Hanson
EST. 1897

Hanson
EST. 1897

Hanson Policy for School Staff

Acceptable use of ICT, mobile devices and social networking sites

Approved by the governing body: May 2018

To be reviewed: May 2019

Signed on behalf of the governing body:

Contents

1. Introduction

The policy defines and describes the acceptable use of ICT (Information and Communications Technology), all mobile devices for school based employees and ensuring all staff are aware of their responsibilities with the growing use of social networking sites. Its purpose is to minimise the risk to students for inappropriate contact from staff, to protect employees and schools from litigation and to minimise the risk to ICT systems.

1.2 Policy Statement

The Governing Body recognises the use of its ICT and communications facilities as an important resource for teaching, learning and personal development and as an essential aid to business efficiency. It actively encourages staff to take full advantage of the potential for ICT and communications systems to enhance development in all areas of the curriculum and school administration. It is also recognised by the Governing Body that along with these benefits there are also responsibilities, especially for ensuring that children are protected from contact with inappropriate material.

In addition to their normal access to the school's ICT and communications systems for work-related purposes, the Governing Body permits staff limited reasonable personal use of ICT equipment and email and internet facilities during their **own** time subject to such use:

- not depriving pupils of the use of the equipment

and/or

- not interfering with the proper performance of the staff member's duties

Whilst the school's ICT systems may be used for both work-related and for personal use, the Governing Body expects use of this equipment for any purpose to be appropriate, courteous and consistent with the expectations of the Governing Body at all times.

This policy document is to be issued to all staff on its adoption by the Governing Body and when new staff are provided with mobile phones and passwords giving access to the ICT network.

1.3 Policy Coverage

This policy covers the use by staff of ICT and communications equipment both school owned and for personal use: examples of which include:

- laptop and personal computers
- ICT network facilities
- personal digital organisers and handheld computers
- mobile phones and phone/computing hybrid devices

- Flash drives and other physical and on-line storage devices
- Image data capture and storage devices including cameras, camera phones and video equipment

This list is not exhaustive.

1.4 Who does the policy apply to?

This policy applies to all school staff employed by the Local Authority, including Community and VA Schools. It will also apply to staff that are employed through agencies, casual workers, volunteers and governors.

1.5 Aims of the policy

- Ensure that employees and others listed above are aware of the risks associated with the inappropriate use of social networking sites and understand the importance of using them safely and securely
- Safeguard employees and others listed in the section above to ensure they do not make themselves vulnerable through their use of social networking sites
- Ensure that school maintains its duty to safeguard children, staff, the reputation of the school, the wider community and the Local Authority.

1.6 Relevant Legislation

- The Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990, updated by the Police and Justice Act 2006
- Regulation of Investigatory Powers Act 2000 (RIPA)

2. The use of school ICT and Communications Facilities

2.1 Use of School ICT Equipment

Staff who use the school's ICT and communications systems:

- must use it responsibly
- must keep it safe
- **must** sign and agree to the terms of the loan agreement (see appendix 1)
- where any damage/loss has occurred the user is responsible for the replacement cost.
- must not share and must treat as confidential any passwords provided to allow access to ICT equipment and/or beyond firewall protection boundaries
- must report any known breach of password confidentiality to the Headteacher or nominated ICT Technicians as soon as possible
- must report known breaches of this policy, including any inappropriate images or other material which may be discovered on the school's ICT systems

- must report to the Headteacher any vulnerabilities affecting child protection in the school's ICT and communications systems
- must not install software on the school's equipment, including freeware and shareware, unless authorised by the school's ICT Technicians
- must comply with any ICT security procedures governing the use of systems in the school, including anti-virus measures
- must ensure that it is used in compliance with this policy

Any equipment provided to a member of staff is provided for their personal use. Any use of the equipment by family or friends is not permitted and any misuse of the equipment by unauthorised users will be the responsibility of the staff member.

Whilst it is not possible to cover all eventualities, the following information is published as guidance for staff on the expectations of the Governing Body. Any breaches of this policy or operation of the school's equipment outside statutory legal compliance may be grounds for disciplinary action being taken.

