Electronic Information Security Policy - schools

The information systems policy covers the use of ICT systems to support learning, the use of telephones, email and the internet by staff, and the use of online tools provided by the school. This policy consists of three sections:

1. **Acceptable use of ICT equipment**
2. **Use of telephones, email and internet by staff**
3. **Safe use of Management Information Systems**
4. **Use of Social Media**

1. Acceptable use of ICT Equipment

The Trust is committed to safeguarding all ICT infrastructure to ensure it can be used in the most effective manner to support teaching and learning processes. Ensuring the safety and integrity of the school's ICT infrastructure is the responsibility of all staff.
The school encourages staff to fully use the ICT infrastructure and to make use of portable ICT equipment offsite to support them in their work. The school encourages this use in a responsible and professional manner.
As a user of ICT services of the school you have a right to use its computing services; that right places responsibilities on you as a user which are outlined below. If you misuse school computing facilities in a way that constitutes a breach or disregard of this policy, you may be subject to disciplinary procedures.
Ignorance of this policy and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.
Staff are advised of this policy during their induction and of the school's requirement for them to adhere to the conditions therein.
For the purposes of this policy the term "computing services" refers to any ICT resource made available to you, any of the network borne services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the Internet). Staff who connect their own ICT to the School's network and the services available are particularly reminded that such use requires compliance to this policy.

Purposes

- To ensure Trust schools are able to provide a high quality education supported by a well- protected ICT infrastructure
- To protect the school's networks and equipment
- To protect the school's data
- To protect the school and its employees from activities that might expose them to legal action from other parties

Guidelines Password security

Access to all systems and services is controlled by a central computing account and password. Staff are allocated their User ID and initial password as part of their induction with the School.
Issuance and continued use of your User Account is conditional on your compliance with this policy. User IDs and passwords are not to be shared or revealed to any other party. Those who use another person's user credentials and those who share such credentials with others or allow others to access or use their account once opened will be in breach of this policy.
Initial default passwords issued to any user should be changed immediately following notification of account set up. Passwords should be routinely changed and should be changed immediately if the user believes or suspects that their account has been compromised.

General Conditions

In general, use of school "computing services" should be for teaching and/or administrative purposes of the school. Modest use of the facilities and services for personal use is accepted so long as such activity does not contravene the conditions of this policy.

- Your use of the school's computing services must at all times comply with the law.
- Your use of the school's computing services must not interfere with any others' use of these facilities and services.
- You are not entitled to use a computer that you have not been authorised to use.
- You must not access any program or data which has not been specifically authorised for your use.
- You must not use or copy any data or program belonging to other users without their express and specific permission.
- You must not alter computer material belonging to another user without the users' permission.
- You must not use school computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.
- You must not use school computing services for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such.
- You must not use the school's computing services to conduct any form of commercial activity without express permission.
- You must not use the school's computing services to disseminate mass (unsolicited) mailings.
- You must not install, use or distribute software for which you do not have a licence, and which is not first authorised by your IT provider for installation
- You must not use any peer-to-peer file sharing software
- You must not use any IRC or messenger software unless expressly authorized to do so for work related purposes
- You must not post or subscribe to newsgroups, on-line discussion boards or email list groups from the school's facilities, unless specifically related to school activities
- You must not use any form of network monitoring which will intercept data not specifically intended for you unless this activity is a part of your normal job responsibilities or has been specifically authorised by the Head teacher

Data Security

The school holds a variety of sensitive data including personal information about pupils and staff. If you have been given access to this information, you are reminded of your responsibilities under data protection law.

You should only take a copy of data outside the school's systems if absolutely necessary, and you should exhaust all other options before doing so. This includes putting sensitive data onto laptops, mobile devices or into emails. If you do need to take data outside the school, this should only be with the authorisation of the Head teacher. As part of this you should perform a risk assessment on the implications of it falling into the wrong hands, and take appropriate steps to mitigate against this. This will almost certainly include encrypting the information, and checking the data protection statements of any recipients of the data.

There are a variety of methods of remote access to systems available (in particular using VPN and remote desktop or terminal services) which allow you to work on data in-situ rather than taking it outside the School, and these should always be used in preference to taking data off-site.

The school's IT provider will be able to advise further.

Anti-Virus and Firewall Security

All personal computers are installed with virus protection and firewall software by the school's IT provider. Users are not to alter the configuration of this software. This software is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

If any user suspects viral infection on their machine, they should **disconnect their PC from the network and inform the school's IT provider immediately.** If your IT provider detects a machine behaving abnormally due to a possible viral infection it will be disconnected from the network until deemed safe.

