STEEL RIVER
ACADEMY TRUST

Staff & Governor Acceptable Use Policy

Review Date	Sept 2023
Review Frequency	Annually
Date for Next Review	Sept 2024
Author	S Marsden

Whale Hill Primary School – Acceptable Use Policy (AUP) for staff, governors and visitors

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.

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs Marsden or Mr Frost (Designated Safeguarding Lead and Online Safety Lead)

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, iPads, digital cameras, smart watches, email, learning platforms, cloud computing services such as Office 365 and social media sites**.**

- School owned information systems must be used appropriately for professional use. 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.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body/Trustees.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities. 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 give out my own personal details, such as mobile phone number, personal email address or any social media link, to pupils

- I will only use the approved, secure email system(s) for any school business

- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act (GDPR 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.

- I will not store any personal information on the school computer system or Cloud Services such as Windows 365 that is unrelated to school activities, such as personal photographs, files or financial information.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- 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 ICT Support Provider (OneIT) as soon as possible.

- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead/Online Safety Lead (Mrs Marsden or Mr Frost) or a Deputy Designated Safeguarding Lead in their absence, as soon as possible, logging the incident on CPOMS as per school safeguarding procedure. I will also report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites.

- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member

- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head Teacher.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head Teacher.

- When using my own device to access school e-mails, I will not use open guest wireless channels.

- If using my own device to access work e-mails, all data will be completely erased before disposing of it. I am aware that simply deleting files will not physically remove data.

- I must not store any school information on my personal devices, or on cloud servers linked to my mobile devices.

- I must take all sensible measures to prevent unauthorised access to my mobile devices, including (but not limited to) the use of a PIN, pattern or password to be entered to unlock the device, and ensuring that the device auto-locks if inactive for a period of time.

- I must report any loss or theft of my mobile device to the school's DPO (Data Protection Officer) immediately.

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

- I will respect copyright and intellectual property rights.

- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

- I will not use personal electronic devices (including smart watches) in public areas of the school unless children aren't present, between the hours of 8.35am and 3.00pm, except in the staff room during a designated break time.

- 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 Online Safety Lead (Mr Frost) or the Head Teacher.

- I understand this forms part of the terms and conditions set out in my contract of employment

Where the school 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.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.
Signature …….…… Date ……
Full Name and Job Title ……..... (printed)