E SAFETY
&
ICT ACCEPTABLE USAGE POLICY

Education Services

Policy Control/Monitoring

Version:	V0.3
Approved by: **(Name/Position in Organisation)** **Date:**	Carole Harder CEO May 2019
Accountability: **(Name/Position in Organisation)**	Heads of Educational Services
Author of policy: **(Name/Position in organisation)**	Jo Reece-Proud HCP
Date issued:	5 July 2015 (V0.1)
Revision Cycle:	Bi-annually
Revised (Date):	May 2019
Target audience:	All education staff with direct contact with children and young people
Amendments/additions	May 2019 JRP included reference to PHF Using images of people and consent procedure.
Replaces/supersedes:	V0.1 V0.2

Associated Policies: **(insert hyperlinks)** **Associated National Guidance**	IT Policy Behaviour Policy Bullying Policy Child Protection Policy Adult Protection Policy Health & Safety Policy Using images of people and consent procedure.
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 Head PHS		
2.0	5/7/18			
3.0	20/5/19	Joanne Rees-Proud College Principal		

Roles & Responsibilities

The following roles will have specific areas of responsibility for this policy:

Role	Responsibility
Chief Executive	Overall responsibility
Heads of Education Services	To ensure the appropriate the deployment of this policy and to ensure that this policy is kept up to date in accordance with current regulations, legislation and guidance.
Pupils, Parents and Staff	Adherence to this policy.

CONTENTS

1. 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.

2. Purpose

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/students 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/students) 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/students and staff, but brought onto school/college premises (such as laptops, mobile phones, camera phones, and portable media players, etc.)

3. Scope

This policy is applies to all members of the school/college community (Teachers/Tutors, Therapists, Support Staff, Parents, Pupils/Students and members of the schools/college Governors).

4. 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/students (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.

5. Principles

5.1 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.

5.2 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/Students will be informed that network and Internet use will be monitored.

- E-safety posters will be prominently displayed, especially in the ICT suite.

5.3 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 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/students on the dangers of technologies that maybe encountered outside school/college may also be done informally when opportunities arise.

- Pupils/Students 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/Students are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.

- Pupils/Students are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils/Students 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/Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

5.4 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/students are regularly reminded of the need for password security.

5.5 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. 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.

5.6 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/students.
- 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.

5.7 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/students are aware that school/college based email and internet activity can be monitored and explored further if required.
- If staff or pupils/students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the class teacher/tutor 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/students wish to bring in work on removable media it must be given to the teacher for a safety check first.
- Pupils/Students 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.

5.8 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/students 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/students within school/college.
- There should be no communication between staff and pupils/students through social networking sites such as Facebook.
- All pupils/students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils/Students 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/Students 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/students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils/Students are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils/students 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/students using the LA Learning Platform or other approved systems.

5.9 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.

5.10 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/student or parent/carer using their personal device.
- Pupils are not allowed to bring personal mobile devices/phones to school unless this is for educational purposes set by the teacher (even then, strict monitoring and controlled usage will only be permitted). Students in college are permitted to carry personal mobile phones but are encouraged to only use these in free periods such as break and lunchtime and not during session time.

- 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.

5.11 Managing email

The use of email within most schools/colleges is an essential means of communication for both staff and pupils/students. Educationally, email can offer significant benefits including; direct written contact between schools/colleges on different projects, be they staff based or pupil/student based, within school/college or internationally. We recognise that pupils/students 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/students 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/students, 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/Students 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 issued accounts-Year 3-6. All other pupils use a class/ group email address. All college students have a college issued account.
- 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/students 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/students are introduced to email as part of the ICT Scheme of Work at Year 3.

5.12 Safe Use of Images

Please refer to Percy Hedley Foundation Using images of people and consent procedure.

5.13 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/young person 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 pupils.
- 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'/students' outside school/college through social networking sites.

6. Monitoring & Review

Overall responsibility for the operation of the procedure lies with the Head Teacher or College Principal. The effectiveness of the procedure will be formally reviewed and monitored as a minimum on a bi-annual 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:

7. Associated Policies & References

IT Policy
Behaviour Policy
Bullying Policy
Child Protection Policy
Adult Protection Policy
Health & Safety Policy
Using images of people and consent procedure.