International

English Schools UK
Breckland

IES BRECKLAND

ACCEPTABLE USE OF ICT & MOBILE PHONES POLICY

Approved by the Governing Body, Chair of Governors:

August 2013

1 Introduction

1.1 Purpose

1.1.1 The purpose of this policy is to:

- define and describe the acceptable use of ICT (Information and Communications Technology) for the School;
- minimise the risk to ICT systems and the information contained in them and protect School Governors and staff from litigation.

1.1.2 It is not the intention of this policy to impose restrictions that are contrary to the established culture of openness and trust, and rights of access to information.

1.2 Background

1.2.1 The primary objectives of this policy are to:

- safeguard the integrity of data and ICT resources;
- minimise the liability arising from the misuse of ICT resources;
- protect the confidentiality of data and privacy of its users, to the extent required or allowed under law;
- maintain the availability of ICT resources.

1.3 Scope

1.3.1 This policy applies to the use of ICT facilities for which the School is accountable and responsible. It is applicable to School Governors, staff, any volunteers, partners and agents who the School have authorised to access ICT facilities including contractors and vendors with access to ICT systems. For the purposes of this Policy all these individuals are referred to as ‘user’ or ‘users’.

1.4 Linked/Other useful policies/procedures

This policy should be read in conjunction with the:

- Social Networking Policy

2. Responsibilities

2.1 Schools

2.1.1 Training – The School will train users in the Acceptable Use of ICT (Schools), including health and safety requirements under the display screen regulations 1992, Information Security and Data Protection, including when it is appropriate and permissible to share data.

2.1.2 Induction, Training and Support – The School is responsible for ensuring that adequate induction and training is undertaken by users and that support is provided to them so as to implement this policy.

2.1.3 User Access to Networks – The Principal, or delegated authority, is responsible for approving and authorising all user access to the School Network and ICT resources.

2.1.4 System or Account Misuse - When a complaint of possible system or account misuse by a user is reported, the validity of the incident will be reviewed according to the *School Policies and Procedures*. Incidents will be acknowledged and investigated in a timely manner. In certain circumstances, breach of this policy by a member of staff may be considered gross misconduct resulting in dismissal.

2.1.5 Equipment Disposal - 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.

2.2 Users

2.2.1 Training and Documentary Evidence - All users should attend the appropriate training courses and ensure that they possess and supply all required documentary evidence (e.g. DBS check).

2.2.2 User Agreement – By using the ICT equipment provided to them and by logging on to ICT systems, users agree to abide by this *Acceptable Use of ICT & Mobile Phones Policy* and other related policies.

2.2.3 User Account Name and Password - All users must have a unique user account name and password.

2.2.4 Access Authorisation – Users must not connect, or attempt to connect, any ICT equipment provided to them to any network, or system; or access, or attempt to access, any network or system without prior explicit authorisation to do so.

2.2.5 Breach of this Policy - Users found to be in breach of this policy may be disciplined in accordance with the *Schools Policies and Procedures*. In certain circumstances, breach of this policy by staff may be considered gross misconduct resulting in dismissal.

2.2.6 Data Protection - All users are expected to act in a responsible, ethical and lawful manner with the understanding that electronic and manual information may be accessible to the public under the relevant information legislation. 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. Users responsible for managing data should follow current *School Policies and Procedures* and best practice. This includes specifying and taking appropriate measures to secure data from unauthorised access during normal working processes, in transit or when in storage. (See also the *Data* section)

2.2.7 Authorised ICT Equipment – Users must only attempt to access the Schools Network from authorised ICT equipment and systems.

2.2.8 Movement of ICT Equipment - Users must not move to a new location ICT equipment that is ordinarily fixed (e.g. PC base units, printers and monitors). Local audit trails detailing current locations must be maintained for mobile devices shared within a team (e.g. laptops and portable data storage devices).

2.2.9 Mobile Devices - Users allocated mobile devices (e.g. laptops, tablets, Blackberry devices) must ensure that they are kept securely when not in use, or being transported and returned when they leave the School. The insurance policies used by the School do not cover loss of equipment from unattended vehicles.

2.2.10 Legal Responsibility - No user may use ICT resources in violation of license agreements, copyrights, contracts or national laws, or the policies, rules or regulations of the School.

2.2.11 Password and User Account Protection - 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 log on to a machine using their password for another user to then use. Users must not under any circumstances reveal their password to anyone.

2.2.12 Access to Another User’s Personal Electronic Documents - 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. Personal electronic documents are those that are solely non-business electronic documents.

2.2.13 Passwords - Users must choose passwords carefully and to comply with the following; all user-level passwords (e.g. for desktop computers, line-of-business applications) must as a minimum:

- be at least eight characters long;
- not contain your user name, real name, or company name;
- not contain a complete dictionary word;
- be significantly different from previous passwords (not Password1, Password2, Password3…etc);
- contain characters from three of each of the following four groups:

<table>
<tr><th>Group</th><th>Examples</th></tr>
<tr><td>Uppercase letters</td><td>A, B, C …</td></tr>
<tr><td>Lowercase letters</td><td>a, b, c …</td></tr>
<tr><td>Numerals</td><td>0, 1, 2, 3, 4, 5, 6, 7, 8, 9</td></tr>
<tr><td>Symbols found on the keyboard (all keyboard characters not defined as letters or numerals)</td><td>` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : “ ; ‘ < > ? , . /</td></tr>
</table>

Staff may keep a record of their password provided it is kept securely.

Passwords are an important aspect of computer security. They are the frontline of protection for user accounts. A user who carelessly selects a password may compromise an entire network.