2.2 Email and Internet

The following uses of the school's ICT system are prohibited and may amount to gross misconduct and could result in dismissal:

- to make, to gain access to, or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those likely to read or see it

- to make, to gain access to, and/or for the publication and distribution of material promoting homophobia or racial or religious hatred

- for the purpose of bullying or harassment, in connection with discrimination or denigration on the grounds of gender, race, religious, disability, age or sexual orientation

- for the publication and/or distribution of libellous statements or material which defames or degrades others

- for the publication of material that defames, denigrates or brings into disrepute the school and/or its staff and pupils

- for the publication and distribution of personal data without authorisation, consent or justification

- where the content of the e-mail correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination

- to participate in on-line gambling

- where the user infringes copyright law
- to gain unauthorised access to internal or external computer systems (commonly known as hacking)
- to create or deliberately distribute ICT or communications systems “malware”, including viruses, worms, etc.
- to record or monitor telephone or email communications without the approval of the Governing Body (or the Chair of Governors). In no case will such recording or monitoring be permitted unless it has been established for that such action is in full compliance with all relevant legislation and regulations (see Regulation of Investigatory Powers Act 2000, below)
- to enable or assist others to breach the Governors’ expectations as set out in this policy

Additionally, the following uses of school ICT facilities are not permitted and could lead to disciplinary action being taken:

- for participation in “chain” e-mail correspondence (including forwarding hoax virus warnings)
- in pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade unions)
- to access ICT facilities by using another person’s password, or to post anonymous messages or forge e-mail messages using another person's identity

3. Use of Social Networking Sites, employees, casual workers, volunteers and governors

3.2 Introduction

Hanson School is committed to ensuring that all staff are aware of their responsibilities in connection with the growing use of social networking sites such as blogs, MySpace, Facebook, Bebo, Youtube, Windows Live Spaces, MSN, forums, Instagram, Twitter, bulletin boards, multiplayer online gaming, chatrooms and instant messenger. Please note that this is a non-exhaustive list for illustrative purposes only and it should not be assumed that if it does not appear on this list the policy does not apply.

Staff are expected to maintain professional boundaries with pupils and there should be a clear separation of the private social lives of staff and that of pupils. Staff are advised that it is inappropriate to have on-line relationships with pupils (except where appropriate within family relationships) or to allow pupils access to their own pages. Similarly accessing pupils’ pages is discouraged as this may cross the professional boundary that should be maintained between staff and pupils.

Employees:

- should not befriend pupils online as personal communication could be considered inappropriate and may potentially make them vulnerable to allegations.
- should not place inappropriate photographs on any social network space.
- should not post indecent remarks.
- if a message is received on their social networking profile that they think could be from a pupil they should report it to their Line Manager/Headteacher so that this can be investigated and the appropriate action taken.
- must not disclose any confidential information or personal data about any individual/pupil/colleague which could be in breach of the Data Protection Act.
- should not post photographs or comments about pupils, other colleagues, the school, parents/guardians on social networking sites.
- should not make defamatory remarks about the school/colleagues/pupils/parents/guardians or the Local Authority or post anything that could potentially bring school or the Local Authority into disrepute.
- should be aware of the potential for on-line fraud and should be cautious when giving out personal information about themselves which may compromise their personal safety and security.
- should not access social networking sites for personal use via school information systems or using school equipment.
- staff should set their Social Network (facebook) settings to the maximum. For guidance on how to do this please see Using Facebook safely A guide for professionals working with young people.

3.3. Mobile Devices

- Staff use of mobile phones during their working day should be:
    - Outside of their contracted hours
    - Discreet and appropriate e.g. not in the presence of pupils
- Staff should not make or take personal calls or engage in personal texting during works time.
- Staff should never contact pupils or parents from their personal mobile phone or give their mobile phone number to pupils or parents.
- Staff should not use their mobile phones on the corridors, student social areas or in classrooms (during the school day)
- Staff are advised not to make use of students' mobile numbers either to make or receive phone calls or to send to or receive from students' text messages other than for approved school business.
- Staff should only communicate electronically with students from school accounts on approved school business, e.g. coursework
- Staff should not enter into instant messaging communications with students.

Note: The above restrictions apply to the use of phones, e-mails, text messaging, internet chatrooms, blogs, and personal websites (including personal entries on Facebook etc).

4. Breaches of the Policy

In instances where it is alleged that an issue has arisen in connection with the use of social media the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure or other appropriate procedure.
- The Governing Body will then take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school. Certain breaches may lead to your contract of employment or other agreed terms of engagement being subject to summary termination.
- Under the Regulation of Investigatory Powers Act 2000 (RIPA), the School can exercise the right to monitor the use of the school's information systems and internet access where it is believed that unauthorised use may be taking place, to ensure compliance with regulatory practices, to ensure standards of service are maintained, to prevent or detect crime, to protect the communications system and to pick up messages if someone is away from school. If such monitoring detects the unauthorised use of social networking sites disciplinary action may be taken where appropriate.
- In certain circumstances the school or Local Authority will be obliged to inform the police of any activity or behaviour where there are concerns as to its legality.