Physical Security

Users of ICT equipment should always adhere to the following guidelines:

- Treat equipment safely, in the same manner as a reasonable person would
- Keep liquids away from ICT equipment
- Do not place heavy objects on ICT equipment
- Do not drop ICT equipment or objects onto it
- Any portable computer must be securely locked away when not in use.
- Portable computer security is your responsibility at all times.
- Do not leave the portable computer unattended in a public place or within the school
- Do not leave the portable computer on view inside your car. It should be locked away in your car's boot out of sight.
- Extra reasonable care must be taken to prevent the loss of external and removable drives which contain confidential school data
- Staff supervising pupils using ICT equipment should ensure pupils take reasonable care of such equipment

Remote Access

Remote access to the school network is possible where this has been granted by your IT provider.
Remote connections are considered direct connections to the school network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy.
All connection attempts are logged.

Monitoring and Logging

Activities regarding network transactions may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised systems personnel and kept for no longer than necessary and in line with current data protection guidelines.
Such records and information are sometimes required - under law - by external agencies and authorities. The school will comply with such requests when formally submitted.

Breaches of This Policy

Incidents which are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of user related activity and evidence. Breaches of this policy will be dealt with in accordance with the Trust's disciplinary policy.

2. Use of telephones, email and internet by staff

Principles

The provisions of this Policy apply to all members of staff, whether or not they have access to, or sole use of, a telephone or e-mail/the Internet on a personal computer. Although access to such facilities does not form part of the benefits provided to staff, it is recognised that there are occasions when employees might legitimately make private use of these facilities. This Policy is intended to make clear what constitutes legitimate use. It is intended not to place employees under unjustifiable scrutiny, but to give them a high measure of security and confidence about their use of e-mail, telephones and the Internet.
The sections of the policy covered by misconduct and misuse should be read in conjunction with the appropriate staff disciplinary procedure.
This Policy has been designed to safeguard the legal rights of members of staff.

Purposes

To provide guidance on inappropriate use of school telephones, email and internet facilities. To clarify when the school may monitor staff usage of these facilities.

Guidelines
Use of telephones

There will be occasions when employees need to make short, personal telephone calls on school telephones in order to deal with occasional and urgent personal matters. Where possible, such calls should be made and received outside the employee's normal working hours or when they do not interfere with work requirements.
The use of school telephones for private purposes, which are unreasonably excessive or for school purposes which are defamatory, obscene or otherwise inappropriate, may be treated as misconduct under the appropriate disciplinary procedure.
Where the school has grounds to suspect possible misuse of its telephones, it reserves the right to audit the destination and length of out-going calls and the source and length of in-coming calls. This would not normally involve the surveillance of calls but in certain rare circumstances where there are reasonable grounds to suspect serious misconduct, the school reserves the right to record calls.
Mobile phones - Do not keep any message or picture on your phone which you would not be happy for others to see. Do not leave your phone where pupils can get hold of it. Do not under any circumstance give your phone number or lend your phone to a pupil for any reason. Do not use your mobile phone to phone or text any pupil. Dialling 141 as a prefix before dialling a number will prevent the caller from seeing your number.If you have an Apple I phone you can change your settings to block caller ID.
Use the school's mobile phone as a contact number if you are going on a trip with the school. Please act wisely if you know pupils personally outside of the school environment.

Use of email

As with telephones it is recognised that employees can use e-mail for personal means in the same manner as that set out for telephones above. E-mail should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter or memorandum is equally unacceptable in an e-mail communication.
Staff should be careful that before they open any attachment to a personal e-mail they receive, they are reasonably confident that the content is in no sense obscene or defamatory to avoid contravening the law. Equally, if a staff member receives an obscene or defamatory e-mail, whether unwittingly or otherwise and from whatever source, s/he should not intentionally forward the e-mail to any other address, unless specifically requested to do so by an investigator appointed by the school. Any other use of e-mail for either personal or school purposes to send or forward messages or attachments which are in any way defamatory, obscene or otherwise inappropriate will be treated as misconduct under the appropriate disciplinary procedure.
Where the school has reasonable grounds to suspect misuse of e-mail in either scale of use, content or nature of messages, it reserves the right to audit the destination, source and content of e-mail to and from a particular address.
The school also reserves the right to access an employee's e-mail account in her/his unexpected or prolonged absence (e.g. due to sickness) in order to allow it to continue to undertake the employee's normal role. In normal circumstances the employee concerned will be contacted before this is done, in order to provide him/her with prior knowledge.

