Northcote Primary School
ICT Acceptable Use Policy Agreement
Staff and other Stakeholders

Review date: September 2024

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

All members of staff have a responsibility to use the school's computer systems in a professional, lawful, and ethical manner.

To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.
This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, digital cameras, email and social media sites.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, digital cameras, email and social media sites.

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

Equipment

All school laptops should be encrypted. Laptops should not be left unattended if taken out of school (e.g. Left in a car).

Photographs should be removed from Teacher IPads as soon as possible and stored on the server. Teachers should log out of the electronic register after completion.

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised

access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulation, May 2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy (see separate policy) and will always take into account parental consent.

- I will not connect any device (including USB flash drives) to the network that does not have up-to-date anti-virus software.

- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of students or staff and will not store any such images or videos at home.

- I will follow the school's policy on use of mobile phones / own devices at school.

- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use."

- I agree that my use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

- I understand that any hardware and software provided for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will always get permission before installing, attempting to install or storing programs of any type.

- I will only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate.

- I will always check files brought in on removable media (such as CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.

- Always check mobile equipment (e.g. laptops, tablet PCs, PDAs etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network.

- Images of children taken on cameras/school mobile phones/IPads should be removed and stored securely on the school server as soon as possible. **Photographs should not be stored on laptops.**

- Sensitive information should not be stored on the desk top of a laptop.

Security and Privacy

- I will ensure all documents, data etc., that are printed and contain confidential information are deleted/shredded after use.

- I will not allow unauthorised individuals to access e-mail / Internet / intranet / network or other school systems.

- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). I will protect the devices in my care from unapproved access or theft.

- I will respect copyright and intellectual property rights.

- I will keep my password to myself and never use someone else's logon name or password. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).

- I will always be wary about revealing my home address, telephone number, school name or picture on the Internet. • I know that other computer users should be respected and should not be harassed, harmed, offended or insulted.

- I will respect the security on the computers and not attempt to bypass or alter the settings.

- I understand that the Head Teacher has the right to review my files and communications to ensure that I am using the system responsibly.

Internet (*See the Online Safety & Social Media Policies*)

- I will access the Internet for school activities only.

- I have read and understood the school Online Safety guidelines which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of students within the classroom and other working spaces.

- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead as soon as possible. I will also report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator or the designated lead for filtering as soon as possible.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the Headteacher as soon as possible.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the Law.

- I understand that all Internet usage and network usage can be logged, and that this information can be made available to the Head Teacher on their request.

- I will not engage in any online activity that may compromise my professional responsibilities.

- I will not browse, download or send material that could be considered offensive to colleagues.

- I will report any accidental access to, or receipt of inappropriate materials, or any filtering breach or equipment failure to the Head Teacher.

- I will not download any software or resources from the Internet that can compromise the network or is not adequately licensed, or which might allow me to bypass filtering and security systems.

- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my school or professional role.

- I will ensure, where used, that I know how to use any social networking sites / tools securely, so as not to compromise my school or professional role.

- I will only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school into disrepute.

- I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Head Teacher.

- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

Email

- I will only use the school's approved systems to communicate with parents and will only do so for teaching and learning purposes.

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

- I will be polite and appreciate that other users might have different views from my own. The use of strong language, swearing or aggressive behaviour is not allowed.

- I will only open attachments to emails if they come from someone I know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.

- If I receive an email containing material of a violent, dangerous, racist or inappropriate content, I will always report this to the Head Teacher / Safeguarding Team.

- The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure.

- If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read the Acceptable Use Policy and understand my responsibility to comply with requirements set down within it.

I, Full name _____ **agree to the above.**

Relationship to School:

Signature:

Date:

Date Policy updated: *January 2023*
Date to be reviewed: *June 2024*
: