

Berrycoombe School

E- Safety Policy



Berrycoombe School is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment. ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Berrycoombe we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. E-safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Berrycoombe School. Our E-Safety Policy has been written following government guidance. It has been agreed by senior management and approved by governors. The school's E-Safety Governor is Hannah Fugil, our Designated Safeguarding Officer is Craig Robertson and Steven Coles is our E-Safety Coordinator. The E-Safety Policy and its implementation shall be reviewed annually. It will be reviewed in the Spring term 2022.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The role of the E-Safety Governor will include:

- Regular meetings with the E-Safety Committee.
- Regular monitoring of E-Safety incident logs.
- Reporting to the Behaviour & Safety Committee.

Headteacher and Senior Leadership Team:

The Headteacher is responsible for ensuring the safety (including E-Safety) of members of the school community, though the day-to-day responsibility for E-Safety will be delegated to the E-Safety Coordinator. The Headteacher/Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.

The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. The Headteacher and Assistant Heads should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.

The E-Safety Coordinator:

- Takes day-to day-responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policy/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Provides training and advice for staff.
- Liaises with school ICT technical staff.
- Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments.

All School Staff:

All staff, including non-classroom based staff, will receive regular training and updates regarding E-safety, cyber-bullying, sexting, Child Exploitation and Radicalisation, including face to face and online training sessions as appropriate to ensure that they are aware of the latest developments. They will all be aware of the flow chart of procedures to follow in the case of an E-safety incident.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience. The school Internet access will be designed expressly for pupil use, including appropriate content filtering. Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. As part of the 2014 Computing curriculum, all year groups have digital literacy units within the Twinkl E-Safety Scheme of Work that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying. Children also receive a discreet series of lessons in the Autumn term to address E-Safety, including cyber-bullying, sexting, Child Exploitation and Radicalisation delivered in a way that is appropriate to each year group.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through meetings our SEN co-ordinator and individual teachers to ensure all children have equal access to succeeding in this subject. Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.

Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to E-Safety and agree to its use. All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. In addition to this, every school device will show a user an applicable acceptable usage criterion before they log on to that device. This includes the pupil iPads. Parents will be informed that pupils will be provided with supervised Internet access. Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be Managed. If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the E-Safety Coordinator. The unsuitable site will then be added to the blocked site on the Smoothwall filtering. Staff will follow the procedures detailed in the Appendix with regard to reporting incidences of a serious nature. The Blocked Logs on Smoothwall will be reviewed monthly by the E-Safety Coordinator. The school will work in partnership with DNS, the provider of the school's network support to ensure that the Smoothwall filtering is as effective as possible at all times. This will be reviewed annually.

E-mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of E-Safety: Pupils have no access to email within school. Access in school to external personal e-mail accounts is not allowed. All official communications which are work related must be sent by staff to and from their work email

address as supplied by the school. Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' their laptop if they are going to leave it unattended. If passwords are to be kept on devices for reference, all staff will use Keeypass to store them securely.

Social Networking

Social networking Internet sites (such as, MySpace, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact. The Use of social networking sites and newsgroups by pupils in the school, is not allowed and will be blocked/filtered. Teacher have access to Facebook as it is currently used as a tool in which to communicate with parents. Each class has a Facebook Page which is managed by the class teacher, which in turn is linked to one Facebook profile that is controlled by the E-Safety Coordinator. These pages and profile were set up in collaboration with Richard Jones, Head of ICT Services for Truro and Penwith Academy Trust (TPAT), and have the appropriate privacy settings to ensure they are not misused by any external individuals.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others. Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Parents should only upload pictures of their own child/children onto their personal social networking sites.

Reporting

All breaches of the E-Safety policy need to be recorded via the E-Safety Coordinator, the Headteacher and the governor for E-Safety. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to one of the Designated Child Protection Officers immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to the E-Safety in the same day. Allegations involving staff should be reported to the Headteachers. If the allegation is one of abuse, then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary, the local authority's LADO should be informed. Evidence of incidents must be preserved and retained. The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted, adult, Childline)

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact. Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the secretary at 8:50 and collected at the end of the day.

