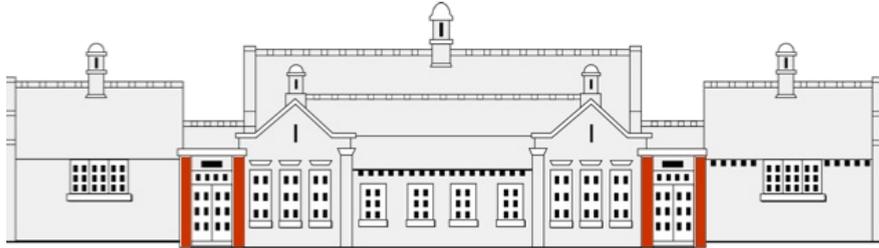


SIR JOHN BARROW SCHOOL



ONLINE SAFETY (E-SAFETY) POLICY & PROCEDURES

2020/2021

APPROVED BY: **Finance, Buildings and Personnel Committee**

Name: Janet Heffernan

Position: Committee Chair

Janet Heffernan

Signed:

Date: March 2020

Review Date: Spring 2021

Contents

POLICY

1. Background/Rationale

2. Definitions

3. Associated School Policies and procedures

4. Communication/Monitoring/Review of this Policy and procedures

5. Schedule for Development / Monitoring / Review

6. Scope of the Policy

PROCEDURES

1. Roles and Responsibilities

1.1 Governors

1.2 Head teacher

1.3 Online Safety Coordinator/Designated Safeguarding Lead

1.4 Network Manager/Technical staff

1.5 All Staff

1.6 Pupils

1.7 Parents

2. Training

2.1 Staff and Governor Training

2.2 Parent Awareness and Training

3. Teaching and Learning

3.1 Why Internet use is Important

3.2 How Internet Use Benefits Education

3.3 How Internet Use Enhances Learning

3.4 Pupils with Additional Needs

4. Managing Information Systems

4.1 Maintaining Information Systems Security

4.2 Managing Email

4.3 Emailing Personal, Sensitive, Confidential or Classified Information

4.4 Managing Published Content

4.5 Use of Digital and Video Images

4.6 Managing Social Networking, Social Media and Personal Publishing Sites

4.7 Managing Filtering

4.8 Webcams

4.9 Managing Emerging Technologies

4.10 Data Protection

4.11 Disposal of Redundant ICT Equipment

5. Policy Decisions

5.1 Authorising Internet Access

5.2 Assessing Risks

5.3 Unsuitable/Inappropriate Activities

5.4 What are the risks?

- 5.5 Responding to Incidents of Concern
- 5.6 Managing Cyber-bullying
- 5.7 Managing The Blog
- 5.8 Managing Mobile Phones and Personal Devices

6. Communicating Policy and procedures

- 6.1 Introducing the Policy and procedures to Pupils

7. Acknowledgements

Please ensure that prior to publication, any working Appendices and references to those Appendices in the body of the Policy and procedures are removed.

Appendix A	-	School Online Safety Audit
Appendix B	-	Sample EYFS, Primary and Special School Online Safety Posters
Appendix C	-	Sample Secondary School Online Safety Poster
Appendix D	-	EYFS, Primary & Special School Pupil Acceptable Use Agreement
Appendix E	-	Secondary School Pupil Acceptable Use Agreement
Appendix F	-	Staff/Volunteer Acceptable Use Agreement
Appendix G	-	Governor Acceptable Use Agreement
Appendix H	-	Social Networking Sites (Facebook) Guidance for Parents
Appendix I	-	Response to an Incident or Concern Flow Chart
Appendix J	-	Sample Online Safety Incident Log
Appendix K	-	Online Safety Links
Appendix L	-	Legal Framework
Appendix M	-	Glossary of Terms

Note: Not all of the Appendices will be appropriate or deemed necessary for your school and only those required/ approved should be used with your Policy and procedures. Please ensure that all statements within the Acceptable Use Agreements are appropriate and necessary for your setting

POLICY

2.1. Background/Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use online and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The school Online Safety Policy and procedures will help to ensure safe and appropriate use. The development and implementation of such a strategy will involve all the stakeholders in a child's education from the Head teacher and Governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to/loss of/sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The risk of being targeted by extremists in order to promote and encourage radicalisation;
- The risk of being targeted by those involved in child sexual exploitation;
- 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 use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this Online Safety Policy and procedures is used in conjunction with other school Policies including the Overarching Safeguarding Statement, Child Protection, Data Protection and Whole School Behaviour.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The Online Safety Policy and procedures that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2.2. Definitions

For the purposes of this document a child, young person, pupil or student is referred to as a 'child' or a 'pupil' and they are normally under 18 years of age.

Wherever the term 'parent' is used this includes any person with parental authority over the child concerned e.g. carers, legal guardians etc.

