Benson Community School

There are no limits to what you can achieve

Acceptable use of Technology agreement

Purpose

The policy defines and describes the acceptable use of Technology (Includes, Computers, Mobile Phones, iPads,Apple Watches and any other recordable devices) for school-based employees/contractors.

Its purpose is to minimise the risk to pupils, protect staff and to minimise the risk to ICT systems and Data.

Scope

This policy deals with the use of Technology and applies to all school-based employees, Agency staff and other authorised users, e.g. volunteers/contractors.

School Responsibilities

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.

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

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.

If the Headteacher has reason to believe that any ICT equipment has been misused, he/she should consult the Central School Support Officer and seek advice without delay. The Child Protection Officer will also be contacted. An appropriate strategy for the investigation of the allegations will be agreed. Incidents will be investigated in a timely manner in accordance with agreed procedures.

Internal school staff should not carry out any investigations unless they are both qualified and authorised to do so.

Date Agreed Next Review Date

User Responsibilities

Staff found to be in breach of this policy may be disciplined in accordance with the LA disciplinary procedures. 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.

The school is responsible for ensuring that adequate induction, training and support is undertaken to implement this policy.

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 (e-safety and Data Protection Policies)

All users must practice good housekeeping, ensuring user areas are regularly reviewed for data that is no longer required.

You will be allocated a certain amount of space on the network. This is yours to manage in line with school policies.

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.

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.

Staff must make sure the equipment is locked away in the correct location after use and return the key to the main office.

Staff must get permission from the head teacher when taking a school device off site and ensure that it is kept securely and safely at all times.

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 LA.

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.

Staff Must Change passwords on a Periodic basis containing a least one capital letter and 1 number

Staff must ensure that all computers are locked upon leaving their desks for any period of time

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.

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.

Users must take care to store sensitive information, e.g. pupil data safely in the designated areas to make sure its stored securely on all school systems, including laptops.

Staff should not take sensitive Data off site without prior consent from the Head teacher, all sensitive data off site must be kept on an encrypted device

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 (e.g. viruses, Trojans, worms) or another destructive program on any ICT resource.

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.

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 LA or 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 the LA or its partners from liability.

Establishing the existence of facts relevant to the business.

Date Agreed   Next Review Date

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.

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 e.g. by using initials. Use passwords on sensitive documents that must be sent to external recipients.

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

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.

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 e.g. breach of copyright

Material that may generate security risks and encourage computer misuse

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/Deputy Headteacher. This may avoid problems later should monitoring systems be alerted to the content.

Staff should not sign in and tweet from the School twitter account on their personal devices.

Personal Memory sticks must not be used, the school will issue you with an encrypted device at the start of your employment.

Staff have a responsibility to make sure all computers / devices are locked when leaving them unattended, please see data protection policy for more information

Personal Use and Privacy

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: Staff are expected to demonstrate a sense of responsibility and not abuse this privilege.

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.

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 of the Internet must not involve attempting to access the categories of content described above that is normally automatically blocked by web filtering software.

Communication

Staff are advised not to give their home telephone number or their mobile phone number to pupils. All communications with pupils/parents/carers must go through the main School Office. Mobile phone communication should be used sparingly and only when deemed necessary eg: late return from a trip/residential.

Photographs and videos of pupils should not be taken with personal devices; iPads, Apple Watches, Mobile Phones or any personal mobile recording device.

Staff should only communicate electronically with pupils from school accounts for approved school business, e.g. coursework. (Applies mainly to Secondary Schools)

If a pupil tries to contact a member of staff via technological communications this must be reported to either the Headteacher or Deputy Headteacher immediately. The parents of the child will then be contacted and informed.

Staff must not engage with pupils / parents via personal social media accounts

Links : Data Protection, E-safety Policy.

Technology changes regularly, no policy can lay down the rules for every possible situation, this policy is designed to express the philosophy of the school and provide general principles for using ICT. If ever in doubt staff must ask their Line Managers/Headteacher for clarification.

Name…………………………………………..

Signed……………………………………….

Date ……………………………………

I consent for my name and photograph to be used on all official school media like the website and twitter account, unless I state otherwise.

Date Agreed   Next Review Date