The sending of abusive or inappropriate text messages is forbidden.

Staff should always use the school phone to contact parents.

Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day.

Staff may use their mobile phones in the staffroom/one of the school offices. No school related information may be accessed or stored on staffs' personal mobile devices.

Parents cannot use mobile phones on school trips to take pictures of the children. On school trips teachers can use personal mobile for emergency only.

Digital/Video Cameras/Photographs

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred. Pupils will not use digital cameras, video equipment or camera apps at school unless specifically authorised by staff. Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.

Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background. The Head Teacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner. Staff should always use

a school camera or iPad to capture images and should not use their personal devices. The exception to this is where a camera has been logged by the E-Safety Coordinator and the serial number of the camera noted. Photos taken by the school are subject to the Data Protection act.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents. Contact details on the Website will be the school address, e-mail and telephone number. Staff and pupils' personal information will not be published. The Head Teacher and PSA will take overall editorial responsibility and ensure that content is accurate and appropriate. Photographs and videos that include pupils will be selected carefully and will not include children for whom permission to use their photo has not been granted. Pupils' full names will not be used in association with photographs. Consent from parents will be obtained before photographs of pupils are published on the school Website. Work will only be published with the permission of the pupil.

Information System Security

School ICT systems capacity and security will be reviewed regularly. Virus protection will be installed and updated regularly by the school network support: DNS. Security strategies will be discussed and reviewed regularly by the Online Safety Committee and our filtering suppliers and those arrangements incorporated in to our agreement with them.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act.

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of internet access. The school will audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate.

Handling E-Safety Complaints

Complaints of internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Head

Teacher. Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure.

Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils:

Rules for keeping safe on-line will be made explicit when teachers are delivering the E-Safety element of the Computing curriculum. Pupils will be informed that internet use will be monitored. Pupils will be informed of that the use of social networking websites have age restrictions beyond those of a Primary aged child.

Staff:

All staff will be given the School E-Safety Policy and its importance explained.

Parents:

Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the school Website.

Appendices

- Student / Pupil Acceptable Usage Policy
- Staff and Volunteers Acceptable Usage Policy
- Parents / Carers Acceptable Usage Policy Agreement
- Use of Digit/Video Images
- School Filtering Policy
- School Password Security Policy
- School Personal Data Policy
- School E-Safety Charter
- Ideas for schools to consider
- Legislation
- Links to other organisations and documents
- Resources
- Glossary of terms

Pupil Acceptable Use Policy Agreement

School Policy

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 information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

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

Acceptable Use Policy 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.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal hand held / external devices (USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not use chat and social networking sites in school

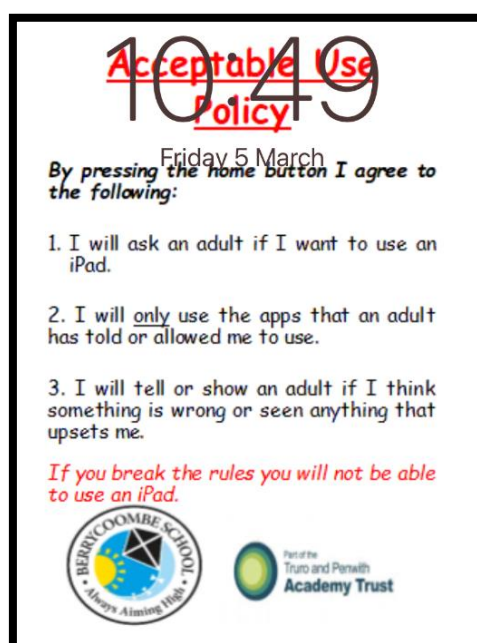
When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

This acceptable usage policy and its content will be explicitly shared with each student as part of a whole class session once every academic year. In addition to this, every time a pupil uses an iPad they will view, read and agree to the acceptable usage policy located on the screen of the iPads before they access the home screen:



The image shows a screenshot of a digital document titled "Acceptable Use Policy" with the time "10:49" displayed in large red numbers. The text is as follows:

Acceptable Use Policy
10:49

Friday 5 March
By pressing the home button I agree to the following:

1. I will ask an adult if I want to use an iPad.
2. I will only use the apps that an adult has told or allowed me to use.
3. I will tell or show an adult if I think something is wrong or seen anything that upsets me.