2.3. Associated School Policies and procedures

This Policy should be read in conjunction with the following school Policies/procedures:

- Overarching Safeguarding Statement
- Child Protection Policy and procedures

- Data Protection Policy including procedures for CCTV
- Health and Safety Policy and procedures
- Whole School Behaviour Policy
- Procedures for Using Pupils Images
- Code of Conduct for staff and other adults
- Voluntary Home-School Agreement

2.4. Communication/Monitoring/Review of this Policy and procedures

This Policy and procedures will be communicated to staff, pupils and the wider community in the following ways:

- Posted on the school website/ shared staff server
- Policy and procedures to be discussed as part of the school induction pack for new staff and other relevant adults including (where relevant) the staff Acceptable Use Agreement
- Acceptable Use Agreements discussed with pupils at the start of each year
- Acceptable Use Agreements to be issued to external users of the school systems (e.g. Governors) usually on entry to the school
- Acceptable Use Agreements to be held in pupil and personnel files

The Online Safety Policy is referenced from within other school Policies and procedures as outlined above.

2.5. Schedule for Development / Monitoring / Review

The school will monitor the impact of the Policy and procedures using:

- *Logs of reported incidents*
- *Surveys/questionnaires of*
 - *Pupils, parents and staff*

2.6. Scope of the Policy

This Policy and procedures applies to all members of the SJB School community (including staff, pupils, volunteers, parents, visitors, community users) who have access to and are users of the school systems, both in and out of SJB School.

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

The school will deal with such incidents within this Policy and procedures and the Whole School Behaviour Policy which includes anti-bullying procedures and will, where known, inform parents of incidents of inappropriate on-line safety behaviour that take place out of school.

PROCEDURES

3.1. Roles and Responsibilities

The following section outlines the roles and responsibilities for on-line safety of individuals and groups within the school:

1.1. Governors

The role of the Governors/online safety Governor is to:

- ensure that the school follows all current online safety advice to keep the children and staff safe;
- approve the Online Safety Policy and procedures and review its effectiveness. This will be carried out by the Governors/Governors Sub-committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body (*Jan Heffernan*) has taken on the role of Online Safety Governor

- support the school in encouraging parents and the wider community to become engaged in online safety activities;
- regular review with the ICT Co-ordinator/ Online Safety Co-ordinator

1.2. Head teacher

The Head teacher has overall responsibility for online safety provision. The day to day responsibility for online safety may be delegated to the Online Safety *Coordinator* / ICT lead.

The Head teacher will:

- take overall responsibility for data and data security;
- ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements;
- ensure that the Online Safety Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- be aware of the procedures to be followed in the event of a serious online safety incident or an allegation being made against a member of staff or volunteer and relevant Local Authority/ school disciplinary procedures). The procedures for dealing with allegations against staff or volunteers can be found within the school Child Protection Policy and all staff/volunteers are provided with a copy on induction.

1.3. Online Safety Coordinator/Designated Safeguarding Lead

The Online Safety Coordinator/Designated Safeguarding Lead will:

- take day-to-day responsibility for online safety issues and take a lead role in establishing and reviewing the school online safety procedures and documents;
- promote an awareness and commitment to e-safeguarding throughout the school community;
- ensure that online safety education is embedded across the curriculum;
- liaise with the school ICT Co-ordinator
- communicate regularly with SLT and the designated online safety governor to discuss current issues, review incident logs and filtering/change control logs;
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident or allegation against a member of staff or volunteer;
- ensure that an online safety log is kept up to date;
- facilitate training and advice for staff and others working in the school;
- be aware of emerging online safety issues and legislation, and of the potential for serious child protection issues to arise from:
 - sharing of personal data
 - access to illegal/inappropriate materials
 - inappropriate online contact with adults/strangers
 - potential or actual incidents of grooming
 - cyberbullying and the use of social media

1.4. Network Manager/Technical staff

The Systems Manager will:

- report any online safety related issues that arise, to the ICT lead.
- ensure that users may only access the school's networks through an authorised and properly enforced password protection procedures, in which passwords are regularly changed;
- ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack e.g. keeping virus protection up to date;
- that the school meets the online safety technical requirements outlined in the School Acceptable Use Agreements and any relevant Local Authority Online Safety Policy and guidance;
- ensure the school's procedures on web filtering, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices;
- that he/she keeps up to date with the school's Online Safety Policy and procedures and technical information in order to effectively carry out their Online safety role and to inform and update others as relevant;
- that the use of the network/ email is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Coordinator/Head teacher/Senior Leaders/ICT Coordinator for investigation/action/sanction;

- ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster and in order to complement the business continuity process;
- keep up-to-date documentation of the school's e-security and technical procedures.

