# St. John's CE First School

# School E-Safety and ICT Acceptable Use Policy

**As a Church of England School we are guided by our Christian values in supporting the learning of all our children**

## E-Safety Policy

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school is committed safeguarding its pupils and as such, this policy should be read in conjunction with other relevant policies including our safeguarding policies; Behaviour, Anti –bullying and Social networking policies

## Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the South West Grid for Learning including the effective management of content filtering.

The school's ICT Coordinator acts as our e-Safety coordinator.

Our e-Safety Policy has been agreed by the staff and approved by governors.

The e-Safety Policy will be reviewed annually.

## Why is Internet Use Important?

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 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 pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality internet access

Pupils 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.

## How does Internet Use Benefit Education?

Benefits of using the internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- 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 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; access to learning wherever and whenever convenient.

## How can Internet Use Enhance Learning?

- The school internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils 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 pupils in on-line activities that will support 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.

## Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents are informed that pupils will be provided with supervised internet access.
- Parents are asked to sign the permission form for pupil access which is located in the Home/School Link book.

## World Wide Web

- If staff or pupils discover unsuitable sites, when possible, the URL time, content and computer should be recorded and reported to the e-safety coordinator who will ensure that the information is passed on to SWGfL. Parents of children involved should be informed, usually by the class teacher, detailing the school's response.
- If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to the Internet Service Provider (South West Grid for Learning) via the e-safety coordinator or network manager. The ICT technician will also block unsuitable websites directly from our school.
- The school will ensure that the use of internet derived materials by pupils and staff complies with copyright law.

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

## Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts may be blocked.
- E-mail 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 letters is not permitted

## Mobile phones

- Pupils are not permitted to bring mobile phones to school.

## Social Networking

- Pupils are advised not to use social networking sites.
- Social networking is not permitted on school equipment and social networking sites and newsgroups are blocked by the school's filter.
- Pupils are advised never to give out personal details of any kind which may identify them or their location
- Pupils are advised not to place personal photos on any social network space.

## Filtering

The school will work in partnership with the Local Authority, Becta and the Internet Service Provider to ensure filtering systems are as effective as possible.

## Video Conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the internet.
- Video conferencing will only ever take place under direct supervision from a member of staff.

## Published Content and the School Web Site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

## Publishing Pupils' Images and Work

- Pupils' full names will not be used anywhere on the Web site particularly in association with photographs.
- Children are only referred to using their first names on our website
- If the pupil is names – avoid using their photograph
- If a photograph is used – avoid naming the pupil
- Only use images of pupils in suitable dress to reduce the risk of inappropriate use of images of pupils

## Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is installed and updated regularly by the ICT technician.
- Security strategies will be discussed with the Local Authority.

## Protecting Personal Data

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

## Assessing Risks

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- 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. Neither the school nor Dorset County Council can accept liability for the material accessed, or any consequences of internet access.
- The school should 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 headteacher.
- 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.

## Communication of Policy

### Pupils

- Rules for e-safety are located near the computers in each classroom and in the learning centre.
- Pupils are informed that internet use can 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.

**Parents**

- The e-safety policy will be available for parents on the school's website or in hard copy upon request.
- The  Internet – Acceptable use policy and permission form are located within the Home /School Link book