If you break the rules you will not be able to use an iPad.

At the bottom, there are two logos: the circular logo for "BERRYCOOMBE SCHOOL" with the motto "Always Aiming High", and the logo for "Part of the Truro and Penwith Academy Trust".

Staff and Volunteers Acceptable Use Policy Agreement

School Policy

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 information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy 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. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.

- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will store my usernames and password in Keepass.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- Use of personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school is not permitted. If, for any reason beyond the school's control, it is necessary for the usage of a personal device, this will have to be authorised by the E-Safety Committee and a Bring Your Own Device to Work Policy (BYOD) will have to be created and implemented.
- I will not use my personal devices to access school emails, any electronic platform used within school or access the server remotely.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/ security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others on devices provided by the school, as outlined in the School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

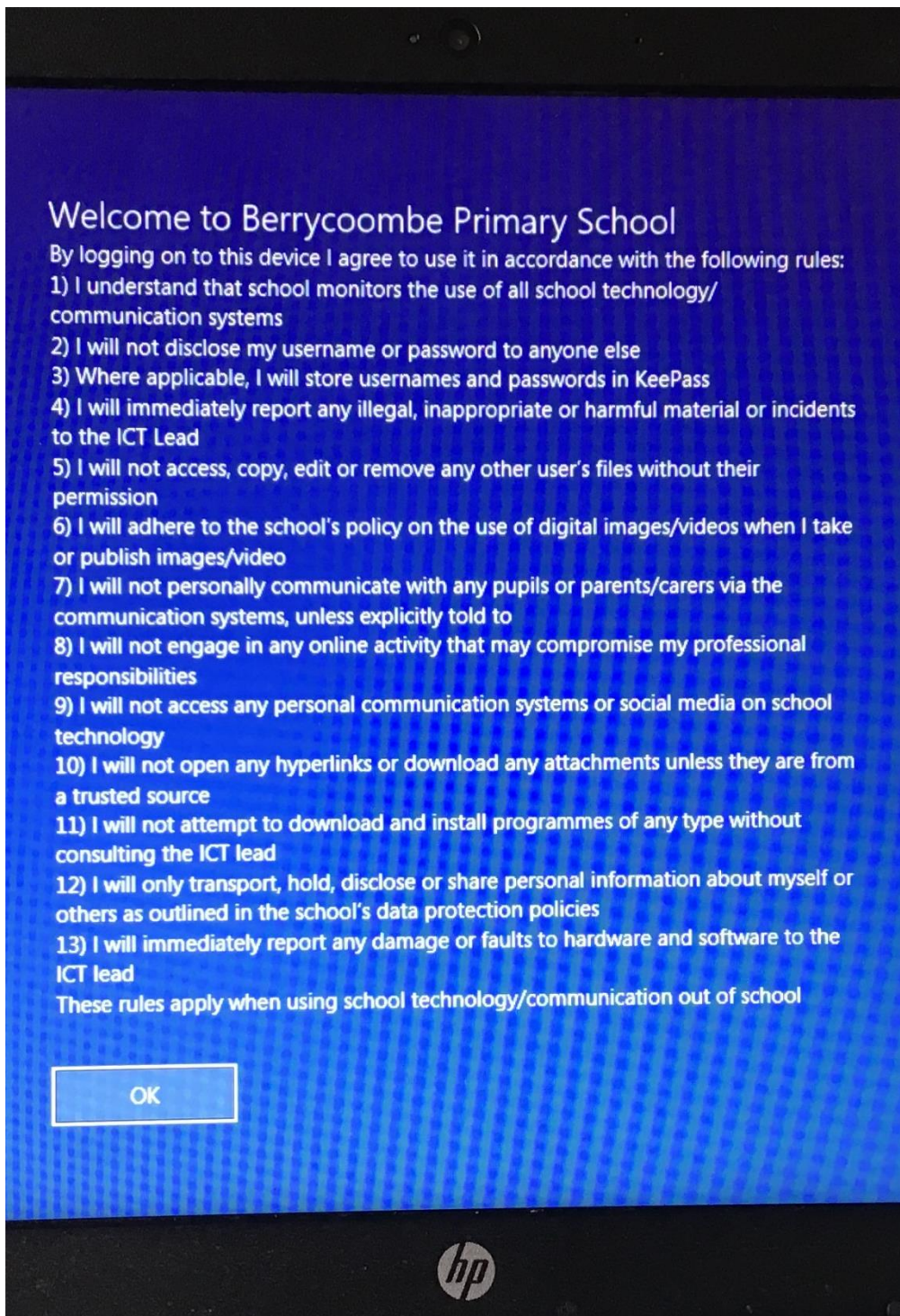
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