1.5. All Staff

It is the responsibility of all staff to:

- read, understand and help promote the school's Online Safety Policy and procedures
- read, understand and adhere to the school Staff Acceptable Use Agreement;
- be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school procedures with regard to these devices;
- report any suspected misuse or problem to the Online Safety Coordinator;
- maintain an awareness of current online safety issues and guidance e.g. through CPD opportunities;
- model safe, responsible and professional behaviours in their own use of technology;
- ensure that any digital communications with pupils are on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones or social media messaging or posts.

Teachers must:

- ensure that online safety issues are embedded in all aspects of the curriculum and other school activities;
- monitor, supervise and guide pupils carefully when engaged in ICT activity in lessons, extra-curricular and extended school activities;
- ensure that pupils are fully aware of research skills and are made aware of legal issues relating to electronic content such as copyright laws.
- ensure that during lessons where internet use is pre-planned pupils are guided to sites checked as suitable for their use and that processes are known and used when dealing with any unsuitable material that is found in internet searches.

1.6. Pupils

Taking into account the age and level of understanding, the key responsibilities of pupils are to:

- use the school ICT systems in accordance with the Pupil Acceptable Use Agreement – see Appendix B, which they and/or their parents will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- know and understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- know what action to take if they or someone they know feels worried or vulnerable when using online technology;
- know and understand school procedures on the use of mobile phones, digital cameras and hand-held devices.
- know and understand school procedures on the taking/use of images and on cyber-bullying;
- understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy and procedures covers their actions out of school, if related to their membership of the school;
- take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home;
- help the school in the creation/review of the Online Safety Policy and procedures.

1.7. Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents 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, newsletters, letters, website updates and information about national/local online safety campaigns/literature*.

The key responsibilities for parents are to:

- support the school in promoting online safety which includes the pupils' use of the Internet and the school's use of photographic and video images;
- endorsing (by signature) the Pupil Acceptable Use Agreement – see Appendix B

- access the school website/VLE/online pupil records in accordance with the relevant school Acceptable Use Agreement;
- consult with the school if they have any concerns about their children's use of technology;
- ensure that they themselves do not use the internet/social network sites/other forms of technical communication in an inappropriate or defamatory way;
- support the school's approach to online safety by not uploading or posting to the Internet any pictures, video or text that could upset, offend or threaten the safety of any member of the school community or bring the school into disrepute.

3.2. Training

2.1. Staff and Governor Training

This school:

- ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- makes regular training available to staff on online safety issues and the school's online safety education programme.
- provides, as part of the induction process, all new staff (including those on university/college placements and work experience) and volunteers with information and guidance on the Online Safety Policy and procedures the school's Acceptable Use Agreements.

2.2. Parent Awareness and Training

This school operates a rolling programme of advice, guidance and training for parents, including:

- the introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear;
- the provision of information leaflets, articles in the school newsletter, on the school website;
- demonstrations and practical sessions held at the school;
- suggestions for safe Internet use at home;
- the provision of information about national support sites for parents.

3.3. Teaching and Learning

3.1. Why Internet use is Important

- **Internet use is part of the statutory curriculum and is a necessary tool for learning.**
- **The Internet is a part of everyday life for education, business and social interaction.**
- **The school has a duty to provide pupils with quality Internet access as part of their learning experience.**
- **Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.**
- *The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.*
- *Internet access is an entitlement for pupils who show a responsible and mature approach to its use.*

3.2. How Internet Use Benefits Education

Benefits of using the Internet in education include:

- *access to worldwide educational resources including museums and art galleries;*
- *inclusion in the National Education Network (NEN) which connects all UK schools [Click here to access NEN](#);*
- *educational and cultural exchanges between pupils worldwide;*
- *vocational, social and leisure use in libraries, clubs and at home;*
- *access to experts in many fields for pupils and staff;*
- *professional development for staff through access to national developments, educational materials and effective curriculum practice;*
- *collaboration across networks of schools, support services and professional associations;*
- *improved access to technical support including remote management of networks and automatic system updates;*
- *exchange of curriculum and administration data with the Local Authority and DfE;*
- *access to learning wherever and whenever convenient.*

3.3. How Internet Use Enhances Learning

This school:

- Has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE curriculum. This covers the teaching of a range of skills and behaviours which are appropriate to the age and experience of the pupils concerned and include those to:
 - STOP and THINK before they CLICK;
 - develop a range of strategies to evaluate and verify information before accepting its accuracy;
 - be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be;
 - know how to narrow down or refine a search;
 - [for older pupils] understand how search engines work and to understand that this affects the results they see at the top of the listings;
 - understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
 - understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
 - understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
 - understand why they must not post pictures or videos of others without their permission;
 - know not to download any files – such as music files – without permission;
 - have strategies for dealing with receipt of inappropriate materials;
 - [for older pupils] understand why and how some people will ‘groom’ young people for sexual reasons;
 - Understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying;
 - Know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind pupils about their responsibilities through an end-user Acceptable Use Agreement which will be displayed throughout the school or when they log on to the school’s network.
- ensures staff will model safe and responsible behaviour in their own use of technology during lessons;
- ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying online, online gaming/gambling etc.

