E-Safety Policy

Policy Date: May 2018
Review Date: May 2019

ICT Co-ordinator – S Manifold

Rationale

The use of the internet is important in supporting high quality learning and teaching at REACH. Within our aim to produce competent ICT literate learners, the use of ICT and the internet is an important tool particularly in developing research skills and individualised learning programmes for our students. However REACH recognises its responsibilities in ensuring safe use of the internet and other communication systems for all students and so this policy outlines our strategy to protect students. Our e-Safety Policy has been written by the service, building on the Stoke-on-Trent e-Safety Policy and government guidance.

Student Protection

It is our intention to protect our students from inappropriate or undesirable material. The following criteria define inappropriate or undesirable materials.

- Obscene, offensive, illegal or inaccurate.
- Students should not feel or become uncomfortable, threatened or worried by material or information on websites or from e-mail.
- Similarly students must not harass, insult, attack others, violate copyright, or trespass in others' folders.
- Where students images and work are used in published materials including the REACH website or other areas the REACH will ensure that:
    - Parent/carer permission will be obtained on student entry.
    - E-mail and postal addresses of pupils will not be published
    - Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for the work to be displayed.

Managing Internet Access

E-mail

- Students will only use the approved e-mail account on the Centre's system.
- Students must immediately tell a member of staff if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain letters will be actively discouraged and the potential harm that can be caused will be included within e-safety learning.
- Students may only access the Internet when a member of staff is present or if they have permission.

Public Web published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone number. Staff or Students' personal information will not be published.
- E-mail addresses will be published carefully, to avoid spam harvesting.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications, including respect for intellectual property rights and copyright.

Web Publishing Students' images and work

- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of Students are electronically published to the web.

Social networking and personal publishing

- The City Council/REACH will block/filter access to social networking sites, except those specifically purposed to support educationally approved practice.
- Newsgroups will be blocked unless a specific use is approved.
- Staff and students will be advised never to give out personal details of any kind which may identify them or their location.
- Staff and students should be advised not to publish specific and detailed private thoughts on social networking sites.
- Staff and students will not contact each other using social networking sites.

Policy Decisions

Authorising Internet access

- A current record will be maintained of all staff and students who are granted access to REACH electronic communications, which includes internet access. The record will be kept up-to-date, for instance a member of staff may leave or a students access be withdrawn.
- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.
- Parents/carers will be asked to sign and return a consent form.
- Sanctions for inappropriate use will be drawn up and shared with staff and students.

Assessing risks

- REACH will take all reasonable precautions to ensure that users access only appropriate 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 Centre computer. Neither REACH nor Stoke-on-Trent City Council can accept liability for the material accessed, or any consequences of Internet access.
- REACH will audit ICT provision to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

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 the Centre's child protection procedures.
- Students and parents/carers will be informed of the complaints procedure.
- Parents/carers and students will need to work in partnership with staff to resolve issues.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Cyberbullying – Understanding and addressing the issues

- The opportunities for students to bully or be bullied via technology (including mobile), such as e-mail, texts or Social Networking, are becoming more frequent.

- As such, teaching students about appropriate behaviours when using technology provides a vital grounding for future use. Whilst not wanting to provoke unrecognised opportunities in students, consideration must be given to suitable teaching and procedures to address any issues of cyberbullying.
- As felt appropriate for the age and use of technology by the students:
    - The school's anti-bullying policy will address cyberbullying. As with other whole-school policies, all staff and young people will be included and empowered to take part in the process.
    - Students, parents/carers, staff and governors will all be made aware of the consequences of cyberbullying. Young people and their parents/carers will be made aware of students' rights and responsibilities in their use of new technologies, and what the sanctions are for misuse.
- Sessions will be delivered by a CEOP ambassador

Cyberbullying - How will risks be assessed?

- REACH will take all reasonable precautions to ensure against cyberbullying whilst students are in its care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a Centre's computer will not occur. Neither the REACH, nor Stoke-on-Trent City Council, can accept liability for inappropriate use, or any consequences resulting outside of school.
- REACH will proactively engage with all students in preventing cyberbullying by:
    - understanding and talking about cyberbullying, e.g. inappropriate use of e-mail, text messages;
    - ensuring easy and comfortable procedures for reporting;
    - promoting the positive use of technology;
    - evaluating the impact of prevention activities.
- Records of any incidents of cyberbullying will be kept and will be used to help to monitor the effectiveness of the Centre's prevention activities.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will cyberbullying reports/issues be handled?

- Complaints of cyberbullying will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher.
- Evidence of offending messages, pictures or online conversations will be kept, in order to demonstrate to others what is happening. It can be used by REACH, internet service provider, mobile phone company, or the police, to investigate the cyberbullying.
- Students and parents/carers will be informed of the complaints procedure.

- Parents/carers and students will need to work in partnership with staff to resolve issues.

- Incidents of cyberbullying will be dealt with via the bullying and behaviour policies.

Communicating the e-safety Policy

Introducing the e-safety policy to students

- E-safety rules will be posted in all rooms and discussed with students on entry to REACH and as the need arises.
- Students will be informed that network and Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- E-Safety rules will be on the website.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its application and importance explained.
- All staff will be informed that all computer and Internet use will be monitored. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on the REACH e-Safety Policy will be provided as required.
- Staff that manage filtering systems or monitor ICT use will have clear procedures for reporting issues.
- The E-Safety Policy will be on the website.

Enlisting parents' support

- Parents'/carers' attention will be drawn to the School e-Safety Policy in initial interviews and it will be on the REACH website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.

REACH

Rules for Safe Internet Use

We use the school computers and the Internet for learning. These rules will help us be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will only use my own network login and password, which I will keep secret.
- I will not knowingly download or bring software on storage devices into REACH without permission.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I will never give out personal details such as my home address, telephone numbers or arrange to meet anyone.
- If I see anything I am not happy with, or receive messages I do not like, I will tell a teacher immediately.
- I know that the school may check my computer files and any Internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.
- I will not disclose details of staff/students over social networks
- I will not use electronic devices to take pictured of staff or students without prior permission
- **I have read, understood and agree with the Information Systems Code of Conduct.**

Name:_____ **Signed:**_____ **Date:**_____

Staff Information Systems
Code of Conduct
May 2018

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 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 using remote access where appropriate and if necessary.
- 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 students are compatible with my professional role.
- I will not publish any content which might put myself or the school in a compromising situation, breech the school's confidentiality in any way or bring the school's reputation into disrepute.
- I will promote e-safety 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.
- I will not use electronic devices to take images off staff/students without prior permission
- I will not disclose and details of staff/students over social networks

REACH 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 Centre'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: …… PRINT: …… Date: ……

Accepted for REACH: …… PRINT: ……