ACCEPTABLE USE OF ICT AND MOBILE PHONES POLICY

Including POLICY ON THE USE OF SOCIAL NETWORKING SITES

Plan Owner / Author:	Sarah Wood
Date of Implementation:	September 2019
Review Date	September 2025
Version Number:	2

Document Change History

Version	Author	Date	Change Details
2	SW	September 2023	Reviewed inline with KCSIE 2023

ACCEPTABLE USE OF ICT AND MOBILE PHONES POLICY

1. Purpose

1.1 The policy defines and describes the acceptable use of ICT (Information and Communications Technology) and mobile phones for school-based employees. Its purpose is to minimise the risk to pupils of inappropriate contact from staff, to protect employees and schools from litigation and to minimise the risk to ICT systems.

2. Scope

2.1 This policy deals with the use of ICT facilities in schools in Suffolk and applies to all school-based employees and other authorised users eg volunteers. Non school-based staff are subject to the County Council's ICT Acceptable Use Policy.

3. School Responsibilities

3.1 The Governing Body is responsible for ensuring that its employees act in a lawful manner, making appropriate use of school technologies for approved purposes only.

3.2 The Governing Body is responsible for adopting relevant policies and the Headteacher for ensuring that staff are aware of their contents.

3.3 The Headteacher is responsible for maintaining an inventory of ICT equipment and a list of school laptops and mobile phones and to whom they have been issued.

3.4 Equipment disposal will be managed in accordance with the *Waste Electrical & Electronic Equipment Directive (WEEE)*. Mobile Media (e.g. CD ROMS, DVDs) should be disposed of by way of shredding.

3.5 If the Headteacher has reason to believe that any ICT equipment has been misused she should consult HR for advice without delay. HR will agree with the Headteacher and CSD's Policy and Compliance Manager an appropriate strategy for the investigation of the allegations. Incidents will be investigated in a timely manner in accordance with agreed procedures.

3.6 Headteachers should make it clear that internal school staff should not carry out any investigations unless they are both qualified and authorised to do so.

4. User Responsibilities

4.1 Staff found to be in breach of this policy may be disciplined in accordance with the disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in termination of employment. Users must report all suspected breaches of this policy to the Headteacher.

4.2 Users and their managers are responsible for ensuring that adequate induction, training and support is undertaken to implement this policy.

4.3 By logging on to ICT systems, users agree to abide by this Acceptable Use Policy and other policies that relate to the use of ICT.

4.4 All users are expected to act in a responsible, ethical and lawful manner with the understanding that school electronic and manual information may be accessible to the public under the Freedom of Information Act 2000. Users should uphold privacy and confidentiality in accordance with the Data Protection Act 1998. Care must also be taken not to breach another person's copyright, trademark or design, nor to publish any defamatory content.

4.5 Staff who have been given the use of a school laptop will be expected to sign for its use on receipt. Staff may use school equipment for authorised business use only, except as allowed for in paragraph 5.1

4.6 Staff must follow authorised procedures when relocating ICT equipment or taking mobile devices offsite.

4.7 No one may use ICT resources in violation of license agreements, copyrights, contracts or national laws, or the standing orders, policies, rules or regulations of the school or the County Council.

4.8 Users are required to protect their password and not share their account details with others for their use, nor utilise another users' account or misrepresent their identity for any reason. Users must not under any circumstances reveal their password to anyone else.

4.9 No user shall access (eg read, write, modify, delete, copy move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law.

4.10 Users must not load or download software on any device without the authorisation of the Headteacher. Periodic audits of software held on ICT equipment will be undertaken.

4.11 Users must take care to store sensitive information eg pupil data safely and to keep it password protected, on all school systems, including laptops.

4.12 Network connected devices must have school approved anti-virus software installed and activated. Users may not turn off anti-virus software. All users of ICT resources have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. No one may knowingly create, install, run or distribute any malicious code (eg viruses, Trojans, worms) or another destructive program on any ICT resource.

