Shebbear College

E–Safety Policy

From EYFS to Sixth Form

Last reviewed by Governing Body – 9th November 2017

Next Review Date by Governing Body by November 2018

Policy Review at Shebbear College

The Governors acknowledge their responsibility to ensure that this policy is effective and follows regulatory requirements. Governors undertake a regular review (at least annually) to satisfy themselves that the implementation of this policy is effective.

Introduction

Shebbear College believes that the use of information and communication technologies in our school brings great benefits.

Recognising the e-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications. This policy will help our school to review our e-Safety regularly.

Table of contents

2.1 Who will write and review the policy?

2.2 Teaching and Learning

2.2.1 Why is Internet use important?

2.2.2 How does Internet use benefit education?

2.2.3 How can Internet use enhance learning?

2.2.4 How will pupils learn how to evaluate content?

2.3 Managing Information Services

2.3.1 How will information systems security be maintained?

2.3.2 How will email be managed?

2.3.3 How will published content be managed?

2.3.4 Can pupil images and work be published?

2.3.5 How will social networking and personal publishing be managed?

2.3.6 How will filtering be managed?

2.3.7 How will videoconferencing be managed?

2.3.8 How can emerging technologies be managed?

2.3.9 How should personal data be protected?

2.4 Policy Decisions

2.4.1 How will Internet access be authorised?

2.4.2 How will risks be assessed?

2.4.3 How will complaints be handled?

2.4.4 How should the Internet be used across the community?

2.4.5 How will Cyber bullying be managed?

2.4.6 How will Learning Platforms be managed?

2.5 Communications Policy

2.5.1 How will the policy be introduced to pupils?

2.5.2 How will the policy be discussed with staff?

2.5.3 How will parents’ support be enlisted?

2.1 Who will write and review this policy?

The e–Safety Policy is a key element of our Child Protection and Safeguarding Policy and our Anti-Bullying Strategy. It also relates to other policies including those for behaviour, personal, social and health education (PSHE) and for citizenship. Policy construction provides an opportunity to review practice and the more that staff, parents, governors and pupils are involved in deciding the policy, the more effective it will be.

The school has appointed an e–Safety Coordinator. This is the Designated Safeguarding Lead, **Mr Matthew Newitt.**

The network manager is Mr Dave Balman. The governors involved in the formulation of this policy are **Nick Buckland** (who has oversight of Digital Technology) and **Rev Simon Leigh** (who has oversight of Safeguarding and Child Protection)

The e–Safety Policy and its implementation is reviewed annually.

Our e–Safety Policy has been written by the SMT, building on the e–Safety Policy suggestions and government guidance. It has been agreed by the Senior Management Team and approved by the governing body.

2.2 Teaching and learning

2.2.1 Why is Internet use important?

The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through ICT and Internet use.

Internet use is part of the statutory curriculum and 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 students 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 students who show a responsible and mature approach to its use.

2.2.2 How does Internet use benefit education?

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;

- inclusion in the National Education Network which connects all UK schools;

- 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.

- Access to learning wherever and whenever convenient.

2.2.3 How can Internet use enhance learning?

Increased computer numbers and improved Internet access may be provided but its impact on pupils learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Methods to detect plagiarism may need to be developed.

The school's Internet access is designed to enhance and extend education.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Shebbear College will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

- This education is delivered in all subjects, tutorials, ICT and PSHE

2.2.4 How will pupils learn how to evaluate Internet content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy provide an opportunity for pupils to develop skills in evaluating Internet content. For example researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of. **If in doubt about this type of situation seek advice from the Deputy Head (Pastoral)**

The following statements require adaptation according to the pupils' age:

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The evaluation of online material

- Materials are a part of teaching/learning in every subject.

- Making sound judgements in relation to viewing and being involved in downloading materials

2.3 Managing Information Systems

2.3.1 How will information systems security be maintained?

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

ICT security is a complex matter and cannot be dealt with adequately in this document.

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.

- Users must take responsibility for their network use. For Shebbear College staff, disregarding the ICT acceptable use policy may be regarded as a reason for dismissal.

- Workstations should be secured against user mistakes and deliberate actions.

- Servers must be located securely and physical access restricted.

- The server operating system must be secured and kept up to date.

- Virus protection for the whole network must be installed and current.

- Access by wireless devices must be proactively managed.

The security of the school information systems and users will be reviewed regularly.

Virus protection will be updated regularly.

- Unapproved software will not be allowed in pupils' work areas or attached to email.

- Files held on the school's network will be regularly checked.