## Referral Process – Appendix A

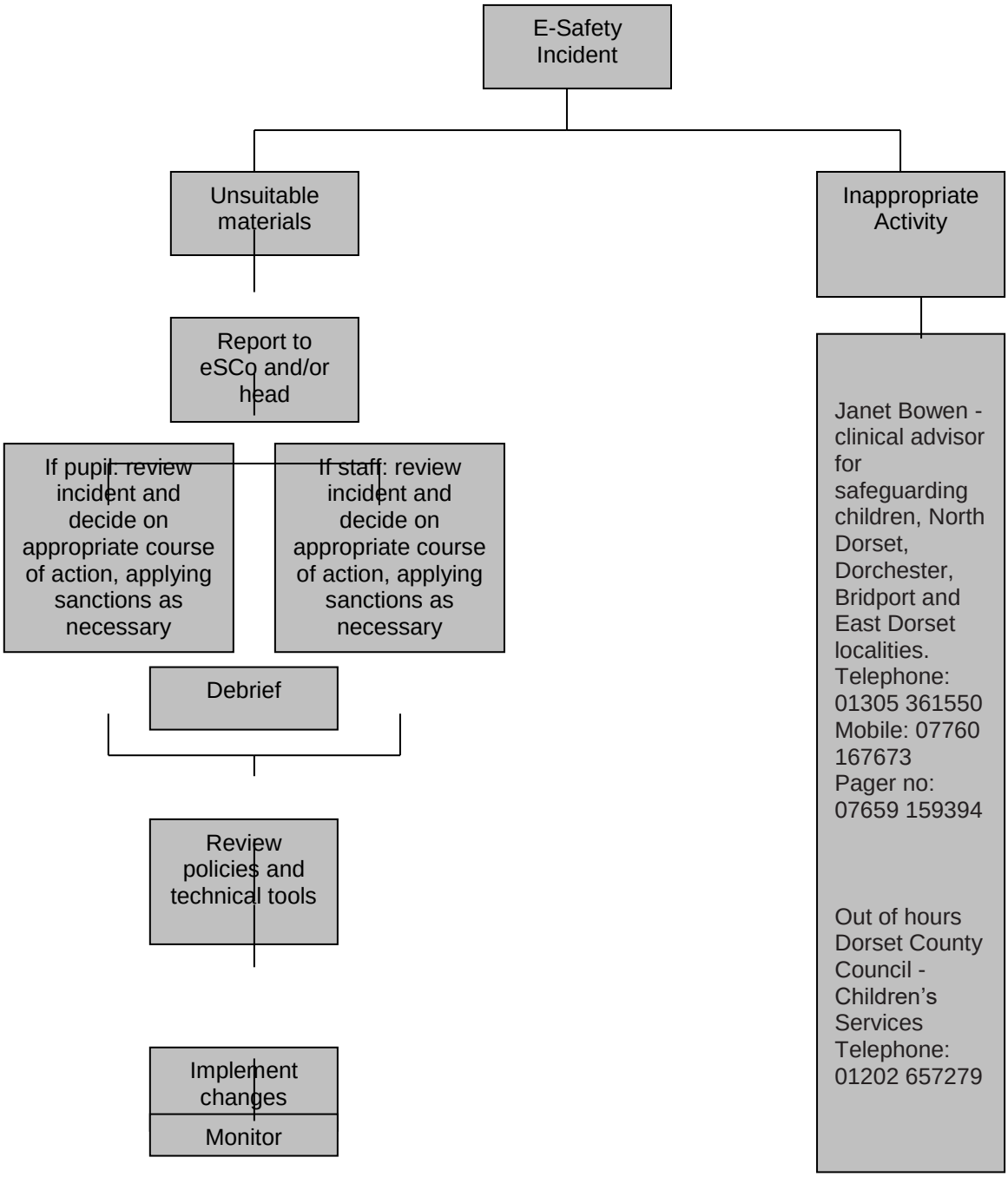
## E-Safety Rules– Appendix B

## Staff Acceptable Use Policy – Appendix C

## E-Safety Audit Form – Appendix D

# Appendix A

**Flowchart for responding to e-safety incidents in school**




Adapted from Becta – E-safety 2005

## E-Safety Rules– Appendix B

### Elephants, Giraffes, Dolphins

# Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the internet with an adult.

We always ask if we get lost on the internet.

We press the ‘Hector’ button if we see anything we don’t like and we tell an adult straight away.

**Pandas and Snow Leopards**

# Think then Click

e-Safety Rules

- We ask permission before using the internet.
- We only use websites that an adult has chosen.
- We press the ‘Hector’ button if we see anything we are uncomfortable with and we tell an adult immediately.
- We only e-mail using EasyMail and we only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails sent by anyone we don’t know.
- We do not use internet chat rooms.

# E-Safety Rules

These e-Safety Rules help to protect pupils 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 may 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.

# Staff Acceptable Use Policy – Appendix C

## 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 e-safety 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 headteacher.
- 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 e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will not use technology in any way which may put myself or the school at risk of allegation of abuse or inappropriate conduct.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail 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: …… Capitals: …… Date:

Accepted for school: …… Capitals: ……

# E-Safety Audit Form – Appendix D

## E-Safety Audit Form

| | |
|---|---|
| Has the school an e-Safety 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 e-Safety Coordinator is: | |
| Has e-safety training been provided for both pupils and staff? | Y/N |
| Is the Think U Know training being considered? | Y/N |
| Are Think U Know internet safety lessons / resources used? | 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 e-Safety Rules? | Y/N |
| Have school e-Safety Rules been set for pupils? | Y/N |
| Are these Rules displayed in all rooms with computers? | Y/N |
| Internet access is 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 has been approved by SMT? | Y/N |
| Is personal data collected, stored and used according to the principles of the Data Protection Act? | Y/N |

**Acceptable use of the computer equipment**

**Pupils and staff are expected to treat the equipment with care and to follow the guidelines and advice given by the teachers, teaching assistants and ICT Coordinator.**

**Unacceptable use of the computer equipment.**

Unacceptable use of the equipment is not tolerated. The following list, while not exhaustive, is a good indicator and pupils should be made aware of this. Pupils not using the equipment correctly will be met with the application of the appropriate school sanctions. Parents may be asked to contribute to the cost of repair/replacement.

- Damaging the computers and computer equipment through silly behaviour.
- Excessive use of force when using the keyboard, mouse, headphones and other equipment.
- Bringing food and drinks into the computer area.
- Sending rude, offensive or abusive material to another user, or using it to talk to others about another person in a rude, offensive or abusive way.
- Attempting to damage, change or erase any files or data belonging to another individual.
- Being untidy with the computer equipment.
- Failing to notify teachers of any problems that may arise with the computers to do with damages and 'warning messages' that pop-up on screen.
- Using equipment that they have not been authorised to use or instructed on how to use.
- Corrupting, editing, changing data.
- Violating the privacy of other users.
- Disrupting the use of the equipment by others.

Reviewed: March 2015
Date for review: March 2017