4.13 No one may knowingly or willingly interfere with the security mechanisms or integrity of ICT resources. No one may use ICT resources to attempt unauthorised use, or interfere with the legitimate use by authorised users, of other computers on internal or external networks. Access to networks will be monitored.

4.14 Within the terms of the Data Protection Act 1998, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the County Council or school may record or inspect any information transmitted through or stored in its computers, including email communications and individual login sessions, without notice when:

- There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy
- An account appears to be engaged in unusual or unusually excessive activity
- It is necessary to do so to protect the integrity, security, or functionality of ICT resources or to protect the County Council or its partners from liability
- Establishing the existence of facts relevant to the business

- Ascertaining or demonstrating standards which ought to be achieved by those using the ICT facilities
- Preventing or detecting crime
- Investigating or detecting unauthorised use of ICT facilities
- Ensuring effective operation of ICT facilities
- Determining if communications are relevant to the business (for example, in the last resort where an employee is off sick or on holiday and business continuity is threatened)
- It is otherwise permitted or required by law

4.15 Do not send private, sensitive or confidential information by unencrypted email – particularly to an external recipient – if accidental disclosure could lead to significant harm or embarrassment. Anonymise personal data where possible eg by using initials. Use passwords on sensitive documents that must be sent to external recipients.

4.16 Websites should not be created on school equipment without the written permission of the Headteacher.

4.17 No one may use ICT resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law. No one may abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a school account.

4.18 The following content should not be created or accessed on ICT equipment at any time:

- Pornography and "top-shelf" adult content
- Material that gratuitously displays images of violence, injury or death
- Material that is likely to lead to the harassment of others
- Material that promotes intolerance and discrimination on grounds of race, sex, disability, sexual orientation, religion or age
- Material relating to criminal activity, for example buying and selling illegal drugs
- Material relating to any other unlawful activity eg breach of copyright
- Material that may generate security risks and encourage computer misuse

4.19 It is possible to access or be directed to unacceptable Internet sites by accident. These can be embarrassing and such sites can be difficult to get out of. If staff have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the Headteacher. This may avoid problems later should monitoring systems be alerted to the content.

5. Personal Use & Privacy

5.1 In the course of normal operations, ICT resources are to be used for business purposes only. The school permits limited personal use of ICT facilities by authorised users subject to the following limitations.

5.2 Personal use must be in the user's own time and must not impact upon work efficiency or costs. The level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided.

5.3 Personal use must not be of a commercial or profit-making nature.
Personal use must not be of a nature that competes with the business of the school or conflicts with an employee's obligations.

5.4 Personal use of the Internet must not involve attempting to access the categories of content described in section 4.18 that is normally automatically blocked by web filtering software.

5.5 The school restricts and monitors access to social networking websites from its computers at all times. Access will only be allowed where use of such websites is for school purposes. (See Appendix 1 - Policy on the Use of Social Networking Sites).

6. Mobile Phone Communication and Instant Messaging

6.1 Staff are advised not to give their home telephone number or their mobile phone number to pupils. Mobile phone communication should be used sparingly and only when deemed necessary.

6.2 Photographs and videos of pupils should not be taken with mobile phones.

6.3 Staff are advised not to make use of pupils' mobile phone numbers either to make or receive phone calls or to send to or receive from pupils text messages other than for approved school business.

6.4 Staff should only communicate electronically with pupils from school accounts on approved school business, eg coursework.

6.5 Staff should not enter into instant messaging communications with pupils.

POLICY ON THE USE OF SOCIAL NETWORKING SITES

1. General

This policy on social networking websites is in addition to the school's existing Acceptable Use of ICT policy. It takes account of the ACAS guidance on Social Networking.

In this policy 'staff' means employees, volunteers (including governors), agency staff or anyone working within the school and using the school's IT equipment.

In addition, the 'Nolan Principles' apply to all staff and will sit alongside this policy.

The revised core standards for teachers (implemented September 2012), regarding expected behaviour in and outside of school, apply to this policy. The school expects all staff to abide by these standards.