3.4. Pupils with Additional Needs

- A fundamental part of teaching online safety is to check pupil’s understanding and knowledge of general personal safety issues. Some pupils may need additional teaching that includes reminders and explicit prompts to link their existing knowledge of “how to keep safe” to the rules that will apply specifically to, for instance, internet use.

3.4. Managing Information Systems

4.1. Maintaining Information Systems Security

- **The security of the school information systems and users will be reviewed regularly.**
- **Virus protection will be updated regularly.**
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus/malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school’s network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.

- use of user logins and passwords to access the school network will be enforced – see Section 6.2 below.

The school broadband and online suppliers are CLEO Broadband and Cumbria Schools ICT Support

4.2. Managing Email

- **Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.**
- **Whole-class or group email addresses will be used in primary schools for communication outside of the school.**
- **The official school email service may be regarded as safe and secure and is monitored.**
- **Users need to be aware that email communications may be monitored.**
- **Users must immediately report, to the nominated person – in accordance with the school Policy and procedures, 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.**

4.3. Emailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using email - emailing confidential data is not recommended and should be avoided where possible;
- The use of Hotmail, BTInternet, G-mail or any other Internet based webmail service for sending email containing sensitive information is not permitted;
- Where your conclusion is that email must be used to transmit such data:
 - Obtain express consent from your manager to provide the information by email;
 - Exercise caution when sending the email and always follow these checks before releasing the email:
 - Verify the details, including accurate email address, of any intended recipient of the information;
 - Do not copy or forward the email to any more recipients than is absolutely necessary.
 - Send the information as an encrypted document **attached** to an email;
 - Provide the encryption key or password by a **separate** contact with the recipient(s);
 - Do not identify such information in the subject line of any email;
 - Request confirmation of safe receipt.
 - Use only the initials of the person/ persons being discussed

4.4. Managing Published Content

- **The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information are not published.**

4.5. Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, pupils and parents 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. The school will inform and educate users about these risks and will implement procedures to reduce the likelihood of the potential for harm:

- We gain parental permission for the use of digital photographs or video involving their child as part of the school agreement form when their child joins the school. This is a once in a school lifetime consent. Parents are required to inform the school if their consent changes.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials.
- When using digital images on the school blog/ social media feeds, we adhere to our Media Permissions slips.
- Staff sign the school's Acceptable Use Agreement and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;

- Staff are allowed to take digital/video images to support educational aims, but must follow school procedures concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents.
- Parents sign a form to confirm whether they give consent or not for images and voice recordings of their child to be published in online media (which school directly controls) that will be available worldwide. No child will be identifiable from their work that is featured on any of the school media (e.g. the prospectus, the school website, school Twitter feed, school Blog).

4.6. Managing Social Networking, Social Media and Personal Publishing Sites

- The school will control access to social media and social networking sites – Children have no access to these and staff (where necessary) have access to the blog and Twitter feed.
- The official blog is password protected and accessed through iPads with approval from the Senior Leadership Team.
- Further guidance can be found in the document 'Safe Use of Facebook and Other Social Networking Sites' on the KAHSC website.
- *A sample advice leaflet for parents on Social Networking Sites, in particular, Facebook, can be found at Appendix H.*

4.7. Managing Filtering

- The school's broadband access includes filtering appropriate to the age and maturity of pupils.
- The school will work with the Schools System provider (Paul Maynard, Systems IT) to ensure that filtering procedures are continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the System provider who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list [Click here to access](#).
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF [Click here to access](#), Cumbria Police or CEOP [Click here to access](#).
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

4.8. Webcams

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs.
- Misuse of the webcam by any member of the school community will result in sanctions.
- Consent is sought from parents and staff on joining the school, in the same way as for all images.
- We use a designated workstation (Year 4 laptop) for Skype contact with other schools and Face Time through an iPad for specific learning opportunities.

4.9. Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

4.10. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 (enhanced by the General Data Protection Regulations, May 2018) which states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;

- Adequate, relevant and not excessive;
- Accurate;
- Kept no longer than is necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Only transferred to others with adequate protection.

More detailed information can be found in the School Data Protection Policy.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected;
- the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected);
- the device must offer approved virus and malware checking software;
- the data must be securely deleted from the device, in line with school procedures (below) once it has been transferred or its use is complete.

4.11. Disposal of Redundant ICT Equipment

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We 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
 - The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
 - Environment Agency Guidance (WEEE) [Click here to access](#)
 - ICO Guidance - Data Protection Act 1998/GDPR 2018 [Click here to access](#)
 - Electricity at Work Regulations 1989
- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.
- The school's disposal record will include:
 - Date item disposed of;
 - Authorisation for disposal, including:
 - verification of software licensing
 - any personal data likely to be held on the storage media? *
 - How it was disposed of e.g. waste, gift, sale
 - Name of person and/or organisation who received the disposed item

** if personal data is likely to be held the storage media will be over written multiple times or 'scrubbed' to ensure the data is irretrievably destroyed.*

3.5. Policy Decisions

5.1. Authorising Internet Access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the Staff Acceptable Use Agreement before using any school ICT resources.
- Parents will be asked to read and sign the School Acceptable Use Agreement for pupil access and discuss it with their child, where appropriate.

