

St John's Catholic Junior School

Love one another as I have loved you



E-Safety and Internet Policy

Agreed by Governors _____

Signed _____ Head teacher

Signed _____ Chair of Governors

Contents:

| | |
|----|---|
| | |
| 1 | Why is Internet Use Important? |
| 2 | How Does Internet Use Benefit Education? |
| 3 | How Can Internet Use Enhance Learning? |
| 4 | Authorised Internet Access |
| 5 | Internet Use |
| 6 | Email Management |
| 7 | Password Protection |
| 8 | Filtering |
| 9 | Video Conferencing |
| 10 | Social Networking |
| 11 | Published Content and the School VLE Site |
| 12 | iPad Acceptable Use |
| 13 | Use of Cloud Services to Save Work from iPads |
| 14 | Digital Cameras |
| 15 | Parents/Carers Use of Mobile Phones /Digital Cameras |
| 16 | Storage of Photographs |
| 17 | Mobile Phones and Other Hand Held/Communication Devices |
| 18 | Managing Emerging Technologies |
| 19 | Information System Security |

| | |
|------------|---|
| 20 | USB Memory Sticks and Other Portable Data Storage Devices |
| 21 | Protecting Personal Data |
| 22 | Assessing Risks |
| 23 | Handling eSafety Complaints |
| 24 | Training |
| 25 | Communication of Policy |
| 26 | Staff AUP - Staff Information Systems Code of Conduct |
| 27 | Student AUP |
| Appendix A | Staff E-Safety Rules |
| Appendix B | Flowchart for Responding to eSafety Incidents |
| Appendix C | eSafety Audit |
| Appendix D | Are you an eSafe school? |
| Appendix E | eSafety Incident Log |

1. Why Is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for students who show a responsible and mature approach to its use. Our school has a duty to provide students with quality Internet access.

Students will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2. How Does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient;
- Access to world-wide educational resources including museums and art galleries;
- Educational and cultural exchanges between students world-wide;
- Access to experts in many fields for students and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the Local Authority and DCSF.

3. How Can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for student use and includes filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide students in on-line activities that will support learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

4. Authorised Internet Access

- The school will maintain a current record of all staff and students who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that students will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for student access on entry into the school.

5. Internet Use

- If staff or students discover unsuitable sites, the URL (address), time, content must be reported to Headteacher and recorded in the e-safety log.
- School will ensure that students and staff are aware of copyright law with the use of Internet derived materials.
- Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

6. Email Management

- The class teacher has the responsibility to ensure that no abuse of the e-mail facility occurs.
- If there is a class email account, it must only be used under the supervision of the class teacher.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts is not permitted on school machines.
- The forwarding of chain letters is not permitted.

7. Password Protection

- Each pupil must have a unique username to log into the school network.
- Each pupil must have a unique username to access Google Classroom.
- All staff must have a unique username and unique password.
- Students must not disclose passwords to other students.

8. Filtering

The school will work in partnership with their technical support provider and **Exa Networks** to ensure filtering systems are as effective as possible.

9. Video Conferencing

- Video conferencing will be appropriately supervised for the pupils' age and will be conducted in the presence of staff.

10. Social Networking

- The School will block/filter access to social networking sites and newsgroups unless a specific use is approved
- Students will be advised never to give out personal details of any kind which may identify them or their location
- Students should be advised not to place personal photos on any social network space
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others
- Staff are fully informed of their responsibilities regarding the use of social networking sites, such as Facebook. At St John's Catholic Junior School, it is agreed that personal and professional commitments should be separated on these sites. Therefore, it is essential that the following groups should not be allowed as contacts and friends:
 1. Ex pupils. Many of these sites are targeted by adults. It is not appropriate to have contacts in this context of teacher to pupil relationship.
 2. All staff are aware that they could face charges of gross misconduct if the social networking platforms communicate personal opinions which may be defamatory or abusive to individuals or organizations associated with the school.
 3. Staff are also aware that they are responsible for the security protocols regarding any social networking accounts. This is a professional responsibility.

