ICT Usage Policy (to be signed by pupil and/or parent)

Pembridge Hall School

Date of adoption of this policy	September 2021
Date of last review of this policy	September 2021
Date for next review of this policy	June 2022
Primary person responsible for this policy	Seema Manji [Head of Digital Learning] seema.manji@pembridgehall.co.uk

Circulation: This policy has been adopted by the governors and is available to parents on request. It is addressed to all members of staff and volunteers and applies wherever they are working with pupils.

'Parents' refers to parents, guardians and carers.

Contents

Appendices

1. 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 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 pupils within our care. This policy should therefore be read in conjunction with our other related policies, notably:

- Online safety
- Safeguarding and pupil protection
- Anti-Bullying
- Social Media
- Mobile Phones and Devices
- Photos and Images
- PSHEE and RSE

Bearing in mind the scope and content of our other related (above-mentioned) policies, the objectives of this[1] ICT Usage Policy are:

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

- to clarify the rules which pupils must follow

Our policies comply with *Keeping Pupils Safe in Education 2021* and are regularly reviewed and updated in consultation with a variety of resources, including:

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

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

[1] NB - Staff usage of ICT is governed by the Alpha Plus Group *ICT Acceptable Use Policy*, which is available under the ICT heading of the Alpha Plus Group section of the Portal.

resources for learning and development. Reinforcing the principle expressed in our Online Safety policy, we believe that the internet and the constantly evolving technologies and devices to which pupils have access can be tools that enrich their lives. We therefore teach them to view technology and new media positively whilst simultaneously protecting themselves. The education of pupils in regard to risks arising from ICT usage is incorporated into the curriculum, not only within ICT and PSHEE 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.

2. Expectations of pupils

All pupils are encouraged to use ICT resources to support their programmes of learning. Pupils 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.

Pupils 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 pupils, 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 pupil who knowingly abuses the privileges of ICT resources will face disciplinary procedures.

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 pupils of why things are prohibited
b) stay vigilant to the actual behaviour of pupils in their interaction with ICT

c) establish an environment where pupils 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, nor 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, and 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 resource (including email and internet browsing), nor 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 ICT Coordinator, in addition to any other reporting processes as required by other policies (Safeguarding, Anti-Bullying, Online Safety), for example to the Designated Safeguarding lead (DSL).

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.

PUPILS 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 IT**, 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 **ICT 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.

The name and email address of our ICT Coordinator is listed on the front cover of this policy.

b) Broader welfare issues of E-safety.
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 closely with the ICT Coordinator to ensure the security and effectiveness of the ICT controls. The DSL also works closely with the Local Safeguarding Children Partnership (LSCP) and other agencies where appropriate. The curriculum and pastoral aspects of educating pupils (and parents) on the risks of ICT usage, along with staff training, are explained in our *Online 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 ICT Coordinator and (if safeguarding issues are suspected) to the DSL.

Appendix 1

Acknowledgement of ICT Usage Policy
(to be signed by child and parent/guardian)

I have read and understood this ICT Usage policy, including the list of prohibited content and activities listed in Appendix 2. I agree to support the safe and responsible use of ICT.

Name of child: ……

Signature: ……..

Date: ……

Name of parent/guardian: …….

Signature: ……..

Date: ……

This data will be processed in line with Alpha Plus Group's *Privacy Notice*, which is available on request or can be accessed via the Group's public portal.

Appendix 2

List of prohibited content and activities

The ICT resources of the 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 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.

(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 pupils, 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)

[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 organisation.
[4] 'Extremism' is defined as vocal or active opposition to *fundamental British values*, including democracy, 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)

- 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
- 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 authorised 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

[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**.