Saffron Valley
COLLEGIATE

THE ACCEPTABLE USE OF THE INTERNET AND RELATED TECHNOLOGIES, AND E-SAFETY

LAST REVIEWED: 02.12.15, amendment 23.11.16
TO BE REVIEWED: Autumn 2017

This Policy is written in the context of and with regard to the statements below:

The Federation and its component PRUs seek to provide a personalised educational experience that identifies and responds to the circumstances and needs of each individual young person and in doing so will enable them to fulfil their potential and become successful young people.

EQUALITIES STATEMENT:

All who work at the PRU are committed to the celebration of diversity, and the challenging of disadvantage and discrimination, in all its forms.

These values are explicit to the ethos of the PRU and implicit in all policies and practices.

Overview

This policy should be read in conjunction with the SVF Safeguarding Policy.
The Green Paper *Every Child Matters* and the provisions of the *Children Act 2004*, *Working Together to Safeguard Children* set out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of PRU
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the PRU to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the PRU's physical buildings.

This policy document is drawn up to protect all parties – the students, the staff and the PRU and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

1. The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in PRU and, more importantly in many cases, used outside of PRU by children include:

- The Internet
- e-mail
- Our Managed Learning Environment via Fronter
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Blogs and Vlogs
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications
- Tablets/iPads.

This list is not exhaustive.

2. Whole PRU approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this PRU:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-safety education programme for pupils, staff and parents.

Reference: Becta - E-safety Developing whole-PRU policies to support effective practice [1]

3. Roles and Responsibilities

e-Safety is recognised as an essential aspect of strategic leadership in this PRU and the Headteacher, with the support of Management Committee, aims to embed safe practices into the culture of the PRU. The headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to a member of the senior management team.

The Management Committee need to have an overall understanding of e-Safety issues and strategies at this PRU. We ensure our Management Committee are aware of our local and national guidance [2] on e-Safety and are updated on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following PRU e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the PRU's policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of PRU network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- Cyberbullying procedures;
- their role in providing e-Safety education for pupils;

4. The Use of the Internet

The following procedures are recommended for community groups:

- Ban access to sex sites, pornographic sites and violent and racially abusive sites
- Place the computer where everyone can use it and where everyone can see it, rather than out of sight in another room.
- Supervise use of the Internet.
- Suggest sites that could be visited by children and young people, e.g. those connected with children's TV programmes.
- Talk to children and young people about what sorts of sites they can and

[1] http://PRUs.becta.org.uk/index.php?section=is

[2] Safety and ICT - available from Becta, the Government agency at: http://PRUs.becta.org.uk/index.php?section=lv&catcode=ss_lv_str_02&rid=10247

cannot visit.

- Ensure children are aware that chat sites are open to misuse and they should be as cautious of strangers they meet on the Internet, as they would be when meeting strangers in real life.
- Advise that children and young people do not give out personal details over the Internet, e.g. surname, address, phone number or e-mail address.
- Advise children to never arrange a face-to-face meeting with anyone they come into contact with on the Internet.
- Encourage children to report anything they come across which they feel is abusive or offensive.
- Limit the amount of time children spend online.
- Explore the use of filters, which block access to certain sites (although remember that these are unlikely to be foolproof and cannot replace proper supervision).
- In addition, groups should not publish recognisable photographs of children on their own websites.

Benefits of using the Internet in education include

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in government initiatives such as the National Grid for Learning (NGfL) and the Managed Learning Environment (MLE);
- Educational and cultural exchanges between pupils world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Staff professional development through access to national developments, educational materials and good curriculum practice, training via webinars
- Communication with support services, professional associations and colleagues;
- Improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LEA and DfE.

How Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the 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 and retrieval.
- They will have a clear understanding of plagiarism and an understanding of how to use the WWW as a resource.

Evaluating Internet content

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.

