other online publishing outside of school.

Using mobile phones

- All students will be asked to hand in their mobile phones to reception on arrival at school.
- Students will collect their phones prior to going home.
- All students will be made aware that they cannot use their phones to take images of other students within school. Any incidents where students are found to have taken images of others on their phones will be reported immediately to the safeguarding team.
- Students may be allowed to use their mobile phones for specific learning activities such as off-site learning. Their use will be supervised by staff and students will be regularly reminded about the safe use of phones. Students will not be allowed to take photographs of other students.
- Staff will not provide their personal phone numbers to students. Where staff members are required to use a mobile phone for school duties they must take with them a school mobile phone.
- Staff should not use their personal mobile phones to make contact with students or parents / carers. If this is necessary, for example in an emergency situation, 141 should be placed in front of the number dialled to make the caller unidentifiable.

- If members of staff are personal friends or relatives of parents contact with parents on personal mobiles is acceptable out of school hours.
- Staff accessing email or the schools learning platform using personal mobile phones must ensure that they have appropriate security settings to protect personal data (as described under data protection and passwords).
- Staff should never use their mobile phones to take photographs of students.
- Mobile phones, as well as tablet and game systems, are a common vehicle for cyberbullying. All students will be reminded about the unacceptability of this during PSD AND PSHE lessons and otherwise as needed.

The school website and other online content published by the school

- The school website will not include the personal details, including individual email addresses, of staff or students.
- A generic contact email is used for all enquiries received through the school website
- All content for the school's website and twitter account will be published through the school's website team only and will be approved prior to publication.
- Permission will be gained from parents / carers to publish student photographs / information. Students' names will not be used alongside photographs.
- Staff and students should not post school-related content on any external website without seeking permission first from the head teacher, Sacha Schofield .

Communication Technologies

The grid below shows which technologies we have agreed as a staff will be allowed in school

	Students	Staff
Personal mobiles brought into school	Allowed but must be handed into reception/class and collected at the end of the day Allowed for some off-site activities with permission appropriate education / and supervision	Allowed in restricted areas of the school (offices, staffrooms and staff workrooms).They **should not** be used in classrooms or any other student areas. See mobile phone policy for exceptional circumstances
Taking photographs / videos on personal equipment	May be allowed on some off-site visits but not for taking photographs of other students. Must be closely monitored.	Not allowed
Taking photographs or videos on school's devices.	Allowed with permission	Allowed
Use of hand-held devices such as PDA's, MP3 players	Not allowed	Not allowed
Use of personal email addresses in school	Not allowed	Allowed at certain times

Use of online chat rooms in school	Not allowed	Not allowed
Use of instant messaging services	Not allowed	Allowed at certain times
Use of blogs, wikis, podcasts	Allowed within learning activities under staff guidance and supervision	Allowed within guidance provided.
Use of video conferencing or other online meetings	Allowed within learning activities under staff guidance and supervision	Allowed for professional purposes

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

- Deliberate access to illegal / inappropriate content
- Accidental access to illegal / inappropriate content
- Failure to report deliberate or accidental access to illegal / inappropriate content
- Inappropriate use of personal technologies within school, i.e. mobile phones
- Accessing non-educational websites during lesson time
- Sharing your username / password with others
- Failure to log off a computer when leaving the room
- Accessing school ICT systems using someone else's username / password
- Using school or personal equipment to send a message or create content that is offensive or bullying in nature.
- Attempting to circumnavigate school filtering, monitoring or other security settings
- Sending messages or create content which could bring the school into disrepute
- Revealing the personal information (including digital images, videos and text) of others without permission
- Use of online content in any way as to infringe copyright.
- Careless use of personal data, i.e. Insecure transfer of personal / sensitive data
- Use of digital communications to communicate inappropriately with students / parents (for example use of personal phones / emails to communicate, communication through social networking sites)
- Unauthorised downloading or uploading of files
- 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
- Actions which could compromise the staff member's or others' professional standing
- Any actions which could bring the school into disrepute or breach the integrity of the ethos of the school

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.