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

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

This acceptable usage policy and its content will be explicitly shared with each member of staff once every academic year and with volunteers when applicable. In addition to this, every time a member of staff or volunteer uses a laptop or desktop provided by the school they will view, read and agree to the acceptable usage policy located on home screen before being able to log on and use the laptop or desktop:



Parent / Carer Acceptable Use Policy Agreement

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 information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students / pupils* will have good access to ICT to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

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

Permission Form

Parent / Carers Name:

Pupil Name:

As the parent / carer of the above *pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school. I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

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

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

Signed:

Date:

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

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

Parents are requested to sign the permission form below to allow the school to take and use images of their children.

Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *student* I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school. I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed

Date

School Filtering Policy

Introduction

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

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the E-safety/ICT Co-ordinator. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

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

- be logged in change control logs
- be reported to a second responsible person - Angela Clay
- be reported to the E-Safety Committee every term in the form of an audit of the change control logs

All users have a responsibility to report immediately to ICT Co-ordinator or Craig Robertson any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

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

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

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

- *signing the AUP*
- *induction training*
- *staff meetings, briefings, Inset.*

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

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the ICT Co-ordinator/ESafety who will decide whether to make school level changes (as above). If it is felt that the site should be filtered (or unfiltered) at a higher level, the responsible person should email NCI Ltd with the URL.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use agreement. Monitoring will take place as follows:

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person (Craig Robertson)
- E-Safety Committee
- E-Safety Governor
- Local Authority on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

School Password Security Policy

Introduction

The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email and Virtual Learning Environment (VLE).

Responsibilities

The management of the password security policy will be the responsibility of E-Safety/ICT Coordinator.

All users (adults and young people) will have responsibility for the security of their username and password, 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.

Passwords for new users, and replacement passwords for existing users can be allocated by ESafety/ICT Co-ordinator.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in ICT and / or e-safety lessons (the school should describe how this will take place)
- through the Acceptable Use Agreement

Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).

All users (at KS1 and above) will be provided with a username and password by the ICT Coordinator who will keep an up to date record of users and their usernames.

The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (Keepass). (Alternatively, where the system allows more than one "master / administrator" log-on, the Headteacher or other nominated senior leader should be allocated those master / administrator rights. A school should never allow one user to have sole administrator access).

Audit / Monitoring / Reporting / Review

The responsible person (E-Safety/ICT co-ordinator) will ensure that full records are kept of:

- User IDs and requests for password changes
- User log-ons
- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

Local Authority Auditors also have the right of access to passwords for audit investigation purposes

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by *the* E-Safety Committee at termly intervals.

This policy will be regularly reviewed termly in response to changes in guidance and evidence gained from the logs.

School Personal Data Handling Policy

Introduction

Schools should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature (Becca – Good Practice in information handling in schools – keeping data secure, safe and legal – Sept 2008).

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Any loss of personal data can have serious effects for individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. All transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow “good information handling principles”.

Policy Statements

The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the “Fair Processing Code” and lawfully processed in accordance with the “Conditions for Processing”.

