# St George's Primary School
# E-Safety Policy

# October 2019

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's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Anti- Bullying, Acceptable ICT Use Agreement, Social Networking for School Staff and Curriculum etc.

## 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. This will include a secure school network design and use.

- Safe and secure broadband from the South West Grid for Learning including the effective management of content filtering.

- National Education Network standards and specification

# School e-Safety Policy

The school will appoint an e-Safety coordinator.
Our e-Safety Policy has been written by the school. It has been agreed by the senior management team and approved by governors.

The e-Safety Policy will be reviewed annually. This policy will next be reviewed October 2018

## 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 of 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 especially 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 and safe 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;
- access to experts in many fields for 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 appropriate.

## 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 appropriate Internet use, what 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 through 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 for research, including the skills of locating information, 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 will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.

## World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to the Local Authority helpdesk via the e-safety coordinator or network manager.
- 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.

## Social Networking

- Schools should block/filter access to all social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

## 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.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

## Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.

## 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 head teacher or nominee(s) will take overall editorial responsibility and ensure that content is accurate and appropriate.

## Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified unless permission is granted.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents.

## Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- 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

- 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 L.A. 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 head teacher.
- 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.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

## Communication of Policy

### Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils 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.
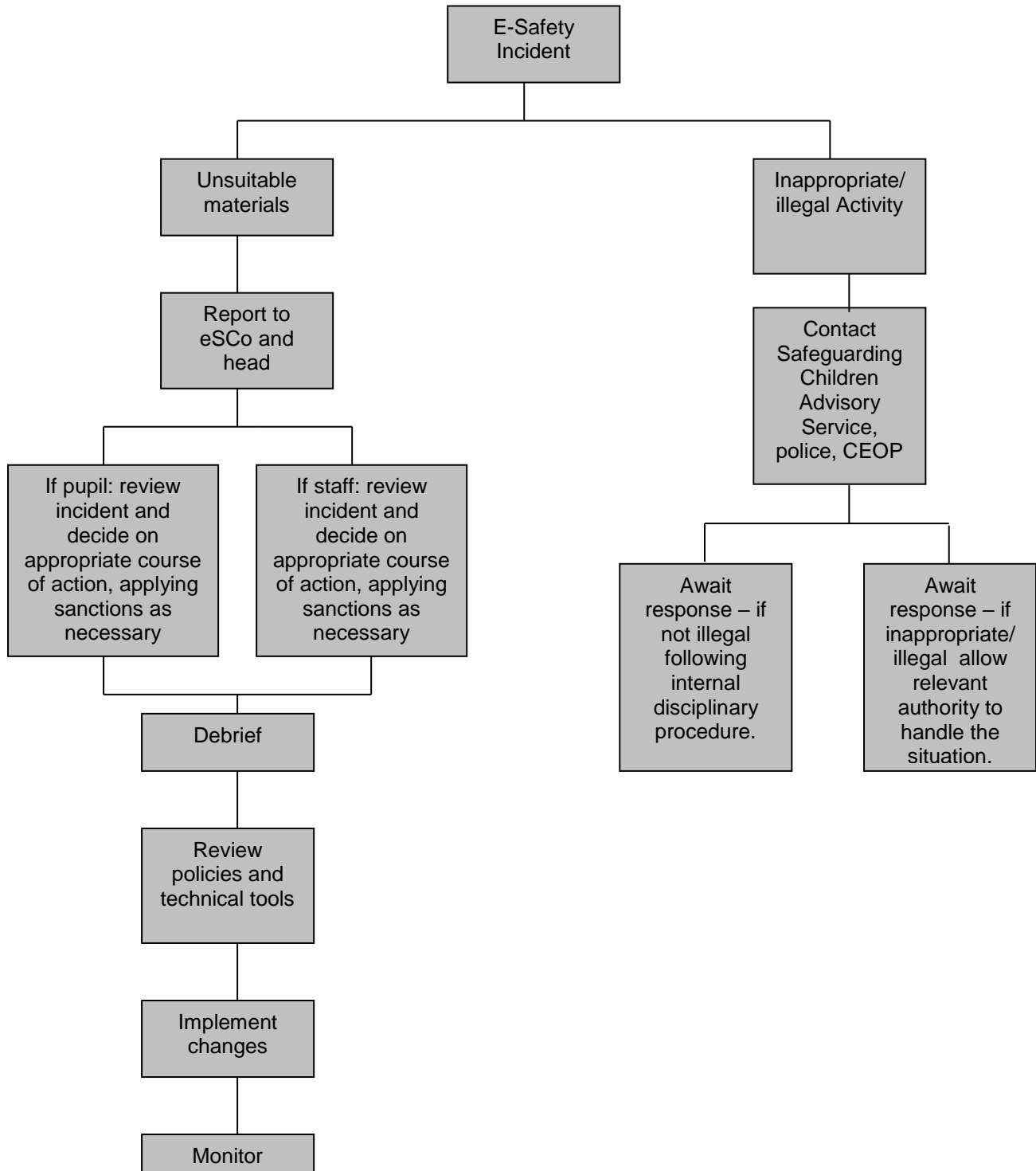
### Parents

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

This policy complies with and is in line with the 9 principles set out in the Single Equality Policy and an initial screening Equality Impact Assessment has been carried out.

# Referral Process – Appendix A

# Appendix A

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

```
                          ┌─────────────────┐
                          │    E-Safety     │
                          │    Incident     │
                          └────────┬────────┘
                 ┌─────────────────┴─────────────────┐
        ┌────────────────┐                   ┌────────────────┐
        │   Unsuitable   │                   │ Inappropriate/ │
        │    materials   │                   │ illegal Activity│
        └────────┬───────┘                   └────────┬───────┘
        ┌────────────────┐                   ┌────────────────┐
        │   Report to    │                   │    Contact     │
        │   eSCo and     │                   │  Safeguarding  │
        │     head       │                   │    Children    │
        └────────┬───────┘                   │   Advisory     │
                                             │   Service,     │
                                             │  police, CEOP  │
                                             └────────┬───────┘
```

| If pupil: review incident and decide on appropriate course of action, applying sanctions as necessary | If staff: review incident and decide on appropriate course of action, applying sanctions as necessary |
|---|---|

**Debrief**

**Review policies and technical tools**

**Implement changes**

**Monitor**

| Await response – if not illegal following internal disciplinary procedure. | Await response – if inappropriate/ illegal allow relevant authority to handle the situation. |
|---|---|

Adapted from Becta – E-safety 2005