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

Staff ICT Acceptable Use Policy Template 2025

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 and mobile 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 and should be read in conjunction with the Safeguarding/child protection, KCSIE 2025, online safety, staff code of conduct and confidential reporting code (whistle-blowing) policies.

This template Acceptable Use Policy (AUP) provides a structure which is appropriate to the school online 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.

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.

All staff need to have read and understood **at least** part 1 of Keeping Children safe in Education Sept. 2025. DSLs, governors/trustees and senior leaders need to familiar with all sections.

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.

A Staff AUP is not intended to unduly limit the ways in which members of staff teach or use technology, 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.

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 and other related policies before being granted access to any of the school systems.

Some settings may wish to provide more explicit guidance for staff around use of social networking and email as, even when use of social media sites occur in their own time using their own computer, it can leave staff vulnerable to abuse or a blurring of professional boundaries. Schools must be aware they cannot ban staff from using sites in their own personal time; however, they can put in place appropriate guidance and boundaries around staff interaction with pupils (past or present) and parents. It is recommended that any contact with pupils and parents only takes place via school approved communication channels e.g. 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 are encouraged to 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 made 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 thought to have been deleted or privately shared).

Settings may also wish to consider adding a statement regarding their policy on staff using school equipment for personal use. Occasional personal use of the school’s computers can be beneficial to the development of staff IT skills and to enable staff to maintain a positive work-life balance. However, this is at the school’s discretion and can be revoked at any time. Any online behaviour and activity by a member of staff whilst using the school systems must be in accordance of the school AUP and any policies relating to staff conduct and personal use must not interfere with the member of staff’s duties or be for commercial purpose or gain (unless authorised by the SLT).

Elements in the AUP template highlighted in yellow will require modification to suit the needs to the school, and the policies agreed by SMT and governors

It is suggested that schools do not make changes to any elements typed in red as these are linked to fundamental safeguarding or data protection issues.

The Staff AUP should be reviewed regularly (at least annually) and should be revisited and updated in response to any changes, for example after an incident, introduction of new technologies or after any significant changes to the school organisation or technical infrastructure. Any amendments to the AUP should then be communicated to all staff.

This template has been produced by schools, child protection officers, multi-agency children’s workforce professionals and Kent Police to help schools write their own AUP. The AUP template suggests a range of statements and should be used to develop the schools e-Safety ethos and whole-school approach. This AUP template is suitable for all schools and other educational settings (such as Pupil Referral Units, 14-19 settings and Hospital Schools etc) and we encourage establishments to ensure that their AUP is fit for purpose and individualised for their context. For simplicity we have used the terms ‘school’ and ‘pupils’, but wider educational settings are equally relevant.

Schools will want to ensure that measures they expect staff to take to protect data are clearly indicated in the policy and are in line with GDPR legislation.

Further Information

- “Social networking guide for teachers” is available on the Childnet website, it is aimed at ECTs but provides useful information to all staff Teachers & professionals | Childnet

- 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 - both the school systems and personal mobile technology and social media use, 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, smartwatches and other mobile and smart technology 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 and Smart technology (including mobile phones, smartwatches, tablets etc)

   a) Staff mobile phones will be stored in staffroom lockers during the school day and may only be used in the staffroom or office.

   b) Staff mobile phones will never be used for any reason when children are present.

   c) Staff mobile phones are allowed in school, but are not allowed to be used in sensitive areas (EYFS, cloak rooms, toilets, when children are changing, swimming). Mobile phones should only be used for communication when not working with children. Mobile phones should not be visible to pupils unless their use is linked to learning, for instance as a stopwatch or to play music.

   d) Smart watches are not to be used for any reason when children are present.

   e) Cameras on personal devices will not be used to take pictures of children in any circumstances.

   f) 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 {and can only be used for school related work}

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 10 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 also the school Data Protection Policy}*

a) I will ensure that any personal data is kept in accordance with the General Data Protection Regulations. 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 or accessed remotely. Any personal data on portable devices (USB, laptops, tablets etc) {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. EHCP's 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 Online 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 using social media without the express permission of the Headteacher. *{Some schools may use social media to communicate directly with pupils, in this instance staff should use a social media account that is purely used for work purposes. They should complete a risk assessment to ensure that both staff and pupils are protected.}*

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 Safeguarding lead (DSL) (Dawn Dunn, Lynsey Johnson Acting HT) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the designated lead (or NCDAT) for filtering as soon as possible KCSIE 2025 Paragraph 134 – 148 is useful to update knowledge of staff.

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 (NCDAT) as soon as possible.

15) I will promote Online Safety with the pupils in my care and in line with the school policy and curriculum.

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 DSL (Dawn Dunn or Lynsey Johnson Acting HT) or their deputy.

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.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: ……..…….... Print Name: …… Date: ……..…

Accepted by: …… Print Name: ……..