According to Setting Type:

- At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

5.2. Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit online ICT use/risks to establish if the Online Safety Policy and procedures is adequate and that the implementation of the Online Safety Policy is appropriate – see Appendix A for the audit template.
- Methods to identify, assess and minimise risks will be reviewed regularly.

5.3. Unsuitable/Inappropriate Activities

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					
	adult material that potentially breaches the Obscene Publications Act in the UK					
	criminally racist material in UK					
	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						
Using school systems to run a private business						
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school						
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions						

Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer / network access codes and passwords)					
Creating or propagating computer viruses or other harmful files					

5.4. What are the risks?

The risks that can be posed to young people and adults when online have been identified by the EUKids online project, which was later referenced in paragraph 1.3 of Dr Tanya Byron in "Safer Children in a Digital World" (2008).

	Commercial	Aggressive	Sexual	Values
Content (Child as recipient)	Adverts Spam Sponsorship Personal Info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias, Racist or Misleading info or advice
Contact (Child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers, Being groomed	Self-harm, Unwelcome persuasions
Conduct (Child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading information/advice

Byron Review (2008): [Click here to access](#)

5.6. Managing Cyber-bullying

- Cyber-bullying (along with all other forms of bullying) of any member of the school community will not be tolerated.
- There are clear procedures in place to support anyone in the school community affected by cyber-bullying.
- All incidents of cyber-bullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyber-bullying.

5.7. Managing The Blog

- SLT and staff will regularly update the blog and, with reference to the Media Permissions document, include appropriate photographs/ videos.

5.8. Managing Mobile Phones and Personal Devices

- The use of mobile phones and other personal devices by pupils and staff in school will be decided by the school and covered in the school Acceptable Use Agreement. Staff have designated areas where they can use their mobile phones within school.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/Behaviour Policy.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable materials, including those which promote pornography, violence or bullying.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour Policy or bullying procedures.
- If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

Pupils use of personal devices:

- The school strongly advises that pupil mobile phones should not be brought into school. However, the school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. If this is the case, the circumstances should be discussed with the class teacher and the normal rules regarding use during the school day will apply.
- If a pupil breaches the school procedures then the phone or device will be confiscated and will be held in a secure place in the school office.

Staff use of personal devices:

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone when on a school trip.
- Mobile phones and personally owned devices will be switched off or stored in a bag/ box in a cupboard.
- If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Senior Leadership Team.

3.6. Communicating Policy and procedures

6.1. Introducing the Policy and procedures to Pupils

- All users will be informed that network and Internet use will be monitored.
- An online safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An online safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- Online Safety rules or copies of the pupil Acceptable Use Agreement will be posted in all rooms with Internet access.

- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to Online Safety education will be given where pupils are considered to be vulnerable.

3.7. Acknowledgements

With thanks to Jeff Haslam (E-Safety Consultant), Hertfordshire County Council, Kent County Council, the South West Grid for Learning, Cumbria LSCB, CEOP, UKCCIS, Childnet and the DfE whose guidance and information has contributed to the development of this Policy and procedures.

THIS PAGE IS INTENTIONALLY BLANK FOR PRINTING PURPOSES

**SIR JOHN BARROW SCHOOL
ONLINE SAFETY AUDIT**

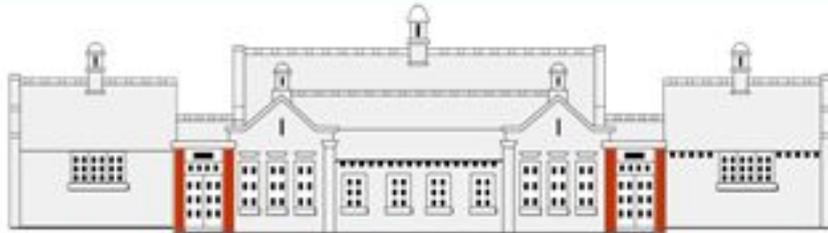
This self-audit is to be completed by the lead staff member and lead governor for e-safety. The outcomes of the audit are to be reported to the Finance, Buildings and Personnel Committee as part of the H&S standing agenda item.