If any apparent or actual misuse appears to involve illegal activity e.g.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act

- Criminally racist material
- Other criminal conduct

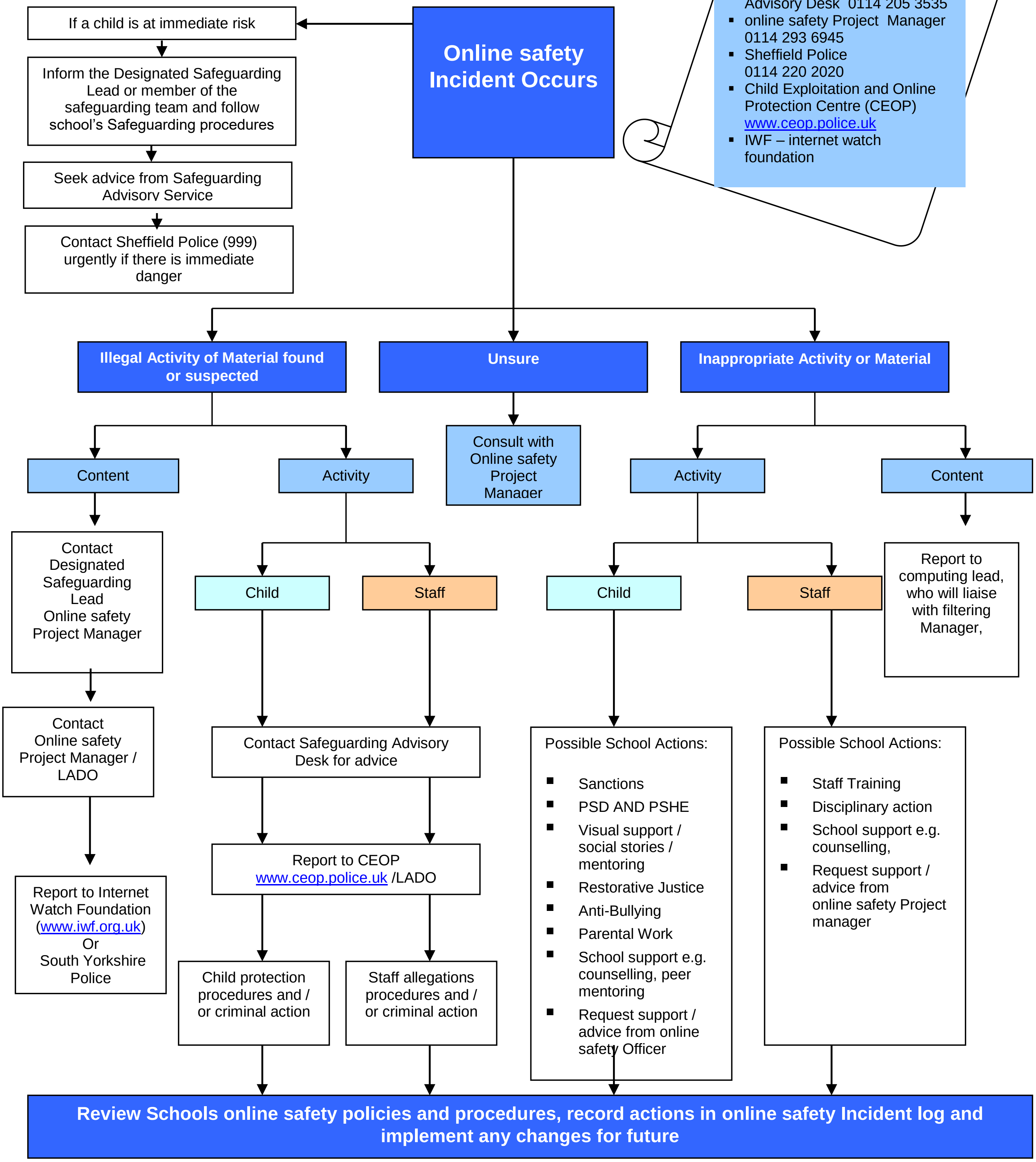
The Safeguarding Sheffield Children’s Board flow chart will be consulted and actions followed in line with the flow chart.

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. Incidents of misuse will be dealt with through normal behaviour / disciplinary procedures; by investigation led by the head teacher with guidance and support from human resources.