As staff are aware, the internet is provided (primarily) for school use. We recognise however, that many employees may rarely use the internet for personal purposes while in school. We also recognise that many employees participate in social networking on websites such as Facebook, Twitter, MySpace, Bebo and Friendster outside of work.

The purpose of this policy is to outline the responsibilities of staff using the internet to access social networking websites.

This policy applies to all staff using the school's IT equipment.

2. Personal Use of the Internet

The school restricts and monitors access to social networking websites from its computers at all times. Access will only be allowed where use of such websites is for school purposes.

3. Personal Conduct

The school respects staff's right to a private life. However, the school must also ensure that confidentiality, its pupils, employees, volunteers, and its reputation are protected. It therefore requires staff using social networking websites to:

- use caution when posting information on social networking sites and blogs
- refrain from identifying themselves as working for the school
- ensure that they do not conduct themselves in a way that is detrimental to the school
- take care not to allow their interaction on these websites to damage working relationships between members of staff, pupils at the school and their families, and other stakeholders or working partners of the school.

If staff become aware of inappropriate material/comments they should notify the Headteacher as soon as possible, and if possible provide print outs of the comments made or of the pictures displayed.

Staff must not be 'friends' or communicate with students on any social network sites or similar websites, including, but not limited to, 'Facebook', 'MySpace', 'Twitter' etc. If any student makes contact with any staff member, they must notify the Headteacher as soon as possible without making a response. Similarly,

if any member of staff or individual associated with the school makes unintended contact with a pupil, it must be notified to the Headteacher as soon as possible. In the absence of the Headteacher, the Leading Teacher must be contacted. The Headteacher can then deal with the situation as appropriate.

Staff are reminded that bullying and harassment against any other member of staff via social media sites is taken as seriously as workplace bullying and harassment. Any allegations will be dealt with under the school's normal bullying and harassment or disciplinary policies as appropriate, and may also be treated as a criminal offence.

Employees that post defamatory statements that are published on the internet may be legally liable for any damage to the reputation of the individual concerned. As a representative of the school, any statement made by employees could mean the school is vicariously liable for those statements if done in the course of employment, even if performed without the consent or approval of the school. The school takes these acts seriously and disciplinary procedures will be invoked if any such defamatory statements are made by its employees, which may lead to dismissal.

In the case of governors, whilst volunteers and not subject to disciplinary procedures, referral to Governor Services in the Local Authority will be made and their advice and guidance will be taken.

4. Monitoring of Internet Access at Work

We reserve the right to monitor staffs' internet usage, but will endeavour to inform affected individuals when this is to happen and the reasons for it. We consider that valid reasons for checking a member of staff's internet usage include suspicions that they have:

- been spending an excessive amount of time viewing websites that are not work-related
- or acted in a way that damages the reputation of the school and/or breaches confidentiality
- contravened safeguarding policies or given cause for concern about their suitability to work with children.

The school reserves the right to request information regarding members of staff's use of the internet from our Internet Service Provider (ISP).

5. Disciplinary Action

If the school monitors staffs' internet use to ensure that it is in accordance with this policy, access to the web may be withdrawn in any case of misuse of this facility.

If appropriate, disciplinary action will also be taken in line with the school's disciplinary policy.

6. Security and Identify Theft

Staff should be aware that social networking websites are a public forum, particularly if the individual is part of a "network". Staff should not assume that their entries on any website will remain private. Staff should never send abusive or defamatory messages.

Staff must also be security conscious and should take steps to protect themselves from identify theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, staff must:

- Ensure that no information is made available that could provide a person with unauthorised access to the school and/or any confidential information; and
- Refrain from recording any confidential information regarding the school on any social networking website.

Publishing of information on social network sites should be assumed to be in the public domain as this will be assumed in all cases of breach of the policy.

We ask all staff to consider the following before posting information or images on social networking sites:

- Think carefully before posting information – would you want your employer or a potential employer to see it
- Think carefully about who might see this ie parents, pupils, the wider community, and what you do and don't want them to see
- Review your information regularly – what may have seemed like a good idea at the time may not seem such a good idea some months or years later.