The Bridges Federation

Working together for success

INTERNET & E-SAFETY POLICY

INTERNET and 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 about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Good Habits

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

- Responsible ICT use by all staff and children; 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 Norfolk Grid for Learning including their effective management of content filtering.
- National Education Network standards and specifications.

Why is Internet Use Important?

The purpose of Internet use in our Schools is to raise educational standards, to promote children's' achievement, to support the professional work of staff and to enhance the schools' management information and administration systems.
Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element life for education, business and social interaction. Access to the Internet is therefore an entitlement for children who show a responsible and mature approach to its use. Our Federated schools have a duty to provide children with quality Internet access
Children 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 children 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 Bridges Federation schools internet access is designed expressly for children to use and includes filtering appropriate to the age of the child.
Children 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 children in on-line activities that will support learning outcomes planned for the child's age and maturity.
Children 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 Federation schools will maintain a current record of all staff and children who are granted Internet access.

- All staff must read and sign the 'ICT Code of Practice' before using any school ICT resource.
- Parents will be informed that children will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for child's access.

World Wide Web

If staff or children discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the e-safety coordinator or network manager.
Our Federation schools will ensure that the use of Internet derived materials by children and staff complies with copyright law.
Children will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

If children are given access to email:

- Children may only use approved e-mail accounts on the schools' system.
- Children must immediately tell staff if they receive offensive e-mail.
- Children 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 the schools
- Access in our Federation schools to external personal e-mail accounts may/ is 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

The Bridges Federation schools block/filter access to social networking sites and newsgroups unless a specific use is approved.

- Children will be advised never to give out personal details of any kind which may identify them or their location
- Children will be advised not to place personal photos on any social network space.
- Children will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Children should be encouraged to invite known friends only and deny access to others.

Filtering

The Bridges Federation schools work with EXA our internet provider to ensure filtering systems that are as effective as possible.

Video Conferencing

IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
Children should ask permission from the supervising teacher before making or answering a video conference call.
Video conferencing will be appropriately supervised for the child's age.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in our schools 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 schools' phone where contact with children is required.

Published Content and the Schools Web Site

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

Publishing Children's Images and Work

Photographs that include children will be selected carefully and will not enable individual children to be clearly identified.
Children's full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
Written permission from parents/carers will be obtained before photographs of children are published on the schools' Web site.
Work can only be published with the permission of the child and parents.

Information System Security

The Federated school ICT systems capacity and security will be reviewed regularly by SMT
Virus protection will be installed and updated regularly by network manager

Protecting Personal Data

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

Assessing Risks

The schools 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 schools' computer. Neither the schools nor Norfolk County Council can accept liability for the material accessed, or any consequences of Internet access.
The Federation will audit ICT use to establish if the E-safety Policy is adequate and that the implementation of the E-safety Policy is appropriate. This should happen on a regular basis.

Handling e-safety Complaints

Complaints of Internet misuse will be dealt with by a SMT.
Any complaint about staff misuse must be referred to the Headteacher.
Complaints of a child protection nature must be dealt with in accordance with the Federation schools' safeguarding procedures. Links to Safeguarding Policy
Parents/carers will be informed of the Complaints Procedure.

Communication of Policy

Pupils

Rules for Internet access will be posted in all networked rooms.
Children will be informed that Internet use will be monitored.

Staff

All staff will be given the Federation's 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.
Supply Teachers should be logged on the 'Supply' log on.