Does the school have an Online Safety Policy and procedures	YES / NO
Date of latest update:	
Date of future review:	
The school Online Safety Policy and procedures was agreed by governors on:	
The Policy and procedures is available for staff to access at:	
The Policy and procedures is available for parents to access at:	
The responsible member of the Senior Leadership Team is:	
The Governor responsible for Online Safety is:	
The Designated Safeguarding Lead is:	
The Online Safety Coordinator is:	
Were all stakeholders (e.g. pupils, staff and parents) consulted when updating the school Online Safety Policy and procedures?	YES / NO
Has up-to-date Online Safety training been provided for all members of staff? (not just teaching staff)	YES / NO
Do all members of staff sign an Acceptable Use Agreement on appointment?	YES / NO
Are all staff made aware of the schools expectation around safe and professional online behaviour?	YES / NO
Is there a clear procedure for staff, pupils and parents to follow when responding to or reporting an online safety incident of concern?	YES / NO
Have online safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	YES / NO

Is online safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	YES / NO
Are online safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	YES / NO
Do parents or pupils sign an Acceptable Use Agreement?	YES / NO
Are staff, pupils, parents and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	YES / NO
Has an ICT security audit been initiated by SLT?	YES / NO
Is personal data collected, stored and used according to the principles of the Data Protection Act/GDPR?	YES / NO
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements?	YES / NO
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	YES / NO
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	YES / NO
Does the school log and record all online safety incidents, including any action taken?	YES / NO
Are the Governing Body and SLT monitoring and evaluating the school Online Safety Policy and procedures on a regular basis?	YES / NO

SIR JOHN BARROW SCHOOL

Rules for responsible use of technology



These rules will help you stay safe and be fair to others when using technology at SJB School.

I will not access other people's files

I will use the computers for school work and homework.

I will not bring in pen drives from outside school unless I have been given permission

I will not use the internet without permission

I will not share my home address or telephone number or arrange to meet someone

I will instantly report unpleasant material or messages sent to me to a member of staff

I understand that the school may check my files and may monitor the internet sites I visit

I will follow the SMART rules.

SIR JOHN BARROW SCHOOL

'Think then Click'

We ask permission before using the Internet.

We only use websites that our teacher has chosen.

We immediately close any webpage we don't like.

We only email people our teacher has approved.

We send emails that are polite and friendly.

We never give out a home address or phone number.

We never arrange to meet anyone we don't know.

We never use Internet chat rooms.

We tell the teacher if we see anything we are unhappy with.



PUPIL ACCEPTABLE USE AGREEMENT

SIR JOHN BARROW SCHOOL

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

- I will only use ICT in school for school purposes.
- I will not give my username and passwords to anyone else but my parents.
- If I think someone has learned my password then I will tell my teacher.
- I will only open/delete my own files.
- I will 'log-off' when I leave a computer.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out or share my own/or others details such as name, phone number or home address.
- I will be aware of 'stranger danger' when I am communicating online and will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online and will not show it to other pupils.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of the school ICT systems and email can be checked and my parent contacted if a member of school staff is concerned about my safety.
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher.

Pupil Acceptable Use – Pupil and Parent Agreement

Dear Parent,

ICT including the internet, email and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these online safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mr Connell or Mrs Pearson.

We have discussed this document with (child name) and we agree to follow the online safety rules and to support the safe use of ICT at Sir John Barrow School.

Parent Name		Pupil Class	
Signed (Parent)		Date	
Signed (Pupil)		Date	

STAFF / VOLUNTEER ACCEPTABLE USE POLICY AGREEMENT

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This Agreement is designed to ensure that all staff and volunteers are aware of their responsibilities when using any form of ICT. This applies to ICT used in school and also applies to use of school ICT systems and equipment out of school and use of personal equipment in school or in situations related to their employment by the school. All staff and volunteers (where they are using technology in school) are expected to sign this Agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr Connell (Online Safety Coordinator) or Mrs Pearson (Head teacher).

This Acceptable Use Agreement is intended to ensure that:

- staff and volunteers are responsible users and stay safe while using technologies for educational, personal and recreational use;
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- staff are protected from potential risk from the use of ICT in their everyday work and work to ensure that young people in their care are safe users.

Acceptable Use Agreement

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.

Keeping Safe

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will only use my own user names and passwords which I will choose carefully so they cannot be guessed easily. I will also change the passwords on a regular basis.
- I will not use any other person's user name and password.
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils.
- I will ensure that my data is regularly backed up.
- I will ensure that I 'log off' after my network session has finished.
- If I find an unattended machine logged on under another user's username, I will **not** continue using the machine – I will 'log off' immediately.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.
- I will not accept invitations from school pupils to add me as a friend to their social networking sites, nor will I invite them to be friends on mine.

As damage to professional reputations can inadvertently be caused by quite innocent postings or images, I will also be careful with who has access to my pages through friends and friends of friends, especially with those connected with my responsibilities as a Governor at the school, such as parents and their children.