- The network manager reviews system capacity regularly.

- **A regular meeting is held by the DSL (Mr Matthew Newitt), Mr Dave Balman and Ms Marianne Davies (teacher of ICT/Computer Science) to discuss all aspects of E Safety. A record of this is held by the DSL.**

- **The Governor assigned to all aspects of ICT is Nick Buckland. Rev Simon Leigh reports to the governing body on Safeguarding.**

2.3.2 How will email be managed?

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits and interesting projects between schools and in different continents can be created.

The implications of email use for the school and pupils must be thought through and appropriate safety measures put in place. Unregulated email can provide routes to pupils that bypass the traditional school boundaries.

A central question is the degree of responsibility that can be delegated to individual pupils as once email is available it is difficult to control. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content is possible.

In the school context (as in the business world), email should not be considered private and Shebbear College reserve the right to monitor emails. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

Whilst in school, pupils must use the School Network to access emails and may only use approved email accounts.

Pupils must immediately tell a teacher if they receive offensive 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.

- Excessive social email use can interfere with learning and will be restricted.

- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

- The forwarding of chain messages is not permitted.

- Shebbear College has a dedicated email for pupils to report concerns to staff (anonymously if required) called Confide and a Google reporting system so that staff can report academic, wellbeing and pastoral issues (both of these are monitored by Senior Members of the Pastoral Team.

• Staff should only use school email accounts to communicate with pupils as approved by the Senior Management Team.

2.3.3 How will published content be managed?

Websites can celebrate pupils' work, promote the school and publish resources for projects.

Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

Publication of sensitive information should be considered from a personal and school security viewpoint. Material such as staff lists or a school plan may be better published in the school handbook or on a secure part of the website which requires authentication.

The contact details on the website is the school address, email and telephone number.

Staff or pupils' personal information must not be published.

• Email addresses should be published carefully, to avoid being harvested for spam (e.g. replace '@' with 'AT'.

• The Headmaster will take overall editorial responsibility and ensure that content is accurate and appropriate.

• The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

2.3.4 Can pupil's images or work be published?

Still and moving images and sounds add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount.

Although common in newspapers, the publishing of pupils' names with their images should be carefully considered. Published images could be reused, particularly if large images of individual pupils are shown.

Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. "Over the shoulder" can replace "passport style" photographs but still convey the educational activity. Personal photographs can be replaced with self-portraits or images of pupils' work or of a team activity. Pupils in photographs should, of course, be appropriately clothed.

Images of a pupil should not be published without the parent's or carer's written permission.

Shebbear College ask permission to publish images of work or appropriate personal photographs on entry, some once per year, others at the time of use.

Pupils also need to be taught the reasons for caution in publishing personal information and images online (see section 2.3.6).

Images that include pupils will be selected carefully and will not provide material that could be reused.

Pupils' full names will not be used anywhere on the website in association with photographs.

Written permission from parents or carers will be obtained before images of pupils are electronically published.

Pupils work can only be published with their permission or the parents.

2.3.5 How will social networking, social media and personal publishing be managed?

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

For responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff are made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They are made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

Shebbear College will control access to social media and social networking sites.

Pupils are advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc. This education is delivered by all staff through all areas of the pupil's learning and specifically through ICT and PSHE.

- Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.

- Staff official blogs or wikis should be password protected and run from the school network with approval from the Senior Management Team. Staff are advised not to run social network spaces for pupil use on a personal basis.

- If personal publishing is to be used with pupils then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by school staff.

• Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others by making profiles private.

• Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

2.3.6 How will filtering be managed?

Levels of Internet access and supervision will vary according to the pupil's age and experience. The school filters internet access through I-Boss.

Access profiles must be appropriate for all members of the school community. Older secondary pupils, as part of a supervised project, might need to access specific adult materials; for instance a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily. Systems to adapt the access profile to the pupil's age and maturity are available.

Access controls fall into several overlapping types (commonly described as filtering):

• Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day. Our Web filtering supplier manages this.

• A walled garden or "allow list" restricts access to a list of approved sites. Such lists inevitably limit pupils' access to a narrow range of information.

• Dynamic filtering examines web page content or email for unsuitable words. Filtering of outgoing information such as web searches is also required.

• Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.

• Access monitoring records the Internet sites visited by individual users. Attempted access to a site forbidden by the policy will result in a report.

Shebbear College will work to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL must be reported to the network manager and the e–Safety Coordinator.

The school's broadband access will include filtering appropriate to the age and maturity of the pupil.

• Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Checks are currently made by the Network Manager and the DSL. Amongst their tasks is to ensure the school's has proper regard for the Prevent Strategy in its monitoring of digital usage.

• Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from the network manager.

2.3.8 How can emerging technologies be managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. In such cases the Network Manager should be consulted and a risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety established.

The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites such as Facebook. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication, but is often not possible.

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a pupil using a phone to video a teacher's reaction in a difficult situation.

Shebbear College keeps up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. For instance text messaging via mobile phones is a frequent activity for many pupils and families; this could be used to communicate a pupil's absence or send reminders for exam coursework.

There are dangers for staff however if personal phones are used to contact pupils and staff are given guidelines in regard to this in the Staff code of Conduct.

The inclusion of inappropriate language or images is difficult for staff to detect. Pupils may need reminding that such use is inappropriate and conflicts with school policy. Abusive messages should be dealt with under the school's behaviour, cyber bullying and our anti--bullying policies.

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

- Mobile phones will not be used by pupils during lessons or formal school time unless given permission to do so by a member of staff. The sending of abusive or inappropriate text, picture or video messages is forbidden.

The school will investigate wireless, infrared and Bluetooth communication technologies and has a policy on phone use in school **(see Mobile Phone policy)**

2.3.9 How should personal data be protected?

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 (“the Act”) gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual’s rights
- Kept secure
- Transferred only to other countries with suitable security measures.

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

2.4 Policy Decisions

2.4.1 How will Internet access be authorised?

Shebbear College allocates Internet access for staff and pupils on the basis of educational need.

It is clear who has Internet access and who has not. Authorisation is generally on an individual basis in the Prep school, where pupil usage should be fully supervised. Normally most pupils will be granted Internet access; it may be easier to manage lists of those who are denied access.

Parental permission will be required for Internet access in all cases — a task that may be best organised annually when pupils’ home details are checked and as new pupils join.

The school will maintain a current record of all staff and pupils who are granted access to the school’s electronic communications.

All staff must read and sign the ‘Acceptable Use Policy’ before using any school ICT resource.

All pupils must read and sign the ‘Acceptable Use Policy’ before using an school ICT resource

At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials delivered through ICT and PSHE.

Parents will be asked to sign and return a consent form for pupil access.

- Parents will be informed that pupils will be provided with supervised Internet access.

2.4.2 How will risks be assessed?

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. Shebbear College addresses the issue that it is not possible to completely remove the risk that pupils might access unsuitable materials via the school system.

Shebbear College 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 can accept liability for the material accessed, or any consequences resulting from Internet use.

Shebbear College will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate. The network is protected by the Internet filter – i-Boss.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

- Methods to identify, assess and minimise risks will be reviewed regularly.

2.4.3 How will e–Safety complaints be handled?

Parents, teachers and pupils know how to use the School’s complaints procedure. The facts of the case will need to be established, for instance whether the Internet use was within or outside school.

A minor transgression of the rules may be dealt with by a member of staff. Other situations

could potentially be serious and a range of sanctions will be required, linked to the school’s disciplinary policy. Potential child protection or illegal issues must be referred to the school Designated Safeguarding Lead (who is also the e–Safety Coordinator).

Complaints of Internet misuse will be dealt with under the School’s Complaints Procedure.

Any complaint about staff misuse must be referred to the Headmaster.

All e–Safety complaints and incidents will be recorded by the school — including any actions taken.

• Pupils and parents will be informed of the complaints procedure.

• Parents and pupils will work in partnership with staff to resolve issues.

• Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

2.4.4 How is the Internet used across the community?

Given Shebbear's remote location internet access during the day is not easily available other than through the school network. The school is aware of the ability of pupils to get internet access through 3G and 4G. Boarding staff exercise vigilance in this matter and pupils know they must use the school system or face disciplinary measures. In this regard the best protection of their wellbeing is education.

Where pupils might get other access to the internet – eg – wifi on a shopping expedition then there is a fine balance to be achieved in ensuring open access to information whilst providing adequate protection for children and others who may be offended by inappropriate material. Organisations are developing access appropriate to their own client groups and pupils may find variations in the rules and even unrestricted Internet access. Although policies and practice may differ, community partners adhere to the same laws as schools. Staff may wish to exchange views and compare policies with others in the community. Where rules differ, a discussion with pupils on the reasons for the differences could be worthwhile.

Sensitive handling of cultural aspects is important. For instance filtering software should work across community languages and the school Internet policies may need to reflect the pupils' cultural backgrounds.

• if an issue becomes apparent the school will liaise with local organisations to establish a common approach to e–Safety.