Response to an Incident of Concern

Contacts

- Sheffield Safeguarding Advisory Desk 0114 205 3535
- online safety Project Manager 0114 293 6945
- Sheffield Police 0114 220 2020
- Child Exploitation and Online Protection Centre (CEOP) www.ceop.police.uk
- IWF – internet watch foundation



Online safety Incident Occurs

If a child is at immediate risk

Inform the Designated Safeguarding Lead or member of the safeguarding team and follow school's Safeguarding procedures

Seek advice from Safeguarding Advisorv Service

Contact Sheffield Police (999) urgently if there is immediate danger

Illegal Activity of Material found or suspected

Unsure

Inappropriate Activity or Material

Content

Contact Designated Safeguarding Lead Online safety Project Manager

Contact Online safety Project Manager / LADO

Report to Internet Watch Foundation (www.iwf.org.uk) Or South Yorkshire Police

Activity

Child

Staff

Contact Safeguarding Advisory Desk for advice

Report to CEOP www.ceop.police.uk /LADO

Child protection procedures and / or criminal action

Staff allegations procedures and / or criminal action

Consult with Online safety Project Manaaer

Activity

Child

Possible School Actions:

- Sanctions
- PSD AND PSHE
- Visual support / social stories / mentoring
- Restorative Justice
- Anti-Bullying
- Parental Work
- School support e.g. counselling, peer mentoring
- Request support / advice from online safety Officer

Staff

Possible School Actions:

- Staff Training
- Disciplinary action
- School support e.g. counselling,
- Request support / advice from online safety Project manager

Content

Report to computing lead, who will liaise with filtering Manager,

Review Schools online safety policies and procedures, record actions in online safety Incident log and implement any changes for future

Further Information

- Sheffield Schools and settings can consult with the online safety Project Manager on telephone 0114 2736945.

- Training is available via Safeguarding Training Service on 0114 Telephone: 0114 2735430 or email safeguardingchildrentraining@sheffield.gov.uk

- The UK Safer Internet Centre's Professional Online safety Helpline offers advice and guidance around online safety for professionals who work with children and young people in the UK. The helpline provides support with all aspects of digital and online issues such as social networking sites, cyber-bullying, sexting, online gaming and child protection online. Staff can contact the helpline via 0844 381 4772, helpline@saferinternet.org.uk or can visit www.saferinternet.org.uk/helpline for more information.

- "Safer Use of New Technology" is a Kent Safeguarding Children Board (KSCB) document which discusses ideas and FAQs for professionals on how to use technology safely when working with young people. The document can be downloaded from www.kenttrustweb.org.uk?online safety

- "Supporting School Staff" is an essential document to help staff understand how to protect themselves online created by Childnet International and DfE: http://www.digizen.org/resources/school-staff.aspx

- Teach Today is a useful website which provides useful advice and guidance for staff from industry: http://en.teachtoday.eu

- 360 Degree Safe tool is an online audit tool for schools to review current practice: http://360safe.org.uk/

- "Guidance for Safer Working Practice for Adults who Work with Children and Young People" (2009) contains useful guidance around professional use of technology. www.childrenengland.org.uk/upload/Guidance%20.p

Use of Mobile phones at Bents Green School

General issues

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets or in any classrooms or areas where students are present. Designated areas of the school where mobile phones can be used outside of teaching times include the staff room, staff work areas, staff offices and the school car park.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of the senior leadership team.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- All students are requested to hand in phones and personally-owned devices to reception/class on their way into school. For some activities, for example off-site life skills learning, students will be allowed to keep their mobile phones but will be reminded that they cannot use their phones to take images or videos and of the student Acceptable User policy.
- No images or videos should be taken on mobile phones or personally-owned mobile devices.
- Staff will be provided with school mobile phones to use for off-site activities.
- In exceptional circumstances staff may need to use their personal phones in an emergency situation. Where necessary for safety, personal phones can be used for staff to keep in touch with each other and to contact emergency services and school. Staff should avoid using personal phones to contact parents and families. If absolutely necessary (exceptional circumstances only such as a child absconding or seriously hurt) personal numbers will be protected by the use 141 prior to the family number being dialled.

Students' use of personal devices

- If a student breaches the school Acceptable User policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- All students are requested to hand in phones and personally-owned devices to reception/class on their way into school. For some activities, for example off-site life skills learning, students will be allowed to keep their mobile phones but will be reminded that they cannot use their phones to take images or videos and of the other content within the student Acceptable User policy.