- I understand that data protection requires that any personal data that I have access to must be kept private and confidential, except when it is deemed necessary that I am required by law or by school procedures to disclose it an appropriate authority.
- I will only transport, hold, disclose or share personal information about myself or others as outlined in the school personal data guidelines. I will not send personal information by email as it is not secure.
- Where personal data is transferred outside the secure school network, it must be encrypted. Personal data can only be taken out of school or accessed remotely when authorised, in advance, by the Head teacher or Governing Body. Personal or sensitive data taken off site in an electronic format must be encrypted, e.g. on a password secured laptop or memory stick. Staff leading a trip are expected to take relevant pupil information with them but this must be held securely at all times.
- I will ensure that any private social networking sites/blogs etc. that I create, or actively contribute to:
 - do not reveal confidential information about the way the school operates
 - are not confused with my school responsibilities in any way.
- I will not try to bypass the filtering and security systems in place.
- I will only use my personal ICT in school for permissible activities and I will follow the rules set out in this agreement. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

Promoting Safe Use by Learners

- I will support and promote the school's Online Safety, Data Protection and Behaviour Policies and help pupils to be safe and responsible in their use of ICT and related technologies.

- I will model safe use of the internet in school.
- I will educate young people on how to use technologies safely according to the school teaching programme.
- I will take immediate action in line with school procedures if an issue arises in school that might compromise a learner, user or school safety or if a pupil reports any concerns.

Communication

- I will only use the school's email/Internet/Intranet/Learning Platform and any related technologies for professional purposes or for uses deemed 'acceptable' by the Head teacher or Governing Body.
- I will communicate on-line in a professional manner and tone, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions. Anonymous messages are not permitted.
- I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- I will only communicate with pupils and parents using the school's approved, secure email system(s). Any such communication will be professional in tone and manner.
- I am aware that any communication could be forwarded to an employer or governors.
- I will only use chat and social networking sites that are approved by the school.
- I will not use personal email addresses on the school ICT systems unless I have permission to do so.

Research and Recreation

- I will not browse, upload, download, distribute or otherwise access any materials which are illegal, discriminatory or inappropriate or may cause harm or distress to others.
- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity.
- I know that all school ICT is primarily intended for educational use and I will only use the systems for personal or recreational use if this is allowed by the school.

Sharing

- I will not access, copy, remove or otherwise alter any other user's file, without their permission.
- I will respect the privacy and ownership of others' work online at all times and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission, and will credit them if I use it.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos). If I am unsure about this, I will seek advice.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes using school equipment in line with school procedures.
- I will only take images/video of pupils and staff where it relates to agreed learning and teaching activities and will ensure I have parent/staff permission before I take them.
- If images are to be published on-line or in the media I will ensure that parental/staff permission allows this.
- I will not use my personal equipment to record images/video unless I have permission to do so from the Head teacher or other Senior Manager.
- I will not keep images and/or videos of pupils stored on my personal equipment unless I have permission to do so. If this is the case, I will ensure that these images cannot be accessed or copied by anyone else or used for any purpose other than that for which I have permission.
- Where these images are published (e.g. on the school website/prospectus), I will ensure that it is not possible to identify the people who are featured by name or other personal information.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.

Problems

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the Online Safety Coordinator or Head teacher.
- I will not install any hardware or software on a computer or other device without permission of the Systems Manager.
- I will not try to alter computer settings without the permission of the Systems Manager.
- I will not cause damage to ICT equipment in school.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- 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 understand this forms part of the terms and conditions set out in my contract of employment.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action.

Staff/Volunteer Acceptable Use Agreement

I will use the school network in a responsible way and observe all the restrictions as explained in the staff ICT Acceptable Use Agreement and Data Protection Policy. I agree to use ICT by these rules when:

- ✓ I use school ICT systems at school or at home when I have permission to do so
- ✓ I use my own ICT (where permitted) in school
- ✓ I use my own ICT out of school to access school sites or for activities relating to my employment by the school

Staff/Volunteer Name			
Job Title (where applicable)			
Signed		Date:	

SOCIAL NETWORKING SITES - FACEBOOK GUIDANCE FOR PARENTS

There are many children of Primary School age who have Facebook Profiles despite the permitted minimum age to use the site being 13, according to the site terms and conditions.

Our school is committed to promoting the safe and responsible use of the Internet and as such we feel it is our responsibility to raise this particular issue as a concern. Whilst children cannot access Facebook or other social networking sites at school, they could have access to it on any other computer or mobile technology. Websites such as Facebook offer amazing communication and social connections, however they are created with their audience in mind and this is specifically 13 years old. Possible risks for children under 13 using the site may include:

- Facebook use 'age targeted' advertising and therefore your child could be exposed to adverts of a sexual or other inappropriate nature, depending on the age they stated they were when they registered;
- Children may accept 'friend requests' from people they don't know in real life which could increase the risk of inappropriate contact or behaviour;
- Facebook is one of the social networking sites used by those attempting to radicalise young people;
- Language, games, groups and content posted or shared on Facebook is not moderated, and therefore can be offensive, illegal or unsuitable for children;
- Photographs shared by users are not moderated and therefore children could be exposed to inappropriate images or even post their own;
- Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and other options;
- Facebook could be exploited by bullies and for other inappropriate contact;
- Facebook cannot and does not verify its members therefore it important to remember that if your child can lie about who they are online, so can anyone else!

