



Staff ICT Acceptable Use Policy Template 2012

Guidance for Use

Senior Leadership Teams (SLT) will be encouraging and supporting the positive use of Information and Communication Technology (ICT) to develop curriculum and learning opportunities in schools and settings. Nevertheless it is essential that the use of ICT and online tools is carefully managed to ensure that all members of the school community are kept safe as well as their data and that risks or dangers are recognised and mitigated.

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.

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" (2009), which contains useful guidance around professional use of technology.

www.childrenengland.org.uk/upload/Guidance%20.pdf

Schools must also ensure they comply with the Data Protection Act (DPA) 1998. Under the DPA every organisation that processes personal information (personal data) must notify (register with) the Information Commissioner's Office, unless they are exempt. Specific guidance for education establishments, including information on how to register and check notification may be found here:

http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx

The DPA applies to anyone who handles or has access to information concerning individuals and everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. Schools should have a Data Protection and Security Policy in place to outline the legal responsibilities and actions taken to protect personal data in accordance with the DPA. This may include password safety, use of encryption, use of laptops, email and portable data storage devices (e.g. memory sticks) not sharing login information etc. KCC Data Protection information may be seen at: www.kenttrustweb.org.uk/Policy/dpfoi_data.cfm and schools can read more information from the Information Commissioner's Office:

<http://www.ico.gov.uk/>

A Staff AUP is not intended to unduly limit the ways in which members of staff teach or use ICT, 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 ICT systems and other professional misconduct rules for employees (whether from Kent County Council or other professional bodies) are specific and instances resulting in disciplinary procedures or staff dismissal have occurred.

With internet use becoming more prominent in every day 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' ICT 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 such as Facebook and Twitter 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 red in are areas where schools may wish to personalise the template by referencing their own specific policies and procedures such as Data Security, Photo and Image use, e-Safety, Behaviour and Safeguarding. Schools may also consider providing staff with a written process or chart to follow for reporting any incidents or concerns to ensure that all members of staff are aware of and understand the school's specific safeguarding procedures. Where the school outsources any ICT services it is essential that an AUP is created as part of the service level agreement and is owned and enforced by both the managed service and the school.

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.

This document has been viewed by representatives in the South East for the Teaching Unions. It has been approved by Kent County Council Legal Services, Schools Personnel Service and the Children's Safeguards Team.

If schools or settings wish to discuss the use and application of Acceptable Use Policies or any other e-Safety concerns, please contact the Kent County Council e-Safety Officer: esafetyofficer@kent.gov.uk 01622 221469 www.kenttrustweb.org.uk?esafety

Further Information

- Kent Schools and settings can consult with the e-Safety Officer via: esafetyofficer@kent.gov.uk or 01622 221469. Training is available via CPD Online <http://cpdschools.kenttrustweb.org.uk> and KSCB www.kscb.org.uk
- “Safer Use of New Technology” is a Kent Safeguarding Children Board (KSCB) document which discusses ideas and FAQs for professionals on how to use technology safely when working with young people. The document can be downloaded from www.kenttrustweb.org.uk?esafety
- “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>
- Teach Today is a useful website which provides useful advice and guidance for staff from industry: <http://en.teachtoday.eu>
- 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/>
- “Guidance for Safer Working Practice for Adults who Work with Children and Young People” (2009) contains useful guidance around professional use of technology. www.childrenengland.org.uk/upload/Guidance%20.pdf

Staff ICT Acceptable Use Policy 2012

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.

- 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.
- 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.
- 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.
- 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 attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- 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. (Schools might wish to attach their Data Security Policy). Any images or videos of pupils will only be used as stated in the school image use policy (schools may wish to attach a copy of the image use policy) and will always take into account parental consent.
- 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 (if appropriate). I will protect the devices in my care from unapproved access or theft.
- 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.
- I will respect copyright and intellectual property rights.

- 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 (**Schools might wish to attach a copy of the e-Safety policy or include specific expectations**).
- I will report all incidents of concern regarding children’s online safety to the Designated Child Protection Coordinator (**name**) and/or the e-Safety Coordinator (**name**) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (**name**) the e-Safety Coordinator or (**name**) the designated lead for filtering as soon as possible. (**Schools may wish to attach a reporting flowchart**)
- 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 (**named contact**) as soon as possible. (**Schools may wish to provide more specific details about accessing technical help here**).
- 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.
- 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.
- 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.
- 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.
- 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 (**name**) or the Head Teacher.
- 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: