Acceptable use of ICT, mobile devices and social networking sites by staff

Acceptable use of ICT, mobile devices and social networking sites by staff

Version control

Version	Status	Author	Date	Distribution
1.0	Published	Alan Noble	Nov 2011	All School Heads; Cognita Head Office.
1.1	Published	Andrew Savin	14-Dec-12	All School Heads; Cognita Head Office

Change control

Version	Changes made	New version
1.0	Changed wording of policy to reflect all mobile devices, rather than mobile phones. Replaced all references made to pupils to students. Edits and amendments to clauses 2, 3.4, 4.6, 4.8, 4.15, 4.21, 4.27, 5.2, 6.1.	1.1

Acceptable use of ICT, mobile devices and social networking sites by staff

Contents

Acceptable use of ICT, mobile devices and social networking sites by staff

1. PURPOSE

1.1 The policy defines and describes the acceptable use of ICT (Information and Communications Technology) and all mobile devices for school-based employees. Its purpose is to minimise the risk to students 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 equipment and services in schools in the Cognita Group and applies to all school-based employees and other authorised users, e.g. suppliers, contractors and volunteers.

3. SCHOOL RESPONSIBILITIES

3.1 Cognita acting as 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 Cognita is responsible for adopting relevant policies and the Headteacher for ensuring that the school adopts the policy and staff are aware of its contents.

3.3 The Headteacher is responsible for maintaining an inventory of ICT assets (hardware and software), including any equipment issued to staff for personal use, such as a laptop or mobile phone.

3.4 If the Headteacher has reason to believe that any ICT equipment has been misused, s/he should consult Cognita Head Office without delay. They will agree with the Headteacher an appropriate strategy for the investigation of the allegations. Incidents will be investigated in a timely manner in accordance with agreed procedures.

3.5 Headteachers should make it clear that internal school staff should not carry out any investigations unless they are 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. Staff must report all suspected breaches of this policy to the

Headteacher.

4.2 Staff and their line 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, staff 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. 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 provided with any portable ICT equipment, such as a laptop or mobile phone, are expected to sign for its use on receipt. Staff may use school equipment for authorised business use only.

4.6 Staff must follow authorised procedures when taking mobile devices offsite. Staff are not permitted to relocate ICT equipment without express permission by the ICT Department.

4.7 No one may use ICT resources in violation of license agreements, copyrights, contracts or national laws.

4.8 Users are required to protect their password and not utilise another user's account to misrepresent their identity for any reason.

4.9 No user shall access (e.g. 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 not take personaldata (e.g. student data) away from the school without authorisation from the Headteacher. Any electronic data that is taken offsite must be password protected and encrypted. This includes data held on portable equipment (laptops, USB drives) and Internet based file synchronisation tools, such as Dropbox.

4.12 Any device connecting to the school network 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 (e.g. 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, Cognita or the school may record or inspect any information transmitted through or stored in its computers, including e-mail 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 Cognita 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.

E-mail communication and any user data held on Cognita equipment may be inspected by the central ICT Support team with the agreement of the Headteacher. Other Internet based communication, such as web

browsing, is monitored using automated software.

4.15 Do not send private, sensitive or confidential information either by email or to a public printer – particularly to an external recipient - if accidental disclosure could lead to significant harm or embarrassment. Anonymise personal data where possible, e.g. by using initials. Use passwords on sensitive documents that must be sent to external recipients. The central ICT Support team can provide advice and guidance on solutions for secure email and print.

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, or may impact the image or reputation of the school or Cognita. 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 Users should adhere to the 'good practice guidelines for email communication', contained within the school Induction Pack.

4.19 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 because of race, sex, disability, sexual orientation, religion or age.
- Material relating to criminal activity.
- Material relating to any other unlawful activity e.g. breach of copyright.
- Material that may generate security risks and encourage computer misuse.

4.20 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.

4.21 Remote access to school based systems must be authorised by the Headteacher and configured by the ICT Support team. Examples of remote access methods include: webmail or other mobile email solutions (Blackberry, Windows Mobile), email forwarding to a personal account, Virtual Private Network (VPN) connection, LogMein or other remote desktop connection, web portals, and file synchronisation tools such as Dropbox.

4.22 Users must not connect any personal ICT equipment (e.g. laptop, netbook) to the school network without the authorisation of the Headteacher and the central ICT Support team.

4.23 All portable ICT equipment should be locked away or safely secured when not in use. Any staff authorised to use portable equipment, such as a laptop, for home or roaming use must take all reasonable efforts to keep the equipment safe and secure.

4.24 For security purposes users should log off or lock their computer if they expect to be absent from their desk for any length of time. Users must shutdown their computer at the end of the day.

4.25 Do not copy or install software owned by the school to any personal equipment without authorisation from the central ICT Support team.

4.26 Digital recording equipment e.g. cameras may be available for staff to use as part of delivering ICT and the broader curriculum. Safe and appropriate use of recording equipment should be discussed with the students as part of the curriculum and referred to whenever recording is to take place.

4.27 Staff must not use images and recordings for activities and purposes beyond school endorsed projects. The materials are not to be circulated in the public domain and are not to be used for personal gain. Staff should be aware of the students whose parents have expressly requested that photographs are not to be taken of them.

5. MOBILE PHONE COMMUNICATION AND INSTANT MESSAGING

5.1 Staff are advised not to give their home telephone number, mobile phone number, or personal email address to students. Mobile phone communication should be used sparingly and only when deemed

necessary.

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

5.4 Staff should only communicate electronically with students from school accounts on approved school business, e.g. coursework.

5.5 Staff should not enter into instant messaging communications with students.

5.6 Staff should not make or take personal calls or engage in personal texting when they are on duty – See King's School Mobile Phone Policy.

6. SOCIAL NETWORKING SITES

6.1 Staff should not connect with any current pupil or person under the age of 18 that they have taught on any social networking site.

6.2 Staff should not create any social networking group that links directly to the school or Cognita without the written permission of the Headteacher.

6.3 Staff that use social networking sites should not discuss work-related issues and should not bring the school's reputation in to disrepute.

To be reviewed annually.

Adopted at **School**

Signed…….

Date ……

Reviewed 9th September 2015