Poor password management can result in security breaches and have serious implications including:

- Loss of reputation & credibility;

- Loss of clients and public trust;
- Loss of data and information;
- Financial loss (remedial work, penalties, direct loss, consequential loss);
- Criminal or civil action.

If a member of staff believes that a user account or password has been compromised, this should be reported to the *School's ICT Support* and all passwords must be changed.

2.2.14 Unauthorised Access Protection - Users must log out from or lock their PC or laptop when temporarily away from their desk to prevent unauthorised access. This applies wherever the user is located at the time of use (e.g. home or School).

2.2.15 Access to Data - Users must not access, load or download any data on any device without the knowledge, approval and authorisation of the owner and accountable person for the system the data originates from.

2.2.16 Anti-Virus and Personal Firewall Software - Network connected devices must have approved anti-virus and personal firewall software installed, activated and functioning. Users may not turn off anti-virus and personal firewall 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. If a device is identified as being infected with a possible virus, Trojan or worm, steps will be taken to isolate it from the network immediately.

2.2.17 ICT Security and Connection to Networks - 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. No one may make or attempt to make any unauthorised connection to the Schools network or connect any computer, network system or other ICT device to the School Network unless it has been approved by the School. Access to networks will be monitored as allowed for by this policy and law (see 2.3.6).

2.2.18 Wireless Connections – Users should not connect any School device to an unsecured Wireless Network.

2.2.19 Inappropriate Material - 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.

2.2.20 Inappropriate Content - 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, belief or age;

- material relating to criminal activity, for example buying and selling illegal drugs;
- material relating to any other unlawful activity e.g. breach of copyright;
- material that may generate security risks and encourage computer misuse.

2.2.21 Accidental Access of Inappropriate Material or Content - 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 users have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the Principal. This may avoid problems later should monitoring systems be alerted to the content.

2.2.22 Website Blocking - The School may block user access to various categories of websites, including download of content capability. This could be because the websites are not determined as appropriate for School use, or providing access could compromise the bandwidth of the Internet capability for essential School use, or that the content or download of content could pose a security threat to the School Network. If there is a need to access or download content from a blocked website then the user requiring access must request the access providing a full business case for doing so.

2.2.23 Website Appropriate Access - There may be circumstances where a website that would normally be blocked may not be because there is a legitimate need to access areas of the website, or download appropriate content. In these cases users must not access any areas of the site or download content for which there is not a legitimate need.

2.3 Personal Use and Privacy

2.3.1 Limitations of Personal Use - In the course of normal operations, ICT resources are only to be used for School purposes. The School permits the personal use of ICT facilities by authorised users subject to the following limitations:

- Personal use must be in the user’s own time and must not impact upon the School efficiency or costs;
- The level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided;
- 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;
- Personal use must not conflict with the *Schools Policies and Procedures*.

2.3.2 Examples of Acceptable Personal Use - Examples of acceptable personal use of ICT include online banking, shopping, learning activities, access to news and weather websites and the use of Office and email applications for personal organisation or charitable and other non-profit making activities.

2.3.3 Sound or Image Files - File formats associated with sound or images (e.g. JPEG, WAV, MP3) must not be stored on School ICT equipment for non-work purposes.

2.3.4 Inappropriate Content - Personal use of the Internet must not involve attempting to access the categories of content described in section 2.2.20, that is normally automatically blocked by the web filtering software. If you are connecting a device to any other network than the School Network then this policy still applies.

2.3.5 Recording and Inspecting Information - 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 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, or 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 School 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.

2.3.6 Monitoring - Any necessary monitoring will be carried out in accordance with the Information Commissioner's Office (ICO) *Code of Best Practice on Monitoring Employees*.

2.3.7 Violation of this Policy - Where an individual has reasonable cause to believe that another user has violated, or is violating this policy, or any guidelines, or procedures established to implement this policy then they shall in the first instance inform the Principal for investigation under the *Schools Policies and Procedures*. In certain circumstances the checks may necessitate the immediate suspension of the user's access to the School Network, ICT resources, ICT systems and applications in order that any potential evidence is not compromised.

2.4 Data

2.4.1 Managing Data - Users responsible for managing data should follow best practice. This includes specifying and taking appropriate measures to secure data from unauthorised access during normal working processes, in transit, when in storage or in the possession of third parties.

2.4.2 'Sensitive' or Protectively Marked Data - Where the user is accessing a system showing 'sensitive' data then the screen must not be easily readable by anyone other than the logged-in user. Workstations and screens shall be arranged to ensure that the screen is facing away from the line of sight of any visitors.

2.4.3 Personal Documents and Folders - Personal documents and folders regarded as "personal" must be clearly titled to reduce the risk of administrators inadvertently viewing private, non-work documents. Personal documents and folders must be deleted from the School systems as soon as possible.

2.3.4 Printed Material – Users must securely store or destroy any printed material.

2.3.5 Movement of Data and Records – Users must not remove information (data and records both electronic and paper) from School premises without appropriate approval.

2.3.6 Accessing Folders and Mailboxes of Users

Access to Another User’s Folders or Email Mailbox - Do not attempt to gain access to any other user’s folders or email mailbox without their permission.

2.5 Mobile phone communication, photographs and instant messaging

2.5.1 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.

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

2.5.3 Photographs taken of students/pupils on schools resources must not be placed on personal social networking sites or the school’s website without parental or guardian consent. This is personal related data and individuals must be aware that this information is being published. Failure to obtain consent could result in formal action being taken.

2.5.4 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 and with the Principal’s approval.

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

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

2.5.7 It is not appropriate to use mobile phones during working hours e.g. texting. If access is required this must be discussed and agreed with the Headteacher

Further Advice

For further advice on this policy, please contact:

The School’s ICT Support, HR Manager or Principal