The Percy Hedley Foundation

PERCY HEDLEY EDUCATION SERVICES

E SAFETY POLICY
&
ICT ACCEPTABLE USAGE AGREEMENT

Policy Control/Monitoring

Version:	1.0
Approved by: **(Name/Position in Organisation)** **Date:**	Lynn Watson Director of Education 5 July 2015
Accountability: **(Name/Position in Organisation)**	Katie Murray Head of IT
Author of policy: **(Name/Position in organisation)**	Katie Murray Head of IT
Date issued:	5 July 2015
Revision Cycle:	1
Revised (Date):	5 July 2016
Target audience:	All education staff with direct contact with children and young people
Amendments/additions	
Replaces/supersedes:	

Associated Policies: **(insert hyperlinks)** **Associated National Guidance**	IT Policy Behaviour Policy Bullying Policy Child Protection Policy Adult Protection Policy Health & Safety Policy
Document status	This document is controlled electronically and shall be deemed an uncontrolled documented if printed. The document can only be classed as 'Live' on the date of print. Please refer to the staff login section of the internet for the most up to date version.

Equality Impact Assessment

This document forms part of Percy Hedley's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.
As part of its development this document and its impact on equality has been analysed and no detriment identified.

Version Control Tracker

Version Number	Date	Author/ Title	Status	Comment/Reason for Issue/Approving Body
1.0	5/7/15	Katie Murray	Deputy Headteacher	

Roles & Responsibilities

The following roles will have specific areas of responsibility for this policy:- ***(add/delete as appropriate)***

Role	Responsibility
Chief Executive	Overall safety of all pupils
Director of Human Resources Department	
Head of Service/Head of department	
Training Development Officer	
Quality Manager	
Health and Safety Manager	Linked to Health& Safety Policy
Lead Nurse	

Introduction

As a Non Maintained Specialist Provider working with our local, national and international communities, ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools/colleges need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking – for example Facebook; Bebo
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Percy Hedley, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreements (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school/college (such as PCs, laptops, personal digital assistants (PDAs), webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school/college premises (such as laptops, mobile phones, camera phones, and portable media players, etc).

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school/college the Governing Body have ultimate responsibility to ensure that the policy and practices are embedded and monitored. This responsibility is delegated to the Head. Any extra permission given by the Head must be recorded (e.g. memos, minutes from meetings) in order to be valid.

The named person (Safeguarding Officer) and ICT manager have the responsibility of ensuring these policy is upheld by all members of the school/college community and that they have been made aware of the implication this has. It is the role of these members of staff to keep abreast of current issues and guidance through organisations such as the LA, Becta, CEOP (Child Exploitation and Online Protection), Childnet and Local Authority Safeguarding Children Board.

This policy, supported by the school/college's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school/college community. It is linked to the following mandatory school/college policies: child protection, health and safety, home–school/college agreements, safeguarding policy and behaviour/pupil discipline (including the anti-bullying) policy.

E-safety skills development for staff

- Our staff receive regular information and training on e-safety issues in the form of full staff meetings and memos.

- New staff receive information on the school/college's acceptable use policy as part of their induction through their staff handbooks.

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school/college community.

- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

Communicating the school/college e-safety messages

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.

- Pupils will be informed that network and Internet use will be monitored.
- E-safety posters will be prominently displayed, especially in the ICT suite.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote E-safety. We regularly monitor and assess our pupils' understanding of e-safety.

- The school/college/college provides opportunities within a range of curriculum areas and discrete ICT lessons to teach about e-safety (in accordance with the medium term planning.)
- Educating pupils on the dangers of technologies that maybe encountered outside school/college may also be done informally when opportunities arise.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff have access to this through Administrator Rights on the NGFL network. The pupils from Year R upwards have individual logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

Data Security

The accessing and appropriate use of school/college data is something that the school/college takes very seriously. Staff are aware of their responsibility when accessing school/college data. Level of access is determined by the Associate Director. Data can only be accessed and used on school/college computers or laptops. Staff are aware they must not use their personal devices for accessing any school/college/pupil data.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

- All staff must read and agree to the 'Acceptable ICT Use Agreement' before using any school/college ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school/college software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- School/college internet access is controlled through the LA's web filtering service.

- Our school/college also employs some additional web filtering.

- Staff and pupils are aware that school/college based email and internet activity can be monitored and explored further if required.

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the class teacher who must inform an e-safety co-ordinator.

- It is the responsibility of the school/college, by delegation to the technical support; to ensure that Anti-virus protection (Sophos) is installed and kept up-to-date on all school/college machines.

