Guildhall Feoffment
Community Primary School

Acceptable Use of ICT Policy

Approved by	Full Governing Body- Resources
Date	28th November 2023
Review by	

This authority is committed to safeguarding and promoting the welfare of children, young people and vulnerable adults and expects all staff and volunteers to share this commitment.
A copy of our Safeguarding Policy is available upon request

Table of Contents

1 INTRODUCTION

Purpose

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.

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.

Background

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.

Scope

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'.

Linked/Other useful policies/procedures

This policy should be read in conjunction with the:

- Email Acceptable Use Policy (Schools)
- Information Management Policy

2 RESPONSIBILITIES

School

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.

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.

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

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.

Equipment Disposal - Equipment disposal will be managed in accordance with the Finance Policy, the Waste Electrical & Electronic Equipment Directive (WEEE). Mobile Media (e.g. CD ROMS, DVDs) should be disposed of by way of confidential destruction.

Users

Training and Documentary Evidence - All users should attend appropriate training courses.

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 Policy and other related policies.

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

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.

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.

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. 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)

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

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).

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.

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.

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. (See the Password Management Policy (Schools))

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. (See the Email Acceptable Use Policy (Schools)) Personal electronic documents are those that are solely

non business electronic documents. Shared documents designed with the purpose of being edited by multiple users can be edited by any authorised user.

Passwords - Users must choose passwords carefully and to comply with the Password Management Policy (Schools).

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).

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.

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.

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).

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

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. (See the Email Acceptable Use Policy (Schools))

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.

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 Head Teacher. This may avoid problems later should monitoring systems be alerted to the content.

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.

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.

Personal Use and Privacy

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.

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. (See also Email Acceptable Use Policy (Schools))

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.

Inappropriate Content - Personal use of the Internet must not involve attempting to access the categories of content 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.

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.

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

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 Head Teacher 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.

Data

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.

'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.

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.

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

Movement of Data and Records – Users must not remove information (data and records both electronic and paper) from School premises without appropriate approval. All Teaching Staff will be provided with encrypted memory sticks if they wish to store any confidential or sensitive data about pupils, staff and the school.

Data must not be backed up on any device or by any method not approved by the school. This includes home computers, "Clouds" and unencrypted memory sticks.

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.

3 Policy & Guidance on the use of Social Networking Sites

General

This policy on social networking websites is in addition to the School's existing policy on email and internet use or Acceptable Use 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.

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

Personal use of the internet

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, and Twitter, outside of work.

Access to social networking sites is only allowed where use of such websites is for school purposes.

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; and
- 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, 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 Head Teacher as soon as possible. In the absence of the Head Teacher, the Deputy or Assistant Head or a member of the SLT 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 schools' 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.

Monitoring of internet access at work

We reserve the right to monitor staffs' internet usage, but will endeavour to inform an affected individual 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).

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.

Security and identity 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 identity 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, i.e. 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

4 REVIEW

This policy will be reviewed by the school every two years as a minimum.