We feel that it is important to point out to parents the risks of underage use of such sites, so you can make an informed decision as to whether to allow your child to have a profile or not. These profiles will have been created away from school and sometimes by a child, their friends, siblings or even parents. We will take action (such as reporting aged profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our children.

Should you decide to allow your children to have a Facebook profile we strongly advise you to:

- Check their profile is set to private and that only 'friends' can see information that is posted;
- Monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information and not posting offensive messages or photos;
- Ask them to install the CEOP (Child Exploitation and Online Protection Centre) application from www.facebook.com/clickceop on their profile. This places a bookmark on their profile to CEOP and the 'Report Abuse' button which has been known to deter offenders;
- Have a look at the advice for parents from Facebook www.facebook.com/help/?safety=parents;
- Set up your own profile so you understand how the site works and ask them to add you as a friend on their profile so you can keep track of what they are posting online;
- Make sure your child understands the following rules:
 - Always keep your profile private;
 - Never accept friends you don't know in real life;

- Never post anything which could reveal your identity;
- Never post anything you wouldn't want your parents to see;
- Never agree to meet someone you only know online without telling a trusted adult;
- Always tell someone if you feel threatened or someone upsets you.

We recommend that all parents visit the CEOP ThinkUKnow website for more information on keeping your child safe online [Click here to access](#).

- **UK Council for Child Internet Safety (UKCCIS):** [Click here to access](#)
- **Wise Kids:** [Click here to access](#)
- **Teem:** [Click here to access](#)
- **Know the Net:** [Click here to access](#)
- **Family Online Safety Institute:** [Click here to access](#)
- **e-safe Education:** [Click here to access](#)
- **Facebook Advice to Parents:** [Click here to access](#)
- **Test your online safety skills:** [Click here to access](#)

The above internet site links were correct at the time of publishing. School staff are advised to check the content of each site prior to allowing access to pupils.

Department for Education/Home Office guidance for schools

PREVENT Duty statutory guidance for Public Bodies: England and Wales – March 2015

The PREVENT Duty – non-statutory Departmental advice for Schools and Childcare Providers – DfE – June 2015

How Social Media is used to encourage travel to Syria and Iraq – Home Office advice to schools – June 2015

LEGAL FRAMEWORK

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools should have a copy of The Home Office "Children & Families: Safer from Sexual Crime" document as part of their child protection packs. [Click here to access.](#)

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998 (enhanced by the General Data Protection Regulations, May 2018)

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

The Computer Misuse Act 1990 (sections 1 - 3)

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Public Order Act 1986 (sections 17 — 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
 - Ascertain whether the communication is business or personal;
 - Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess “extreme pornographic image”

63 (6) must be “grossly offensive, disgusting or otherwise obscene”

63 (7) this includes images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead” must also be “explicit and realistic”. Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyber-bullying/ Bullying:

- Head teachers have the power “to such an extent as is reasonable” to regulate the conduct of pupils off site.
- School staff are able to confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying procedures.

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial.
- The right to respect for private and family life, home and correspondence.
- Freedom of thought, conscience and religion.
- Freedom of expression.
- Freedom of assembly.
- Prohibition of discrimination.
- The right to education.

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

GLOSSARY OF TERMS

Becta	British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology) – <i>NOTE: Becta Closed in 2011</i>
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes).
CLEO	The Regional Broadband Consortium of Cumbria and Lancashire – is the provider of broadband and other services for schools and other organisations in Cumbria and Lancashire

CPD	Continuous Professional Development
DfE	Department for Education
FOSI	Family Online Safety Institute
HSTF	Home Secretary's Task Force on Child Protection on the Internet
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by Naace Click here to access
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network.
KS1	Key Stage 1 (2, 3, 4 or 5) – schools are structured within these multiple age groups e.g. KS3 = years 7 to 9 (age 11 to 14)
LA	Local Authority
LAN	Local Area Network
Learning Platform	A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
LSCB	Local Safeguarding Children Board
MIS	Management Information System
MLE	Managed Learning Environment
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. CLEO in Cumbria) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
RBC	Regional Broadband Consortia (e.g. CLEO) have been established to procure broadband connectivity for schools in England. There are 13 RBCs covering most local authorities in England, Wales and Northern Ireland.
SEF	Self Evaluation Form – used by schools for self-evaluation and reviewed by Ofsted prior to visiting schools for an inspection
TUK	Think U Know – educational E-Safety programmes for schools, young people and parents.
URL	Uniform Resource Locator (URL) it is the global address of documents and other resources on the World Wide Web.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol