Staff ICT Acceptable Use Policy

This policy was originally based on guidance from Kent, and we would like to acknowledge their work.

Guidance for Use

Schools increasingly need to ensure that all staff are aware of a common set of rules for the safe use of computing technology. This is to protect pupils, staff and the reputation of the school. This is a document which will continue to undergo modification as both technology and the law relating to technology develop further. This policy links to the schools wider safeguarding systems.

Our Acceptable Use Policy (AUP) provides a structure which is appropriate to the school e-Safety ethos and approach. This document links to our Online Safety Policy. It should be read in conjunction with our Code of Conduct which applies to all members of staff working within school. Those staff working for Durham County Council are bound by the DCC Code of Conduct.

Our school has a duty of care to safeguard and protect staff under the Health and Safety at Work Act 1974 and the Management of Health and Safety at Work Regulations 1999. Key legislation also includes Section 11 of the Children Act 2004 which places a duty on key persons and bodies to ensure that their functions are discharged having regard to the need to safeguard and promote the welfare of children. Information regarding statutory requirements from the DfE is provided in their document Keeping Children safe in Education.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1021914/KCSIE_2021_September_guidance.pdf

Further information is provided in the document “Guidance for Safer Working Practice for Adults who Work with Children and Young People” (2015), which contains useful guidance around professional use of technology. http://www.safeguardinginschools.co.uk/wp-content/uploads/2015/10/Guidance-for-Safer-Working-Practices-2015-final1.pdf

Staff Acceptable Usage Policy: Statement of Intent

Our Staff AUP is not intended to unduly limit the ways in which members of staff teach or use computing but aims to ensure that the school and all members of staff comply with the appropriate legal responsibilities, the reputation of the school is maintained, and the safety of all users is ensured. Members of staff are entitled to seek their own legal advice on this matter before signing the AUP.

In order to protect staff members, it is essential to have an AUP in place which has been viewed and understood. All employees (including teaching and non-teaching staff) must be aware of the school rules for use of information systems and professional conduct online whether on or off site. Misuse of computing systems and other professional misconduct rules for employees are specific and instances resulting in disciplinary procedures or staff dismissal have occurred.

With internet use becoming more prominent in everyday life for personal and professional use, it is important that all members of staff are made aware that their online conduct both in and out of school could have an impact on their role and reputation. Civil, legal or disciplinary action could be taken should they be found to have brought the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities. It is therefore important that the AUP is firmly embedded within the school induction process for all members of staff (including any volunteers, part-time staff or work experience placements). It is also important that all members of staff receive up-to-date and relevant training around this issue on a regular basis. All members of staff should read, understand and sign the AUP before being granted access to any of the schools' systems.

Staff are reminded that there are bound by our Code of Conduct which is reviewed annually and which they must sign. They must only contact families and pupils using the school email address or the school learning platform so it can be monitored and traced in the case of an allegation or concern. However, schools must recognise that in some cases there may be pre-existing relationships which mean that any "ban" from adding pupils or parents as friends or contacts on personal social networking sites may be difficult to enforce. It is therefore recommended that members of staff should make SLT aware of these exceptions in order to protect themselves from allegations or misinterpreted situations. It is crucial that all members of staff are aware of the boundaries and professional practices online in order to protect their professional status. Staff should be advised to check their privacy settings on any personal social media sites they use, however they should always remember that once content is shared online it is possible for it be circulated more widely than intended without consent or knowledge (even if content is though to have been deleted or privately shared).

Schools should also be aware of statutory guidance in the DfE Document "Keeping children safe in Education" which states that the staff behaviour policy or code of conduct should include "*staff/pupil relationships and communications including the use of social media*".

Further Information and Useful Links

- "Cyberbullying: Advice for headteachers and school staff" from the DfE provides advice and is available on the DfE website.
- "Supporting School Staff" is an essential document to help staff understand how to protect themselves online created by Childnet International and DfE: http://www.digizen.org/resources/school-staff.aspx
- "Social networking guide for teachers" is available on the Childnet website, it is aimed at NQT's but provides useful information to all staff.,
- The UK Safer Internet Centre's Professional Online Safety Helpline offers advice and guidance around e-Safety for professionals who work with children and young people in the UK. The helpline provides support with all aspects of digital and online issues such as social networking sites, cyber-bullying, sexting, online gaming and child protection online. Staff can contact the helpline via 0844 381 4772, helpline@saferinternet.org.uk or can visit www.saferinternet.org.uk/helpline for more information.
- 360 Degree Safe tool is an online audit tool for schools to review current practice: http://360safe.org.uk

Staff Acceptable Usage Agreement

As a professional organisation with responsibility for children's safeguarding it is important that all of our 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 system 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.

1) 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, PDAs, digital cameras, email and social media sites**.** This policy covers both school and personally owned devices.
2) The school allow staff to keep mobile phones in their possession and understand that modern

smart phones have multiple uses, which may have a positive role in school. However, staff should ensure that any personal use of phones happens only at break times out of view of pupils. In particular, staff must ensure that electronic equipment is not used when supervising equipment as this may hinder vigilance and the safety of pupils.

3) Cameras on personal phones will not be used to take pictures of children unless in exceptional circumstances where agreed from the Head Teacher has been obtained.
4) A school device is available for trips and visits which staff can collect from the office. If using their own phone to make such calls, steps should be taken (prefix 141) to protect the member of staff's identity.
5) 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.
6) 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.
7) 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 not use the same password for all sites.
8) I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
9) I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. 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 or CDs) will be encrypted by a method approved by the school. Secure means of transporting data are either an encrypted memory stick or use of the school learning platform. Any images or videos of pupils will only be transported by secure media and will always take into account parental consent.
10) 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), unless they are secured and encrypted. Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.
11) I will respect copyright, copyright of design and intellectual property rights.
12) I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
13) I will report all incidents of concern regarding children's online safety to the Head Teacher (Miss Natalie Ward) and/or to one of our other Designated Safeguarding Leads (Mrs Margaret Sleeman or Mrs Anna-Lise Lennox) and our e-Safety Coordinator (Mrs Victoria Nower) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Miss Victoria Nower, the e-Safety Coordinator and designated lead for filtering, as soon as possible.
14) 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 Team via Julieann Sludden (Office Manager) as soon as possible.
15) I will use my school provided email for all work-related communication to ensure protection from

viral infection and to comply with data protection procedure.

16) 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.
17) 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 our school AUP, our Code of Conduct and the Law.
18) 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, or the County Council, into disrepute.
19) I will promote e-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.
20) 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 e-Safety Coordinator (Mrs Victoria Nower) or the Head Teacher (Miss Natalie Ward).
21) I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

At Finchale Primary, we exercise our 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 we believe unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, we will invoke our disciplinary procedure. If we suspect 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: January 2025