Staindrop Church of England Primary School

Staff ICT Acceptable Use Policy September 202526

Our vision is founded on St Luke's Parable of the Sower. We are the rich soil that enables our children to develop deep roots and flourish. We aim to ensure that everyone grows to fulfil their potential. Our school provides an environment rooted in Christian values where learning, laughter and friendship are at the heart of everything we do.
Through God's love, we are the rich soil where roots grow and seeds flourish. Luke 8:4-15

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 needs to link to the schools wider safeguarding systems.

This template Acceptable Use Policy (AUP) provides a structure which is appropriate to the school e-Safety ethos and approach. The AUP will need to be adapted by the school for a variety of different audiences and for their individual requirements and systems. It should be developed by a member of SLT and must be approved by the Head Teacher and Governing Body. It is recommended that staff should be actively involved in writing the AUP to ensure it is appropriate for the establishment and the requirements at the material time.

This document should link to the schools "Online Safety Policy"

Schools may wish to read relevant legislation and information regarding this document and amend the school's AUP accordingly. Schools have 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. Schools may also wish to read and consider 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

In addition schools should be aware of the statutory requirements in the DfE document "Keeping Children safe in Education 2025 26.

https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Schools should also be aware that they need a Data Protection Policy and procedures and that the statements made in this document should reflect that policy.

Further Information

- "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 ECTs 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 ICT Acceptable Use Policy 2025

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 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, tablets, digital cameras, email and social media sites**.**

2) 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.

3) Mobile Phones.

   - Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as relevant policy and procedures, such as: child protection, data security and acceptable use.
   - Staff will be advised to:
     - Keep mobile phones and personal devices in a safe and secure place during lesson time.
     - Keep mobile phones and personal devices on 'silent' mode during lesson times.
     - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
     - Not use personal devices during teaching periods, unless written permission has been given by the headteacher such as in emergency circumstances.
     - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

   a) School devices should only be used to take pictures of children.

   b) In the unlikely event of needing to contact a parent directly a school mobile phone will be issued to the member of staff concerned.

4) I understand that any hardware and software provided by my school for staff use can only be used by members of staff.

5) Personal use of school ICT systems and connectivity is only permitted with the consent of the headteacher,

6) 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).

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

9) Data Protection – See data protection policy

a) 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 personal 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 encrypted laptop / encrypted USB memory / encrypted HDD / approved cloud based system }

b) If I choose to use a portable device (Phone, Tablet etc…) to collect my work e-mail I will ensure that the device is locked by a pin code or password and will be wiped when I dispose of the device.

c) I will not transfer sensitive personal information from my school e-mail account (e.g. Safeguarding Reports, Medical Information) UNLESS the information is encrypted.

d) I will not keep professional documents which contain school-related personal information (including images, files, videos etc.) on any personally owned devices (such as laptops, digital cameras, mobile phones)

e) Digital Images or videos of pupils will {Not be taken away from the school premises OR Only taken from the school premises using encrypted memory OR alternative secure transport method}

f) I will not use unapproved cloud storage systems (Dropbox, icloud etc) for storing personal data of staff or pupils.

10) 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.

11) I will respect copyright and intellectual property rights.

12) Social Media.

a) 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.

b) I will not communicate with pupils or ex-pupils under the age of 18 using social media without the express permission of the Headteacher.

c) 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. *This would include any relatives of current pupils that are my "friends" on a social media site.*

d) 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 school AUP and the Law.

e) 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. This would include any comment made, even in the belief that it is private on social media.

13) I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator/ e-Safety Coordinator (Mr Whelerton or Mrs Harland) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (Mr Whelerton) the e-Safety Coordinator 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 Provider/Team as soon as possible.

15) 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.

16) 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.

17) I understand that my use of the information systems, Internet and email may be monitored and recorded 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.