- If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first.

- Pupils and staff are not permitted to download programs or files on school/college based technologies without seeking prior permission from the ICT Manager.

- If there are any issues related to viruses or anti-virus software, the ICT manager should be informed through the ‘Computer Problems’ book held in the ICT suite.

Managing other Web 2 technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school/college endeavours to deny access to unmonitored social networking sites such as Facebook to pupils within school/college.

- There should be no communication between staff and pupils through social networking sites such as Facebook.

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school/college.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Associate Director.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school/college chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school/college allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school/college allow a member of staff to contact a pupil or parent/carer using their personal device.
- Pupils are not allowed to bring personal mobile devices/phones to school/college unless this is for educational purposes set by the teacher (even then, strict monitoring and controlled usage will only be permitted).
- The school/college is not responsible for the loss, damage or theft of any personal mobile device.

- The sending of inappropriate text messages between any member of the school/college community is not allowed.
- Users bringing personal devices into school/college must ensure there is no inappropriate or illegal content on the device.

Managing email

The use of email within most schools/colleges is an essential means of communication for both staff and pupils. Educationally, email can offer significant benefits including; direct written contact between schools/colleges on different projects, be they staff based or pupil based, within school or internationally. We recognise that pupils need to understand how to style an email in relation to their age and good ‘netiquette’. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

- The school/college gives all staff their own email account to use for all school/college business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. This should be the account that is used for all school/college business.
- Under no circumstances should staff contact pupils, parents or conduct any school/college business using personal email addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school/college headed paper.
- Pupils may only use school/college approved accounts on the school/college system and only under direct teacher supervision for educational purposes.
- The following pupils have their own individual school/college issued accounts- Year 3-6. All other pupils use a class/ group email address.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arranging to meet anyone without specific permission, virus checking attachments.

- Pupils must immediately tell a teacher/tutor/trusted adult if they receive an offensive e-mail.
- Staff must inform the ICT manager if they receive an offensive e-mail.
- Pupils are introduced to email as part of the ICT Scheme of Work at Year 3.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school/college community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school/college equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on school/college trips.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others, this includes when on school/college trips. With the consent of the class teacher, pupils are permitted to take digital cameras from school/college to record images and can download these images on the school/college network.

Publishing pupil’s images and work

On a child’s entry to the school/college, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school/college web site
- on the school’s/college’s Learning Platform
- in the school/college prospectus and other printed publications that the school/college may produce for promotional purposes
- recorded/ transmitted on a video or webcam

- in display material that may be used in the school/college's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school/college
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school/college unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' full names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

Before posting pupils' work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

Images/films of children are stored on the school/college's network.

- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Associate Director
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school/college network/ Learning Platform.
- Teaching Staff have the responsibility of deleting the images when they are no longer required, or when the pupil has left the school/college.

Misuse and Infringements

Complaints

- Complaints relating to e-safety should be made to the ICT manager or Associate Director
- All incidents will be logged and followed up.

- Complaints of a child protection nature must be dealt with in accordance with school/college child protection procedures and must be reported to the Named person (Safeguarding Officer).

- Pupils and parents will be informed of the complaints procedure.

Inappropriate material (see ICT Acceptable Use Agreement)

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-safety co-ordinators.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT manager, depending on the seriousness of the offence; investigation by the Associate Director/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

- Users are made aware of sanctions relating to the misuse or misconduct.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school/college. We regularly consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school/college.

- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school/college website)

- The school/college disseminates information to parents relating to e-safety where appropriate in the form of;

  - Information sessions/workshops
  - Posters
  - Newsletter items

- Parents will be advised that the use of social network spaces outside school/college is inappropriate for primary aged pupil.

- Parents/carers are expected to reinforce the guidance from school/college when using technologies at home. The school/college will not be responsible for communications between pupils’ outside school through social networking sites.

Monitoring & Review

Overall responsibility for the operation of the procedure lies with the xxxxx. The effectiveness of the procedure will be formally reviewed and monitored as a minimum on a xxxxxx basis to ensure that it continues to meet the requirements of The Foundation, the specific service area and that it reflects best practice and statutory legislation as appropriate.

The below table outlines the monitoring and compliance requirements of the procedure:

Element Monitored	Lead Person	Tool	Frequency	Reporting Arrangement	Lead Person - Act on Recommendation	Lead Person – Dissemination of Lessons Learned
E.g Adherence to policy	*Policy Author*	*Audit*	*Annually*		*Policy Author*	*Policy Author*