11. Published Content and the School Website

- The contact details on the website will be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs that include students will be selected carefully and will be appropriate for the context.
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified.
- Permission from parents or carers will be obtained before photographs of students are published on the website.
- Pupils' full names will not be used anywhere on the school website, particularly associated with photographs/digital images and audio content.
- The website should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Learning Platform – Google Classroom

- Students must sign an AUP explicitly for Google Classroom
- Parents sign & return student consent form for Google Classroom

12. iPad/Device Acceptable Use

- Computer, iPad, email, Internet, and Intranet users shall respect the privacy of other users in the school.
- Users may not, under any circumstances, log on under or use another user's account without permission from a teacher.
- Users may not share passwords.
- Any recording device, including but not limited to video and digital cameras and camera phones to take videos or still pictures, may not be used to slander, bully or denigrate any pupil, visitor, staff member on or off the school grounds at any time.
- All messages or postings to any Internet site on or off the school grounds at any time (notes, email,

newsgroups, bulletin boards, wikis, or other interactive forms of communication such as Instant Messaging) shall be educationally purposeful and appropriate. Hate mail, harassment, discriminatory remarks, vulgarity, swear words, other antisocial behaviors, chain letters, and threats of any kind are prohibited.

- Pupils must not use personal accounts on the iPad.
- The use of technology resources to purposefully access inappropriate material or files harmful to the integrity of St John's Catholic Junior School is prohibited.
- Students may not access social networking sites such as Facebook, use Instant Messaging, and access outside email accounts.
- Students may not post images of teachers, staff or other personnel on the Internet without receiving permission from the individual(s) involved.
- Students may not alter the configuration of any school-owned computer or iPad.
- Students may not use the cameras on their iPads unless given permission by and under the supervision of a teacher.

13. Use of the Cloud Services to Save Work from iPads

- The provider must comply with the Safe Harbor list or Model Contract clauses compliant with the Data Protection Act,
"Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

If a company is outside the EU and in the USA then there is a 'Safe Harbor' list maintained of companies that fulfil the level of protection clause

14. Digital Cameras

- Staff are to use school cameras only to photograph students.
- Staff must not use personal equipment to photograph students.
- Storage cards to be cleared when the camera is returned.
- Images are to be regularly uploaded to the network from shared devices.
- Where possible, general shots of classroom or group activities rather than close up pictures of individual children.
- Use images of children in suitable dress, and take care photographing PE or swimming events to maintain modesty, using tracksuits if appropriate for example.
- Remember to include images of children from different ethnic backgrounds in communications whenever possible and positive images of children with disabilities to promote school as an inclusive community, to comply with the Disability Discrimination Act and the Rights set out in the UNCRC (UNICEF).

15. Parents / Carers Use of Mobile Phones / Digital Cameras

- Parents / carers are informed to only take photographs of their own children and that the photographs will not be published on any media including social networking sites.

16. Storage of Photographs

- Photographs to be stored in a secure area within the school network on a shared drive.
- Photographs are not to be downloaded outside of school.
- Photographs to be deleted from the school network when no longer required.

17. Mobile Phones and Other Hand Held/Communication Devices

- Mobile phones & other hand held communication devices should not be used for personal use in the lesson or formal school time (students & staff).
- Sending of abusive or inappropriate messages is forbidden.

18. Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and will be carried out before use in school is allowed.
- The children will be reminded of E-safety procedures before new technology is used e.g. learning platform.
- Children are regularly reminded to report any concerns/ inappropriate content immediately.
- Pupils are not permitted to use mobile phones in school. Any brought to school must be given to class teacher.

19. Information System Security

- School ICT will be reviewed annually.
- Virus protection reviewed annually.
- Security strategies will be discussed and reviewed annually.
- Personal data sent over the Internet should be encrypted or otherwise secured.
- Unapproved system utilities and executable files will not be allowed in the pupils' work area or attached to emails.
- Also see the use of 'USB memory sticks and other portable storage devices' section.
- The IT co-ordinator along with the Technical support provider will ensure that the system has the capacity to take increased traffic caused by Internet use and the number of files stored on the network.

20. USB Memory Stick and other Portable Data Storage Devices

- Staff are to decide what data should be stored on USB sticks/other data storage devices.
- Sensitive data should be encrypted or password protected.

21. Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Relevant documentation will be forwarded directly to the school from the Data Protection Commissioner and should be signed and returned immediately. A copy of the form should be kept in school to comply with audit requirements.

22. Assessing Risks

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 will audit technology and its use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate every 12 months.