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils / students, members of staff and parents and carers eg names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Curricular / academic data eg class lists, pupil / student progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members

Responsibilities

The school's Senior Risk Information Officer (SIRO) is the Headteacher. They will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) for the various types of data being held (eg pupil / student information / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand :

- what information is held and for what purpose
- how information has been amended or added to over time
- who has access to protected data and why

The designated IAOs are:

Craig Robertson - Assessment Data (SIMS)

Nicola Donnithorne - Assessment Data (SIMS)

Kath Williams - SEN Data (SIMS)

Natalie Dowling - (SIMS)

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers – the “Fair Processing Notice”

Under the “Fair Processing” requirements in the Data Protection Act, the school will inform parents / carers of all pupils / students of the data they hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DCSF, QCA, Connexions etc) to whom it may be passed. This fair processing notice will be passed to parents / carers through the Prospectus and School Website.

Training & Awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

Identification of Data

The school will ensure that all school staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher.

All documents (manual or digital) that contain protected data will be labelled clearly with the Impact

Level shown in the header and the Release and Destruction classification in the footer:

Impact levels are as follows:

- IL1–Not Protectively Marked (IL1–NPM)
- IL2–Protect
- IL3–Restricted
- IL4–Confidential

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data.

Release and destruction markings will be shown in the footer as follows:

| [Release] | [Parties] | [Restrictions] | [Encrypt, Securely delete or shred] |
|-------------------------------|---|--|--|
| The authority descriptor | The individuals or organisations the information may be released to | Descriptor tailored to the specific individual | How the document should be destroyed |
| Examples: | | | |
| Senior Information Risk Owner | School use only | No internet access No photos | Securely delete or shred |
| Teacher | Mother only | No information to father ASBO | Securely delete or shred |

Secure Storage of and Access to Data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

All users will be given secure user names and strong passwords which must be changed regularly.

User names and passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media)

Private equipment (ie owned by the users) must not be used.

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 policy (below) once it has been transferred or its use is complete

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

All paper based IL2-Protected and IL3-Restricted (or higher) material must be held in lockable storage.

The school recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests ie. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure Transfer of Data and Access out of School

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.

- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

Disposal of Data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance (see further reading section for reference to the Cabinet Office guidance), and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

As required by the "Data Handling Procedures in Government" document, the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an acceptable use policy, for example. Specific security events should be archived and retained at evidential quality for seven years.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident
- a communications plan, including escalation procedures
- and results in a plan of action for rapid resolution and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Further Reading

Teachernet – Data processing and sharing -

<http://www.teachernet.gov.uk/management/atoz/d/dataprocessing/>

Office of the Information Commissioner website:

<http://www.informationcommissioner.gov.uk>

Office of the Information Commissioner – guidance notes: Access to pupil’s information held by schools in England

Becta – Good Practice in information handling in schools – keeping data secure, safe and legal and it’s four detailed appendices: (September 2008)

http://schools.becta.org.uk/upload-dir/downloads/information_handling.pdf

http://schools.becta.org.uk/upload-dir/downloads/information_handling_impact_levels.pdf

http://schools.becta.org.uk/upload-dir/downloads/data_encryption.pdf

http://schools.becta.org.uk/upload-dir/downloads/audit_logging.pdf

http://schools.becta.org.uk/upload-dir/downloads/remote_access.pdf

Cabinet Office – Data handling procedures in Government – a final report (June 2008)

http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

Online Safety – A School Charter for Action

Name of School – Berrycoombe School

We are working with staff, pupils and parents / carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of ICT, and follows agreed policies to minimise potential e-safety risks.

Our school community

Discusses, monitors and reviews our e-safety policy on a regular basis. Good practice suggests the policy should be reviewed annually or at most every two years.

Supports staff in the use of ICT as an essential tool for enhancing learning and in the embedding of e-safety across the whole school curriculum.

Ensures that pupils are aware, through e-safety education, of the potential e-safety risks associated with the use of ICT and mobile technologies, that all e-safety concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the school's e-safety policy.

Provides opportunities for parents/carers to receive e-safety education and information, to enable them to support their children in developing good e-safety behaviour. The school will report back to parents / carers regarding e-safety concerns.

Parents/carers in turn work with the school to uphold the e-safety policy. Seeks to learn from e-safety good practice elsewhere and utilises the support of relevant organisations when appropriate.

Chair of Governors

Headteacher

Pupil Representative

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

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.

Data Protection Act 1998

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.

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.

Communications Act 2003

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.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

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.

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.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright

covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

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.

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.

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.

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.

Sexual Offences Act 2003

The new grooming offence 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 fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

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

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.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and

empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Links to Other Organisations or Documents

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

SOUTH WEST GRID FOR LEARNING:

"SWGfL Safe" - <http://www.swgfl.org.uk/safety/default.asp>

Child Exploitation and Online Protection Centre (CEOP)

<http://www.ceop.gov.uk/>

ThinkUKnow

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

CHILDNET

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

INSAFE

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

BYRON REVIEW ("Safer Children in a Digital World")

<http://www.dcsf.gov.uk/byronreview/>

Becta

Website e-safety section -

<http://schools.becta.org.uk/index.php?section=is>

Developing whole school policies to support effective practice:

<http://publications.becta.org.uk/display.cfm?resID=25934&page=1835>

Signposts to safety: Teaching e-safety at Key Stages 1 and 2 and at Key Stages 3 and 4:

<http://publications.becta.org.uk/display.cfm?resID=32422&page=1835>

"Safeguarding Children in a Digital World"

http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_tlr_s_03&rid=13344

LONDON GRID FOR LEARNING

<http://cms.lgfl.net/web/lgfl/365>

KENT NGfL

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

NORTHERN GRID

http://www.northerngrid.org/ngflwebsite/esafety_server/home.asp

NATIONAL EDUCATION NETWORK

NEN E-Safety Audit Tool: http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html

CYBER-BULLYING

DCSF - Cyberbullying guidance

<http://publications.teachernet.gov.uk/default.aspx?PageFunction=productdetails&PageMode=spectrum&ProductId=DCSF-00658-2007>

Teachernet

<http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/>

Teachernet "Safe to Learn – embedding anti-bullying work in schools"

<http://www.teachers.gov.uk/wholeschool/behaviour/tacklingbullying/safetolearn/>

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

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

East Sussex Council – Cyberbullying - A Guide for Schools:

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

References to other relevant anti-bullying organisations can be found in the appendix to the DCSF publication "Safe to Learn" (see above)

SOCIAL NETWORKING

Home Office Task Force - Social Networking Guidance -

<http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protectiontaskforce>

Digizen – "Young People and Social Networking Services":

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

Ofcom Report:

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

MOBILE TECHNOLOGIES

“How mobile phones help learning in secondary schools”:

http://partners.becta.org.uk/index.php?section=rh&catcode=re_rp_02_a&rid=15482

Mobile phones and cameras:

http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_mob_03

DATA PROTECTION AND INFORMATION HANDLING

Information Commissioners Office - Data Protection:

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

BECTA - Data Protection:

http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_saf_dp_03

PARENTS GUIDES TO NEW TECHNOLOGIES AND SOCIAL NETWORKING:

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

Resources

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

http://www.swgfl.org.uk/safety/safetyresources.asp?page=schoolst_resources&audienceid=3

BBC Chatguides: <http://www.bbc.co.uk/chatguide/index.shtml>

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

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

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

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

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

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

Digizen – cyber-bullying films:

<http://www.digizen.org/cyberbullying/film.aspx>

London Grid for Learning: <http://cms.lgfl.net/web/lgfl/safety/resources>

College of Policing - radicalisation nalt.com/channel_general_awareness/

Glossary of Terms

AUP Acceptable Use Policy – see templates earlier in this document

Becta British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology)

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.

CPD Continuous Professional Development

CYPS Children and Young Peoples Services (in Local Authorities)

DCSF Department for Children, Schools and Families

ECM Every Child Matters

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 Becta

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 and RBCs.

KS1 .. Key Stage 1 (2, 3, 4 or 5) – schools are structured within these multiple age groups eg 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

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 have been established to procure broadband connectivity for schools in England. There are 10 RBCs covering 139 of the 150 local authorities.

SEF Self Evaluation Form – used by schools for self-evaluation and reviewed by Ofsted prior to visiting schools for an inspection

SRF Self Review Form – a tool used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark

SWGfL South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW

TUK Think U Know – educational e-safety programmes for schools, young people and parents.

VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP Wireless Application Protocol