Fritchley CE (Aided) Primary School

Staff and Governor Acceptable Use Policy

Computers, laptops, iPads and other networked resources, including Internet access, are available to all staff in the school. These resources are intended for educational purposes, and may only be used for legal activities consistent with the rules and policies of the school. It is expected that staff will use online equipment as appropriate and that they will provide guidance and instruction to pupils in the use of the technology. The devices are provided and maintained for the benefit of all staff and children, who are encouraged to use the online resources available to them. Access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

School Owned Online Devices at Home or School

- Do not install, attempt to install, or store apps, device drivers or software of any type (including screen savers and custom mice) on any device without permission from the computing co-ordinator or assistant headteacher.
- Do not damage, disable or otherwise harm the operation of any device or intentionally waste resources.
- Do not use online equipment for commercial purposes, e.g. buying or selling goods unless agreed with the headteacher for school funds. For example, selling old text books.
- Do not open files brought in on removable media (such as CDs, memory sticks etc.) until they have been checked with antivirus software and been found to be clean of viruses.
- Do not connect online equipment to the network until it has been checked with antivirus software and been found to be clean of viruses.
- Access to the school shared network and its resources will only be via laptops that have been given consent by the school. For example, the personal computer of a student teacher may be granted access if appropriate.
- No settings must be changed on your laptop unless authorised by the computing co-ordinator or assistant headteacher; this includes Internet settings, browsers and system preferences.
- You are continually responsible for the laptop issued. Any damage must be reported to the computing co-ordinator or assistant headteacher immediately.
- You must not allow any external agency or support service to access or tamper with school laptops, hardware or software.
- Appropriate and safe care and storage of school devices is expected at home.
- Do not access any other non-internet network from any school device.
- Laptops must be connected to the network at least once per week to allow updates to occur.

Security & Privacy

- Networked storage areas and other external storage hardware (memory sticks, external hard drives) which are distributed by the school are the property of the school and the responsibility of the staff.
- Staff must not retain data of a personal nature for a child on any other source than the encrypted memory stick provided or server.
- Files and communications may be reviewed by SLT or governors to ensure that users are using the system responsibly.
- Do not disclose your password to others or use passwords intended for the use of others.
- Never tell anyone you meet online personal information in relation to your occupation or link with the school.
- Do not use online equipment in a way that harasses, harms, offends or insults others.
- Respect and do not attempt to bypass security in place on school devices or attempt to alter the settings.
- Do not intentionally allow unauthorised access to data and resources on the school network system or other systems.

- Do not intentionally use the computers to cause corruption or destruction of other users' data, or violate the privacy of other users.
- Do not remain logged in to systems which are confidential in nature nor allow the browser to retain your username and password. For example, Integris or email. The is especially relevant if accessing from a mobile phone or shared device.

Child Log Ons

- When using web based services e.g. Times Tables Rockstars, make sure the children understand that they must keep their username and password private.
- Do not allow children to share their log on nor allow a child to use another's account.
- Ensure the usernames and passwords of children are stored securely.
- Do not allow children to share personal information without the prior written consent of the parent.

Internet (please also refer to the school online safety policy)

- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials, which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- You should not post any online comments that purport to represent the school unless authorised by the headteacher.

Personal Social Networking

- Do not make any contact through personal social media to any pupil or parent; future, present or prior without full disclosure to the headteacher.
- Do not be 'friends' with parents, family members or carers of children; future, present or prior
- If you have an online relationship with a parent/carer prior to them joining the school, this should be disclosed to the senior leadership team as soon as possible. E.g. friends on Facebook.
- Ensure your own personal social media accounts have the highest levels of privacy.

Online Communication

Email

Your school e-mail account will be your principal point of contact for all electronic communication.

- Refrain from using use strong language, swearing or aggressive behaviour.
- Never open attachments to emails unless they come from someone you already know and trust. (They could contain viruses or other programs that would destroy all the information and software on your computer).
- The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. (All such messages must be reported immediately to a member of the leadership team)
- School email must only be used for school communication therefore should not be used for personal correspondence.
- Communication with a parent via email must be consented by the parent. Do not access the email from Integris and communicate without prior consent.

Class Dojo

- Ensure content posted on Class Dojo is professional in nature.
- Use Class Dojo to share daily events and learning.
- Abide by safeguarding protocol specifically children whose photos may not be shared.

Posting on the school website

- Posts to be completed by Mrs Shaw and/or Ms Baker.
- Remain professional in nature.
- Do not share the names or ages of the children.
- If an error occurs, contact Mrs Shaw immediately.
- Abide by safeguarding protocol specifically children whose photos may not be shared.

Services

Fritchley Primary and Nursery School will endeavour to alert staff of any network related issues that may affect the use of IT within the school network. There are no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any loss of data as a result of service interruptions from external systems and providers including the internet service providers, server malfunctions or delay and non-delivery of devices and or software. Use of any information obtained via the network is at your own risk.

Review

This Staff Acceptable Use Policy will be reviewed by the Computing curriculum leader and the senior management team.

Reviewed: 10th March 2021

By: Esther Devonport.

Date for next review of this document January 2023 unless significant changes require an earlier update.