Links to other organisations or documents

The following sites will be useful as general reference sites, many providing good links to other sites:

Sheffield Safeguarding Children Board: http:///www.safeguardingsheffieldchildren.org

Safer Internet Centre: http://www.saferinternet.org.uk/

UK Council for Child Internet Safety: http://www.education.gov.uk/ukccis

CEOP - Think U Know - http://www.thinkuknow.co.uk/

Childnet - http://www.childnet.com

Netsmartz http://www.netsmartz.org/index.aspx

Teach Today http://www.teachtoday.eu/

Internet Watch Foundation – report criminal content: http://www.iwf.org.uk/

Byron Review ("Safer Children in a Digital World")
http://webarchive.nationalarchives.gov.uk/tna/+/dcsf.gov.uk/byronreview/

Guidance for safer working practice for adults that work with children and young people -
http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/everychildmatters/resources-and-practice/ig00311/

Information Commissioners Office/education:
http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx

ICO guidance on use of photos in schools:
http://www.ico.gov.uk/youth/sitecore/content/Home/for_the_public/topic_specific_guides/schools/photos.aspx

Ofsted survey: http://www.ofsted.gov.uk/Ofsted-home/Publications-and-research/Browse-all-by/Documents-by-type/Thematic-reports/The-safe-use-of-new-technologies/(language)/eng-GB

Plymouth Early Years Online safety Toolkit:
http://www.plymouth.gov.uk/early_years_toolkit.pdf

Protecting your personal information online:
http://www.ico.gov.uk/~/media/documents/library/data_protection/practical_application/protecting_your_personal_information_online.ashx

Getnetwise privacy guidance: http://privacy.getnetwise.org/

Children and Parents

Vodafone Parents Guide: http://parents.vodafone.com/

NSPCC: http://www.nspcc.org.uk/help-and-advice/for-parents-and-carers/internet-safety/internet-safety_wdh72864.html

Google guidance for parents: http://www.teachparentstech.org/

E-Parenting tutorials: http://media-awareness.ca/english/parents/internet/eparenting.cfm

Practical Participation – Tim Davies: http://www.practicalparticipation.co.uk/yes/

Digital Citizenship: http://www.digizen.org.uk/

Kent "Safer Practice with Technology": http://kentrustweb.org.uk/CS/community/kent_teachers/archive/2009/07/07/safer-practice-with-technology-for-school-staff.aspx

Connect Safely Parents Guide to Facebook: http://www.connectsafely.org/Safety-Advice-Articles/facebook-for-parents.html

Ofcom – Help your children to manage the media: http://consumers.ofcom.org.uk/2010/10/parental-controls-help-your-children-manage-their-media/

Mobile broadband guidance: http://www.mobile-broadband.org.uk/guides/complete-resource-of-internet-safety-for-kids/

Orange Parents Guide to the Internet: http://www.orange.co.uk/communicate/safety/10948.htm

O2 Parents Guide: http://www.o2.co.uk/parents

FOSI – Family Online Internet Safety Contract: http://www.fosi.org/resources/257-fosi-safety-contract.html

Cybermentors (Beat Bullying): http://www.cybermentors.org.uk/

Teachernet Cyberbullying guidance: http://www.digizen.org/resources/cyberbullying/overview

"Safe to Learn – embedding anti-bullying work in schools" http://www.anti-bullyingalliance.org.uk/tackling_bullying_behaviour/in_schools/law,_policy_and_guidance/safe_to_learn.aspx

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

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

CBBC – stay safe: http://www.bbc.co.uk/cbbc/help/home/

Technology

Kaspersky – advice on keeping children safe - http://www.kaspersky.co.uk/keeping_children_safe

Kaspersky - password advice: www.kaspersky.co.uk/passwords

CEOP Report abuse button: http://www.ceop.police.uk/Safer-By-Design/Report-abuse/

Which Parental control guidance: http://www.which.co.uk/baby-and-child/child-safety-at-home/guides/parental-control-software/

How to encrypt files: http://www.dummies.com/how-to/content/how-to-encrypt-important-files-or-folders-on-your-.html

Get safe on line – Beginners Guide - http://www.getsafeonline.org/nqcontent.cfm?a_name=beginners_1

Childnet Parents and Teachers on downloading / music, film, TV and the internet - http://www.childnet.com/downloading/

Microsoft Family safety software: http://windows.microsoft.com/en-US/windows-vista/Protecting-your-kids-with-Family-Safety

Norton Online Family: https://onlinefamily.norton.com/

Forensic Software http://www.forensicsoftware.co.uk/education/clients.aspx