Staff Acceptable Use of ICT Policy

“Learning, Caring and Achieving Together”

Rationale

All members of staff have a responsibility to use the school’s computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign to say they have read and understood the contents of the Acceptable Use of Policy. Members of staff should also consult the school’s E-safety Policy, Computing Policy and Internet acceptable use Policy for further information and clarification.

Introduction

Farnborough Road Infant School is committed to protecting the privacy and security of the personal information it holds for staff, governors and volunteers. Please note our Privacy Statements.

To complement the data protection duties of the school there are duties shared by all staff, governors and volunteers because, as a professional organisation with responsibility for children’s safeguarding, it is essential that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This agreement covers all digital and physical data systems, e.g. Equipment (access devices) mobile phones, digital cameras, laptops, I-pads, email, social networking, the internet, intranet, network resources, learning platform, software, communications tools (online and offline) and paper records, whether printed or handwritten and however stored.

1. I understand that data held by the school may only be processed (acquired, processed, stored, deleted or transmitted) on the legal bases that the school has registered with the Information Commissioner’s Office.

2. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulation 2018. This means that all personal data will be 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 or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks) will be encrypted. Any images or videos of pupils will always take into account parental consent. I will ensure that data no longer needed will be effectively deleted or shredded.

3. 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 ie use a school ICT system for the purpose not permitted by it’s owner; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation. E.g. In the case of the caretaker, the taking of photographs in or around school may only be specifically for the purpose of premises/repairs & maintenance. This must be done so on the request of the Headteacher/ Deputy Headteacher or the Office Manager and must not include images of children or in the use of SIMS,Target Tracker or CPOMS staff should only use the level of access agreed by the Headteacher/ Deputy Headteacher or Office Manager to avoid information being used inappropriately.

4. Such misuse is also covered by the GDPR and any such misuse must be reported to the ICO, and to the data subjects (people) affected, within 72 hours.

5. I understand that laptops and I-pads may not be personalised in any way e.g personal photographs or I messages or social media apps. 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. School related emails must not be sent to personal email addresses eg. Governors should only receive school documents on a School Governor email address not on a personal email address.

6. I understand school l-pads may not be linked to personal SMART phones

7. 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 and not for private purposes or by anyone other than the member of staff the equipment is assigned to. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my device as appropriate. I will not, under any circumstance, use personal equipment to access personal, or sensitive data. Use of personal devices pose a high security risk if they are left vulnerable to theft, loss and unauthorised access.

8. All IT equipment must be kept on the school site unless specific permission is given from the Headteacher. In the event that permission is given all school equipment must be returned to school the following working day. Each laptop and Ipad is individually assigned to a classteacher and signed for to ensure any loss of equipment or data breach can be linked back to a particular device or member of staff.

9. I understand that when school IT equipment is not on the school site it is covered by staff’s personal insurance should it be lost, stolen or damaged in any way. Any school IT equipment must not be left unattended e.g. in a car

10. I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will use a ‘strong’ password and I will adopt school procedures for the safe storage of my passwords and for acquiring new ones. eg passwords must be kept in a secure APP or on Google Drive, passwords must be changed when deemed by the IT technician and Headteacher.

11. 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 use Google Drive to upload any personal/data sensitive documents and files so they are in a password protected environment. Memory sticks must not be used to store or carry personal/data sensitive documents and files. I will protect the devices in my care from unapproved access or theft. I will not share any files or folders on Google Drive with any other user. I will be mindful that when working in a public space that others may be able to see my laptop or tablet screen and will use my discretion as to whether information should be hidden from sight. I am aware that enabling Bluetooth connectivity on mobile devices can be a security threat and will switch this off when it is not needed for a specific connection.

12. I will ensure pseudonymisation by which the most identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms to ensure data cannot be put back together to identify the person or child.

13. I will respect copyright and intellectual property rights.

14. I have read and understood the school’s Data Security Policy and e-Safety Policy which cover the security of data and safe and appropriate access to data.

15. I will report all incidents of concern regarding children’s online safety to the Designated Child Safeguarding / PREVENT Lead Jennifer Taylor (Headteacher) and/or the Computing Lead Joanne Lea as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable/extreme websites to the Computing Lead and IT.Techncian.

16. I will not attempt to bypass or alter any filtering and/or security systems put in place by the school.

17. My 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. I will ensure that a BCC (Blind Carbon Copy) of any emails to parents/carers are sent to the Headteacher. All written notes will be copied onto CPOMS. Any pre-existing relationships which may compromise this will be discussed with the Headteacher or a member of the SLT
18. I will not install any software or hardware without permission of the network technician, Headteacher or office manager. This includes the downloading of free or paid apps. Apps will be removed if deemed unnecessary by the school.

19. I will ensure that I will not have any electronic communications with pupils including email and social networking as compatible with my professional role.

20. I will refrain from using any form of social media to discuss any aspect of school life except purely social events that involve colleagues. I will follow any guidance issued when contributing to the use of social media by the school as an official communication channel.

21. My use of ICT and information systems and my written communication 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 or postal addresses. My use of ICT and other forms of communication will not interfere with my work duties and will be in accordance with the school AUP and the Law.

22. I will not create, transmit, display, write, 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 or the school into disrepute.

23. I will promote E-safety and E-privacy with 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. Similarly, I will promote care for others in the pupils’ writing and any other content that they create.

24. I understand that my use of the information systems, Internet and email may be monitored and recorded by the IT technician under the instruction of the Headteacher to ensure policy compliance.

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 and the School’s Data Security 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.

Updated April 2018
This policy will be reviewed regularly.

Signed _________________________ Date ____________ Headteacher

Signed _________________________ Date ____________ Chair of Governors