23. Handling eSafety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff, Safeguarding officer or Head teacher
- Any complaint about staff misuse must be referred to the Head teacher and ICT leader.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

24. Training

Students

- PSHCE/SMSC/Outside agencies/embedded across the curriculum/assemblies.
- Age appropriate.

Staff

- All staff (teaching & non teaching).
- INSET.

Parents

- Sessions/workshops for parents.

25. Communication of Policy

Students

- Rules for Internet access will be posted in in all rooms.
- Students will be informed that Internet use will be monitored.

Staff

- All staff will be given the School E- Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential

Governors

- AUP (governors to ratify).

Parents

- Parents' attention will be drawn to the School E-safety Policy /procedures in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Relevant leaflets from organisations promoting e-safety will be available for parents to collect.

Visitors

- Visitors to school will be informed about the E-safety policy at the reception desk.
- Rules for visitors clearly displayed (i.e. use of mobile phone/camera/film equipment etc) and signed for on arrival.

26. Staff AUP

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's eSafety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Head teacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school eSafety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with students are compatible with my professional role.
- I will promote eSafety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: Printed:

Date:

Accepted for school:

Capitals:

27. Student AUP

eSafety Rules

All students use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both students and their parents/carers are asked to sign to show that the eSafety Rules have been understood and agreed.

Student:

Form:

Students' Agreement

- I have read and I understand the school eSafety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:

Date:

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school eSafety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that students cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:

Date:

Please print name:

Please complete, sign and return to the school

Appendix A: Staff E-Safety Rules

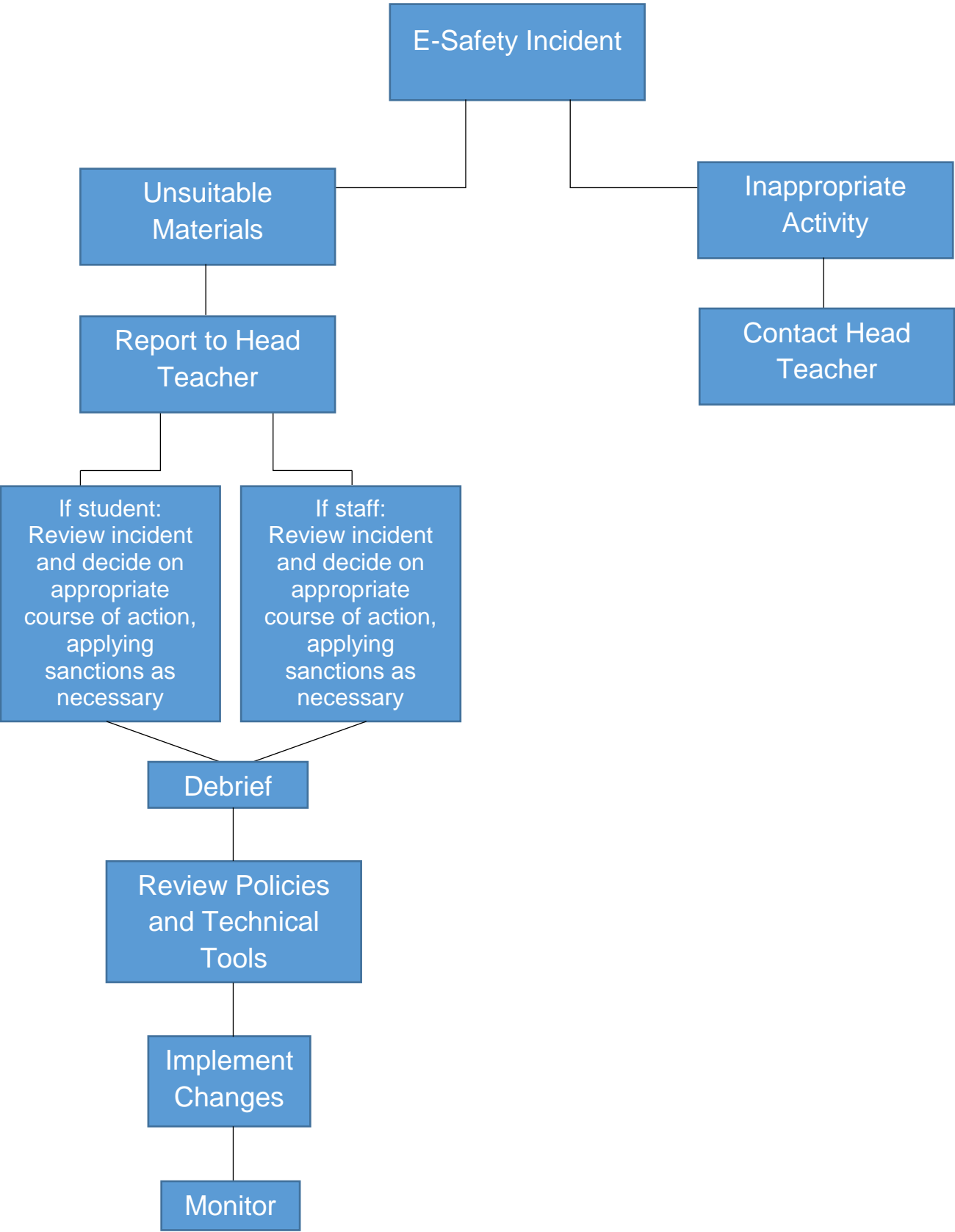
E-Safety Rules

These E-safety Rules help to protect staff and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school will exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Appendix B: Flowchart for Responding to eSafety Incidents



Appendix C: eSafety Audit

This quick self-audit will help the senior management team (SMT) assess whether the eSafety basics are in place.

| | |
|--|-----|
| Has the school an eSafety Policy that complies with CYPD guidance? | Y/N |
| Date of latest update: | |
| The Policy was agreed by governors on: | |
| The Policy is available for staff at: | |
| And for parents at: | |
| The designated Child Protection Teacher/Officer is: | |
| The eSafety Coordinator is: | |
| Has eSafety training been provided for both students and staff? | Y/N |
| Is the Think U Know training being considered? | Y/N |
| Do all staff sign an ICT Code of Conduct on appointment? | Y/N |
| Do parents sign and return an agreement that their child will comply with the School eSafety Rules? | Y/N |
| Have school eSafety Rules been set for students? | Y/N |
| Are these Rules displayed in all rooms with computers? | Y/N |
| Is Internet access provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access? | Y/N |
| Has the school filtering policy been approved by SMT? | Y/N |
| Is personal data collected, stored and used according to the principles of the Data Protection Act? | Y/N |
| Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SMT? | Y/N |

Appendix D: Are you an eSafe school?

| | |
|---|--|
| <p>Do all your staff...</p> <ul style="list-style-type: none"><input type="checkbox"/> Understand e-safety issues and risks?<input type="checkbox"/> Receive regular training and updates?<input type="checkbox"/> Know how to escalate an issue of concern?<input type="checkbox"/> Know how to keep data safe and secure?<input type="checkbox"/> Know how to protect themselves online?<input type="checkbox"/> Know how to conduct themselves professionally online?<input type="checkbox"/> Know about the updated e-safety guidance for QTS standard Q21: Health and well-being? | <p>Does your school...</p> <ul style="list-style-type: none"><input type="checkbox"/> Have a nominated e-safety co-ordinator?<input type="checkbox"/> Audit its e-safety measures?<input type="checkbox"/> Have a robust AUP?<input type="checkbox"/> Use a Becta accredited supplier for internet services?<input type="checkbox"/> Include e-safety measures in Section 4b of your SEF?<input type="checkbox"/> Keep an incident log and monitor your measures?<input type="checkbox"/> Handle cyberbullying issues well?<input type="checkbox"/> Raise awareness of the issues, e.g. through holding an assembly? |
| <p>Do your learners...</p> <ul style="list-style-type: none"><input type="checkbox"/> Understand what safe and responsible online behaviour means?<input type="checkbox"/> Receive e-safety education at appropriate places across the curriculum?<input type="checkbox"/> Get the opportunity to improve their digital literacy skills?<input type="checkbox"/> Know the SMART rules?<input type="checkbox"/> Know how to report any concerns they may have? | <p>Do your parents and governors...</p> <ul style="list-style-type: none"><input type="checkbox"/> Understand e-safety issues and risks?<input type="checkbox"/> Understand their roles and responsibilities?<input type="checkbox"/> Receive regular training and updates?<input type="checkbox"/> Understand how to protect their children in the home? |

