WETHERBY-PEMBRIDGE SCHOOL

ICT Usage Policy

September 2020 – August 2021

Primary person responsible for this policy: Ian Stephenson

Job title: Digital Literacy Coordinator

Last review date: June 2020

Next review date: June 2021

Circulation: This policy is available to parents on request. It is addressed to all members of staff and volunteers and applies wherever they are working with children.

‘Parents’ refers to parents, guardians and carers.

Contents

Appendices

Scope and definition

The acronym ICT (Information and Communications Technology) is commonly used to refer to the increasingly integrated world of data processing and telecommunications systems, the internet, applications, networks and platforms which support hardware such as computers, phones, tablets, electronic whiteboards, projectors, TVs and audio-visual devices used by individuals and organisations.

In this document the term '**ICT resources**' encompasses all of the hardware, software, systems and network facilities of the school, including Wi-Fi internet access, email and social media accounts. Although the policy focuses on the use of ICT resources within the control of the school, the principles described here apply equally to the use of personal mobile phones, laptops and other personal electronic devices.

The competent, responsible and considerate use of ICT resources is a multi-dimensional, social and behavioural objective which is embedded within our educational processes. We take a holistic approach, and this policy is part of our overall strategy for ensuring the welfare of children within our care. This policy should therefore be read in conjunction with our other related policies, notably:

- E-Safety
- Safeguarding
- Anti-Bullying
- Social Media
- Mobile Phones and other Personal Electronic Devices
- Photos and Images
- PSHEE

Our policies comply with *Keeping Children Safe in Education*[1] and are regularly reviewed and updated in consultation with a variety of resources, including:

- *CEOP Command (formerly known as Child Exploitation and Online Protection* www.thinkuknow.co.uk
- *UK Safer Internet Centre* www.saferinternet.org.uk/
- *NSPCC* www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
- *UK Council for Child Internet Safety (UKCCIS)* www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Bearing in mind the scope and content of our other related (above-mentioned) policies, the objectives of this ICT Usage Policy are:

- to promote awareness amongst children and parents of some of the practical, social, and legal issues when taking advantage of ICT resources, and

- to clarify the rules which children must follow

The risks relating to the use of ICT resources are such that this policy may appear rather cautionary and prohibitive. In practice, we embrace the principle that, properly used ICT can be one of the most important resources for learning and development. Reinforcing the principle expressed in our E-Safety Policy, we believe that the internet and the constantly evolving technologies and devices to which children have access can be tools that enrich their lives. We therefore teach them to view technology and new media positively whilst simultaneously protecting themselves.

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
The 2020 KCSIE changes have been suspended due to COVID-19 and a date has not been decided for when this will resume. Keeping children safe in education (KCSIE) 2019 remains statutory guidance.

The education of children in regard to risks arising from ICT usage is incorporated into the curriculum, not only within ICT and PSHE lessons, but wherever and whenever it makes sense to reinforce concepts at an age-appropriate level. This includes assemblies, guest speakers and parent information events.

Expectations of children

All children are encouraged to use ICT resources to support their programmes of learning. Children have no right to use ICT resources for other purposes (e.g. personal recreational, administrative or commercial) which are not connected to their programme of learning.

Children are expected to:

- ask questions and share any concerns or confusion they have about how to interact with ICT
- demonstrate a responsible approach to ICT usage, show consideration for all other users, and treat ICT resources with care and respect
- be clear, polite, respectful and responsible in all electronic communications and use of social media, remembering that they must not write, nor post on-line, anything which could embarrass themselves, other children, staff, parents or the school if it later became more widely seen than was originally intended
- obtain permission from a staff member before connecting any personal electronic device with the ICT resources of the school; removable storage (memory sticks, external hard drives, CDs/DVDs) must be virus-checked before being connected to the school ICT resources
- observe all the conditions of usage laid out in this policy, **avoid the prohibited content and activities as listed in Appendix 2**, and follow the direction of staff members supervising any area where networked resources can be accessed
- report immediately to a staff member wherever they encounter breaches in the controls and security of the network or where they observe any abuse of ICT resources
- sign, and/or have a parent/guardian sign on their behalf, the acknowledgment in Appendix 1 which confirms that they have read, understood and agree to comply with the ICT Usage Policy

Any child who knowingly abuses the privileges of ICT resources will face disciplinary procedures. Please refer to the Behaviour, Discipline and Exclusion Policy for further details.

Expectations of Staff and Parents

The prohibitions listed in Appendix 2 will have little significance and effect in practice without an ongoing commitment by staff and parents to:

a) promote understanding amongst children of why things are prohibited

b) stay vigilant to the actual behaviour of children in their interaction with ICT

c) establish an environment where children are encouraged to talk and ask questions about their interaction with ICT, and where they can feel safe sharing their concerns

d) talk to each other (parents and staff) to share information and concerns

Prohibitions

The ICT resources of the school must not be used to search for, create, store, receive or transmit any materials, or to engage in any activities which are either illegal or prohibited by this policy. **Prohibited materials and activities are listed in Appendix 2**. This is a long but non-exhaustive list. Whilst the school endeavours to educate pupils about all the items on this list, pupils (and parents) should ask for help where they are not clear about any of the issues listed.

Controls, privacy and reporting of breaches

Log-on details (account names and passwords) for access to ICT resources must be kept secret and must not be written down or shared. All users must remember to log-off when they are not in close physical proximity to the machine or device to which they are logged-on. Computers and other user-controlled ICT resources should be either switched off or put on 'stand-by' after use, especially at the end of the day.

In accordance with statutory guidance, and with the aim of mitigating the risk of harmful behaviour and access to harmful materials, the school ICT resources are subject to various preventative and detective controls such as anti-virus protection, internet- and email-filtering, and usage-monitoring. Consequently, pupils should not expect their usage of school ICT resources (including email and internet browsing), or any of the material they store using school ICT resources, to be private or confidential. The school has the right to search and delete any material where it has grounds to suspect that such material may be harmful to the welfare of pupils.

Staff must remain alert to actual and potential breaches of security and of prohibited content and activities. Pupils are encouraged to look after each other and to tell staff if they become aware of prohibited content or activities, or weaknesses in network security or internet filtering. Staff must report actual or potential breaches or weaknesses to the Head of School, Pastoral Coordinator or the Digital Literacy Coordinator, in addition to any other reporting processes as required by other policies (Safeguarding, Anti-Bullying, E-Safety), for example to the Designated Safeguarding lead (DSL) who is the Head of School.

File storage and back-up

Although pupils may use school ICT resources to temporarily store copies of their work, they must not rely on the school to back-up their work.

CHILDREN MUST THEREFORE BE REMINDED TO MAINTAIN THEIR OWN PERSONAL ARRANGEMENTS FOR FILE STORAGE AND BACK-UP

Responsibility for the practical implementation of this policy

a) Security and effectiveness of the ICT resources and infrastructure

The development and maintenance of ICT services and controls, including data protection, network security and internet filters are the responsibility of the **Alpha Plus Group Director of ICT**, and are administered through a team of **On-Site Engineers** assigned to each Group location. This technical team has a key role in maintaining a safe technical infrastructure and in keeping abreast with the rapid succession of relevant developments in technology and new media.

In order to ensure the effective operation of ICT services and controls, it is essential that a member of school staff is nominated as **Digital Literacy Coordinator** and is assigned responsibility for monitoring the effective delivery of such services on behalf of all school users, and for reporting weaknesses and opportunities for improvement where necessary.

b) <u>Broader welfare issues of E-safety</u>

Our **Designated Safeguarding Lead (DSL**) has been trained, and updates their training regularly, in the safety issues relating to the misuse of ICT resources. The DSL works to ensure the security and effectiveness of the ICT controls.

The curriculum and pastoral aspects of educating children (and parents) on the risks of ICT usage, along with staff training, are explained in our *E-Safety Policy*.

All staff have an ongoing responsibility to reinforce this policy with pupils and (where practical) to monitor that their usage of ICT is in compliance with the policy. Serious or persistent breaches must be reported to the Head of School and (if safeguarding issues are suspected) to the DSL who is the Head of School.

Appendix 1

Acknowledgement of ICT Usage

(to be signed by child and parent/guardian)

Pre-Kindergarten, Kindergarten and Grade 1

S

- I will only use school computers and iPads to do things that I have been taught or my teacher says are ok.
- I will only use my own username and password. I will always keep these secret.

A

- I will only edit or delete my own files and not look at or change other people’s files.
- I will always ask before I download anything from the internet or use anything I have brought in from home for the computer.

F

- I know that I need to ask someone if it’s ok before I take their photo or video them.
- Any online messages will be polite and responsible.
- I will not create, send or pass on anything on computers that is made to upset other people.

E

- I will tell a teacher straight away if anything makes me feel unhappy or uncomfortable online.
- I will always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are examples of personal details).

- **I know that once I post a message or an item on the internet then it is completely out of my control.**
- **I understand that my school might check how I have used the internet or other technology and will talk to my parents if they are worried about my E-safety.**
- **I understand that if I don’t follow these rules, in school and outside of school, I could be stopped from using the internet or computer.**

I have read and understand these rules and agree to them.

Signed

Child: ………………………………….…… Date:…………………..……

Parent: ………………………………..…… Date:…………………..……

Grade 2 to Grade 8

When I am using the computer or other technologies, I want to feel safe all the time. I have understood and will comply with the following statements:

S

- I will only go on the internet using my own login details. I will always keep these private. If I think someone knows my password I will tell a teacher.
- I will take care of any school-owned IT equipment and return to the correct place when I have finished using it. I will not eat or drink while using IT equipment.
- I will only bring my mobile phone or other devices to school with permission from my teacher. I will only use these when my teacher tells me I can. I will not take pictures or video with my own devices.