- It is true that there is some material on the Internet that would be offensive to most people, such as pornography, racist and fascist material, and children if using the Internet unsupervised can access this. Our main educational providers try to 'filter' known offensive locations of material of this kind, but there is too much for this filtering to be very effective, and the locations change frequently. The only way to block access to this kind of material is to have a restricted range of pages available, in which case many of the advantages of the global and dynamic nature of the Internet may be lost. It is a feature of the Internet that the information available is free. Increasing restrictions will undoubtedly lead to systems of charging for access to specific material, in addition to the other costs described. An alternative system is to educate pupils and encourage an acceptable use policy and partnership between home and school in dealing with the less savoury side of Internet use. This ethos is promoted via education of pupils, at parent meetings, leaflets sent home and specific letters and agreements between school and home.

- Staff should ensure that the use of Internet derived materials by staff and pupils comply 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.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

Management of e-mail

- Pupils are given an e-mail account to use on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

5. New Technology

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

6. Assessment of Risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The PRU 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 school computer. Neither the PRU nor London Borough of Croydon can accept liability for the material accessed, or any consequences of Internet access.
- 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.
- The Headteacher will ensure that the t policy is implemented and compliance with the policy monitored.

7. Management of Filtering

- The school will work in partnership with parents, the LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the ICT co-ordinator/member of the senior management team.
- The PRU will manage the configuration of the filtering server via our technical advisors.
- Where possible, the filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

8. The Management of Digital Images: Photography, Video and Website

These procedures comply with the requirements of the Data Protection Act 1998, Freedom of Information Act 2000, Human Rights Act 1998 and other relevant acts regarding the taking and use of photographic images of children.

The use of cameras should be considered an essential and integral part of everyday life. As such, children and young people and professionals are to be encouraged to use such technology in a positive and responsible way.
It has to be recognised however, that digital technology has increased the potential for cameras and images to be misused and inevitably there will be concerns about the risks to which children and young people may be exposed.
We recognise that having the right policies and practices in place will also protect PRU staff from misunderstanding, false accusations and damage to reputation around the use of digital images.
Practical steps must be taken to ensure that the use of cameras and images will be managed sensitively and respectfully. A proactive and protective ethos is to be reflected which will aim to promote effective safeguarding practice.
It must, however, be acknowledged that technology itself will not present the greatest risks, but the behaviours of individuals using such equipment will.

These procedures aim to ensure safer and appropriate use of cameras and images through agreed acceptable use procedures. This is to be in line with legislative requirements and will aim to respect the rights of all individuals.

These procedures will apply to:

- All individuals who are to have access to and/or be users of work-related photographic equipment. This will include children and young people, parents and carers, early years practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. *This list is not to be considered exhaustive.*

- The use of any photographic equipment. This will include mobile phones, video cameras, webcams and portable gaming devices with inbuilt cameras as well as other forms of digital technology and resources for storing and printing images. *This list is not to be considered exhaustive.*

The Designated Safeguarding Lead is to be responsible for ensuring the acceptable, safe use and storage of all technology and images. This will include the management, implementation, monitoring and review of these procedures.

All images will be used in a manner respectful of the eight Data Protection Principles. This means that images will be:

i. Fairly and lawfully processed
ii. Processed for limited, specifically stated purposes only
iii. Used in a way that is adequate, relevant and not excessive
iv. Accurate and up to date

v. Kept on file for no longer than is necessary
vi. Processed in line with an individual's legal rights
vii. Kept securely
viii. Adequately protected if transferred to other countries.

We will never publish identifiable photographs of young people.
Where showcasing examples of pupils' work we will not use their names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment, and all adults working with children sign an Acceptable Use Policy and e-safety agreement form.

The Headteacher, (or Deputy Headteacher in her absence), reserves the right to immediately contact the Local Authority Designated Officer (LADO) should she have safeguarding concerns regarding the image contents/appropriate use of a member of staff's mobile 'phone, camera or other electronic device (refer to relevant parts of this policy). The LADO's guidance will be followed.

All parents/carers are asked to sign a form to give their consent (or otherwise) to photographs, digital images and videos being taken, and are made aware of the context, nature and the use to which these will be put.