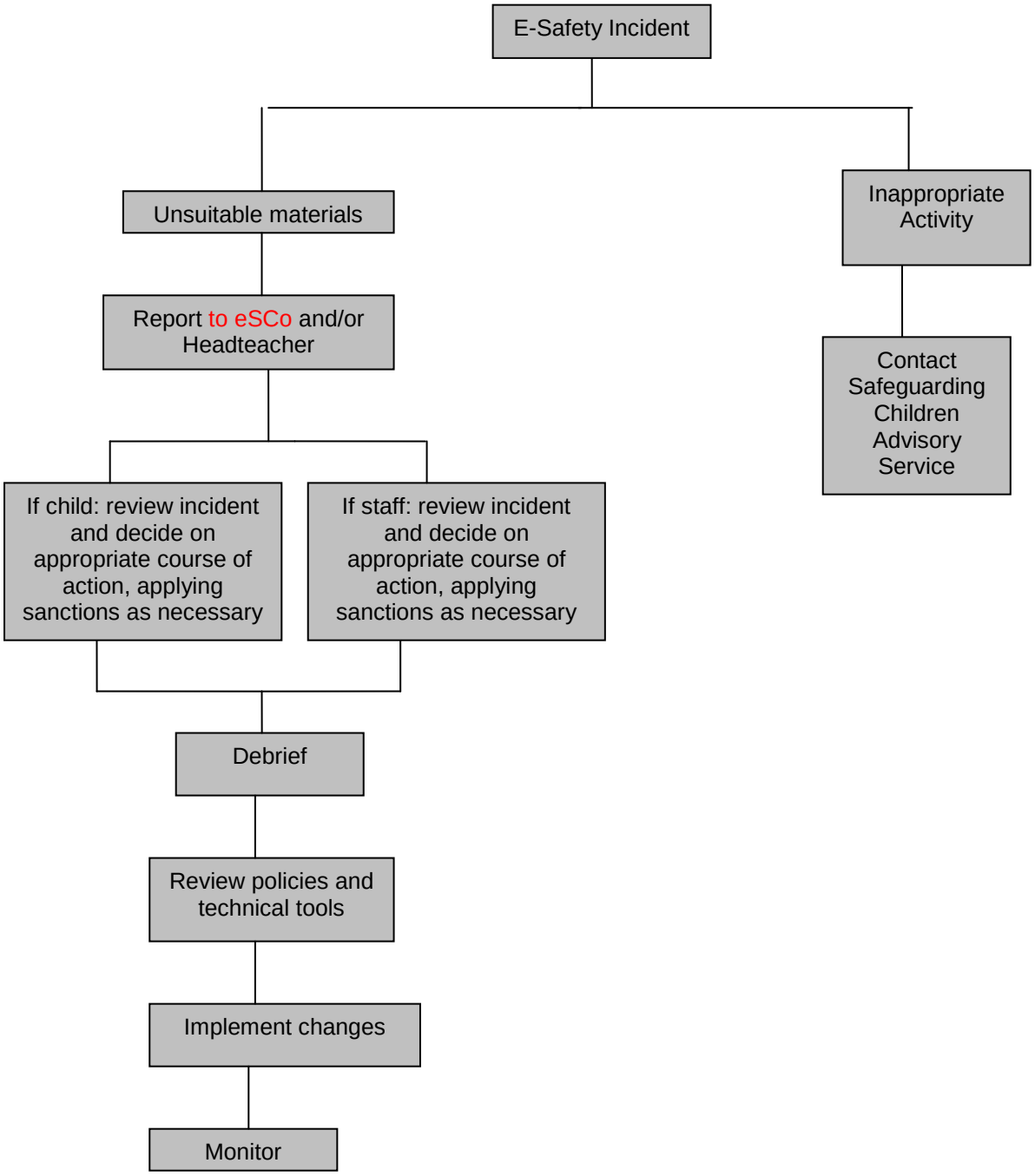
Parents

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

Community

If community members use the system they must be informed of the rules/policy.

Flowchart for responding to e-safety incidents in The Bridges Federation



Key Stage 1

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 can send and open emails together.

We can write polite and friendly emails to people that we know.

Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

We ask permission before using the Internet.
We only use websites that an adult has chosen.
We tell an adult if we see anything we are uncomfortable with.
We immediately close any webpage we not sure about.
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 children and the school by describing acceptable and unacceptable computer use.
The schools own 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 schools.
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.