A

Social Media/Internet Usage:

- I know that some websites and social networks have age restrictions and I should not use them unless I am old enough.
- I will not say nasty or hurtful things about any member of staff or pupil online. If I see anything like this I will tell my teacher immediately.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are examples of personal details). This includes photographs or video images of me, other pupils or members of staff.
- I will tell a teacher straight away if anything makes me feel unhappy or uncomfortable online, this includes any hurtful comments about the school, staff or pupils.
- I will never meet an online friend without taking a responsible adult that I know.

F

Managing Digital Content:

- I will only use school-owned equipment to create pictures, video and sound. Media will only be taken with permission from the individual first.
- I will not publish anything online e.g. images or pictures, without asking my teacher.
- I will only use memory sticks with permission from my teacher.
- I will not install any software on school computers.

E

Email/Messaging:

- I will only use my school email address to contact people I know or those agreed by my teacher.
- I will take care in opening any attachments sent by email. I will not open an attachment or download a file, unless I know and trust the person who has sent it.
- I will make sure all messages I send are respectful and polite.
- I will not use my school email to forward chain emails or spam.

- **I know that once I post a message or an item on the internet then it is completely out of my control.**
- **I understand that my school might check how I use the internet or other technology and will talk to my parents if they are worried about my e-safety.**
- **I understand that if I don't follow these rules, in school and/or outside of school, I could be stopped from using the internet or computer.**

I have read and understand these rules and agree to them.

Signed

Child: ……………………………..…… **Date:…………………..….**

Parent: ……………………………..…… **Date:…………………..….**

Appendix 2

List of prohibited content and activities

The ICT resources at Wetherby-Pembridge School must not be used to search for, create, store, receive or transmit any materials, nor to engage in any activities, which are either illegal or prohibited by this policy. This is a long, but non-exhaustive list. Whilst the school endeavours to educate children about all the items on this list, children (and parents) should ask for help where they are not clear about any of the issues listed.

(a) Prohibited content and materials are those which are or may be deemed to be:

- racist, sexist or causing any form of prejudicial offence
- threatening, abusive or inciting violence
- obscene, indecent or pornographic
- age-inappropriate[2]
- defamatory[3]
- promoting extremist[4] views
- promoting intolerance of the beliefs, sexuality or life choices of others
- likely to mislead or deceive others
- likely to cause unnecessary stress or anxiety to others

(b) Prohibited activities include:

- bullying (also known in this context as cyber-bullying – see our *Anti-Bullying Policy*)
- harassment – unwanted attention, pestering or persecution (including insults and 'jokes')
- arranging to meet in person with someone first met online (without first checking with parents or teachers)
- writing or posting content on the internet, social media, or school network anything which may cause harm or offence to other children, parents, staff or to the school
- sexting[5]
- 'trolling' – mischievously or maliciously upsetting or offending people on the internet or social media by posting inflammatory remarks
- pretending to be someone else, or theft of someone's identity
- gambling
- promotional, advertising or other commercial activities (unless authorized by staff)
- plagiarism – i.e. passing-off as one's own work (by copying or closely imitating) the words or creations of others; this includes (for example) copying and pasting content from the internet, **without** clearly acknowledging[6] the original author/creator
- piracy - the unauthorised reproduction or distribution of any 'content' (e.g. books, music, films, videos, games, photographs and images) which are protected by copyright

[2] Either explicitly labelled as such (e.g. by censorship, classification, parental guidance) or judged to be age-inappropriate through the application of common-sense.

[3] Defamation is the publication of material which adversely affects the reputation of a person or organization.

[4] 'Extremism' is defined as vocal or active opposition to the rule of law, individual liberty, mutual respect, and tolerance of different faiths and beliefs. Extremism includes calls for the death of members of our armed forces, at home or overseas.

[5] The sharing of sexually explicit images (e.g. naked 'selfies') through mobile phones, the internet or other digital media. In relation to images of people under the age of 18, this is a crime with potentially very serious consequences (Sexual Offences Act 2003)

[6] Citing a source (i.e. listing the name of the author, and where and when it was published) is strongly encouraged, not only because it avoids **plagiarism** but, if it is a relatively small extract of the source work, and if done in good faith for educational purposes, it will also significantly reduce or eliminate the risk of any claim for **copyright infringement**.

- hacking (deliberate unauthorised access to websites, devices, networks, systems or databases)
- taking photographs and making audio or video recordings of other people, and distributing such images or recordings, without first obtaining their permission
- unauthorised uploading, such as software licensed to the school, or data owned or protected by the school or by others
- use of peer-to-peer (P2P) sites or networks unless explicitly authorized by the ICT Coordinator

- activities that might:
  - waste staff effort or network resources
  - corrupt, delete, or destroy other users' data
  - violate the privacy or other rights of other users
  - disrupt the work of, or deny service to, other users

- activities that might affect the proper functioning of ICT resources such as:
  - disabling or overloading any computer system or network,
  - attempting to disable, defeat or circumvent any system intended to protect privacy, security, or intellectual property rights (e.g. copyright)
  - installing or connect any devices, software applications (including games) without authorisation
  - altering system settings, desktop wallpapers, icons etc. without authorisation
  - introduce viruses, worms, Trojan horses, trapdoors or similar programmes
  - interfering with power supply or data cabling