E-ACT

St Ursula's E-ACT Academy
Online Safety (E-Safety) Policy
July 2017

E-ACT

The E-Safety Policy is part of the Academy Improvement Plan and relates to other policies including those for ICT, bullying and for child protection.

- The Academy's E-Safety lead is Mrs Durston (IT Lead)

- Our E-Safety Policy has been written by the school, building on the Bristol Safeguarding Children Board (BSCB) E-Safety strategy and government guidance. It has been agreed by senior management and approved by the Safeguarding System Lead.
  .
- The E-Safety Policy was written by Ross Moody (Headteacher)
- It was approved by John Spring (Regional Safeguarding Lead) on:

  …July 2017……
- The next review date is (at least annually):…July 2018…

Learning

1. Why the Internet and digital communications are important

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with high quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

2. Internet use will enhance and extend learning

Staff will be made aware of and pupils will be educated in the safe use of the internet.

Clear boundaries will be set and discussed with staff and pupils, for the appropriate use of the Internet and digital communications.

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

3. Pupils will be taught how to evaluate Internet content

Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

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

E-ACT

Managing Internet Access

1. Information system security

School ICT system security will be reviewed regularly.

Virus protection will be installed and updated regularly.

2. E-mail

Pupils and staff should only use approved curriculum e-mail accounts at outlook.office.com

Pupils must be made aware of how they can report abuse and who they should report abuse to.

Pupils must report if they receive offensive or inappropriate e-mail.

In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The school should consider recommending a standard mail format for all users.

The forwarding of chain letters is not permitted.

3. Published content and the school website

Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.

The Principal or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

4. Publishing students' images and work

Photographs that include pupils will be selected carefully so that images of individual pupils cannot be misused.

Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.

Written permission, using the approved permission form, from parents or carers will be obtained before photographs of pupils are published on the school website.

Work can only be published with the permission of the pupil and parents/carers.

5. Social networking and personal publishing

The school will educate people in the safe use of social networking sites, and educate pupils in their safe use.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Pupils must be made aware of how they can report abuse and who they should report abuse to.

Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.

Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.

Pupils should be made aware of 'Sexting' (Someone taking an indecent image of themselves and sending to their friends or boy / girlfriend via a mobile phone or some other form of technology) and that they could potentially be distributing illegal child images. Staff working at St Ursula's E-ACT Academy will ensure that they are aware of the risks associated with the use of the internet and how to respond appropriately to a 'Sexting' incident.

6. Managing monitoring and filtering

The school will work in partnership with Bristol City Council and E-ACT to ensure that systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Lead or the Network Manager.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

7. Managing videoconferencing

Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing will be appropriately supervised for the Pupils' age.

8. 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.

The senior leadership team should consider in their policy making that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Where contact with pupils is required to facilitate their learning, staff will be issued with a school phone.

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

It should be noted that games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

Adults may only use mobile phones in the staffroom and never photograph pupils with one.

9. Protecting personal data

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

Policy Decisions

1. Authorising Internet access

All staff must read and sign the 'Staff Acceptable Use Policy and Code of Conduct for ICT' before using any school ICT resource, including any laptop issued for professional use.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Parents/carers will be asked to sign and return a consent form.

2. Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Bristol City Council can accept liability for any 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 and effective.

Schools must ensure monitoring software and appropriate procedures are in place to highlight when action needs to be taken by the school.

3. Handling E-Safety complaints

Complaints of Internet misuse will be reported to the E-Safety Lead and action in-line with the Bristol Safeguarding Children Board E-Safety policy will be taken.

Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children should be reported to Social Services within one working day in accordance with Bristol Safeguarding Board policies.

Any complaint about staff misuse must be referred to the Principal and if the misuse is by the Principal it must be referred to the chair of governors in line with Bristol Safeguarding Board Child Protection procedures.

Pupils, parents and staff will be informed of the complaints procedure.

Communicating E-Safety

1. Introducing the E-Safety Policy to pupils

E-Safety rules will be posted in all rooms where computers are used.

Pupils will sign a Pupil Acceptable Use Policy and it will be displayed in all classrooms.

Pupils will be reminded at the start of every ICT lessons about E-Safety.

Staff and Pupils will celebrate E-Safety Day with appropriate lessons.

All system users will be informed that network and internet use will be monitored.

A programme of E-Safety training and awareness raising will be put in place in-line with the Bristol Safeguarding Children Board's E-Safety Strategy.

2. Staff and the E-Safety Policy

All staff will be given access to the Academy E-Safety Policy and its importance explained.

Staff must be informed that network and Internet traffic can be monitored and traced to the individual use, including staff laptops.

Staff that manage filtering systems or monitor ICT use will be supervised by senior leadership and work to clear procedures for reporting issues.

Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

3. Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the Academy E-Safety Policy in newsletters, the school brochure and on the school website.

The Academy will maintain a list of E-Safety resources for parents/carers.