• The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

2.4.5 How will Cyber bullying be managed?

Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

Many young people and adults find using the internet and mobile phones a positive and creative part of their everyday life. Unfortunately, technologies can also being used negatively.

When children are the target of bullying via mobiles phones, gaming or the internet, they can often feel very alone, particularly if the adults around them do not understand cyber bullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that young people, school staff and parents and carers understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyber bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the Anti-Bullying Policy.

There will be clear procedures in place to support anyone 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:

• Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

• The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

• Sanctions for those involved in Cyber bullying may include:

o The bully will be asked to remove any material deemed to be inappropriate or offensive.

o The service provider may be contacted to remove content.

o Internet access may be suspended at school for the user for a period of time.

o Parent/carers may be informed.

o The Police will be contacted if a criminal offence is suspected.

This policy works in accordance with Anti-bullying Policy.

2.4.6 How will learning environments be managed?

The school is developing a VLE. Once established an effective learning platform or learning environment can offer schools a wide range of benefits to teachers, pupils, parents as well as support management and administration. It can enable pupils and teachers to collaborate in and across schools, can share resources and tools for a range of topics, create and manage digital content and pupils can develop online and secure e-portfolios.

Any Learning Platform/Environment (LP) will be subject to careful monitoring by Senior Management Team (SMT). As the usage grows throughout the school then more issues could arise regarding content, inappropriate use and behaviour online by users. The SMT has a duty to review and update the policy regarding the use of the Learning Platform annually and all users must be informed of any changes made.

SMT and staff will monitor the usage of the learning environments by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities.

Pupils/staff will be advised on acceptable conduct and use when using the learning environment.

Only members of the current pupil, parent/carers and staff community will have access to the internet

All users will be mindful of copyright issues and will only upload appropriate content onto the learning environment

When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

2.5 Communication Policy

2.5.1 How will the policy be introduced to pupils?

Many pupils are very familiar with mobile and Internet use and culture and it is wise to involve them in designing the School e–Safety Policy, possibly through a student council. As pupils' perceptions of the risks will vary; the e–Safety rules may need to be explained or discussed.

The School e–Safety rules are included in the pupil planner.

E–Safety lessons are delivered as an ICT lesson activity, part of the pastoral programme and part of every subject whenever pupils are using the internet. PSHE also delivers lessons specific to e-safety through the CEOP programme

Useful e–Safety programmes include:

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Safe Social Networking: www.safesocialnetworking.com
- CEOP – Child Exploitation Online Protection

All users will be informed that network and Internet use will be monitored.

An e–Safety training programme is introduced to raise the awareness and importance of safe and responsible internet use. This is presently delivered by Mrs Fran Lovett, trained with CEOP at Ambassador level

- Pupil instruction in responsible and safe use should precede Internet access.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

2.5.2 How will the policy be discussed with staff?

It is important that all staff feel confident to use new technologies in teaching and the School e–Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.

All staff must understand that the rules for information systems misuse for Shebbear College employees are specific and instances resulting in disciplinary procedures and dismissal have occurred. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

Particular consideration must be given when staff are provided with devices by the school which may be accessed outside of the school network. Schools must be clear about the safe and appropriate use of school provided equipment and rules about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information.

ICT use is widespread and all staff including administration, midday supervisors, caretakers, governors and volunteers should be included in awareness raising and training. Induction of new staff should include a discussion of the school e–Safety Policy.

The e–Safety Policy will be formally provided to and discussed with all members of staff.

To protect all staff and pupils, the school will implement Acceptable Use Policies.

Staff should be aware that Internet traffic can be monitored and traced to the individual user, Discretion and professional conduct is essential.

- Staff that manage filtering systems or monitor ICT use will be supervised by the Senior Management Team and have clear procedures for reporting issues.

- Staff training in safe and responsible Internet use both professionally and personally will be provided.

2.5.3 How will parents' support be enlisted?

Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help parents plan appropriate supervised use of the Internet at home and educate them on the risks. Parents should also be advised to check if their child's use elsewhere in the community is covered by an appropriate use policy. One strategy is to help parents to understand more about

ICT — perhaps by running courses and parent awareness sessions, although the resource implications will need to be considered.

Parents' attention will be drawn to the School e–Safety Policy in newsletters, the school brochure and on the school website.

- A partnership approach with parents will be encouraged. This includes parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e–Safety at other attended events e.g. parent evenings, sports days. CEOP presentation evenings are also given to parents.

• Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.

• Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Useful Contacts and Addresses

Becta: www.becta.org.uk/safeguarding

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation: www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

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

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com