Use of the Internet

The primary reason for the provision of Internet access is for the easy retrieval of information for educational purposes, or to make use of learning resources, or to make legitimate authorised purchases to enhance the ability of staff to undertake their school role. However, it is legitimate for employees to make use of the Internet in its various forms in the same way as email above as long as it is not used to view or distribute

improper material such as text, messages or images which are derogatory, defamatory or obscene.
Unauthorised use of the Internet, which is unreasonably excessive for personal use or for purposes which are defamatory, obscene or otherwise inappropriate will be treated as misconduct under the appropriate disciplinary procedure. The school reserves the right to audit the use of the Internet from particular Personal Computers or accounts where it suspects misuse of the facility.

Monitoring the use of telephone, e-mail and the Internet.

It is not the school's policy, as a matter of routine, to monitor an employee's use of the school's telephone or e-mail service or of the Internet via the school's networks. However, as has been stated, where there are reasonable grounds to suspect an instance of misuse or abuse of any of these services, the Head teacher may grant permission for the auditing of an employee's telephone calls e-mail or the Internet. Once approved, the monitoring process will be undertaken by designated staff acting, for operational purposes, under the direction of the Head teacher. These staff are required to observe the strictest confidentiality when undertaking these activities and they will monitor only to the extent necessary to establish the facts of the case. They will make their reports directly to the Head teacher.

3. Safe use of Management InformationSystems

Principles
This applies wherever access to the school Management Information Systems (MIS) are provided. This applies to all online resources provided by the school, for example Capita SIMS. This policy applies whenever information is accessed through the school MIS, whether the computer equipment used is owned by the school or not. The policy applies to all those who make use of the school's MIS resources.

Purposes Security

- This Policy is intended to minimise security risks. These risks might affect the integrity of the school's data, the authorised MIS User and the individuals to which the MIS data pertains. In particular these risks arise from:

  - the intentional or unintentional disclosure of login credentials
  - the wrongful disclosure of private, sensitive, and confidential information
  - Exposure of the school to vicarious liability for information wrongfully disclosed by authorised users.

Data Access

- This Policy aims to ensure all relevant aspects of the Data Protection Act (1998), GDPR and Fair Processing Policy are adhered to.
- This Policy aims to promote best use of the MIS system to further the communication and freedom of information between the school and Parents/Carers.

Guidelines
The school's online systems are provided for use only by persons who are legally responsible for pupil(s) currently attending the school.

Access is granted only on condition that the individual formally agrees to the terms of this Policy by signing at the end of this policy.

The authorising member of school staff **must** confirm that there is a legitimate entitlement to access information for pupils.

Personal Use

Information made available through the MIS system is confidential and protected by law. To that aim:

Users must not distribute or disclose any information obtained from the MIS to any person(s) with the exception of the pupil to which the information relates **(ONLY if it is done so in a way intended to support learning or good pastoral care**) or to other adults with parental/carer responsibility.

Best practice is not to access the system in any environment where the security of the information contained may be placed at risk. Particular care should be exercised when using a projector or interactive whiteboard connected to a computer with the MIS open, for example if using the MIS to take the attendance register.

Password Policy

Staff must assume personal responsibility for usernames and passwords. Never use anyone else's username or password.

You must always keep your individual user name and password confidential. These usernames and passwords should ***never*** be disclosed to anyone. Passwords and user names should never be shared.

In some instances users may be given the right to change passwords from the one originally issued.

Questions, Complaints and Appeals

MIS users should address any complaints and enquiries about the MIS system to the school in writing to the Head Teacher.

The school reserves the right to revoke or deny access to MIS systems of any individual under the following circumstances:

- the validity of parental/carer responsibility is questioned
- Court ruling preventing access to child or family members is issued
- Users found to be in breach of this policy

If any child protection concerns are raised or disputes occur the school will revoke access for all parties concerned pending investigation.

4. Use of Social Media

The use of social networking sites such as WhatsApp, Facebook, You Tube, Twitter, Flickr, Instagram, etc have become increasingly popular. The use of technology for educational purposes is an important part of our work. However it is imperative that such websites are not abused. For your own protection you are expected to carefully consider the use you make of all social media including messaging and social networking sites, blogging and the internet. High expectations and standards of professional behaviour in relation to the use of electronic interaction are as relevant

as face to face behaviour. Do not mention a pupil by name in any of your interactions and be circumspect in mentioning the name of a colleague, taking data protection matters into consideration at all times.
Be aware of potential problems which can arise by providing personal details on social networking sites. Do not use your personal e-mail address to communicate with pupils or parents. If you do receive work by pupils via e-mail please use the school's official e-mail and keep any comments within professional matters.

Social networking sites – it is not acceptable for you to refer any pupil or colleague by name in any way on a social networking site or in a blog. It is also not acceptable to use any pictures of them on such sites. Do not become an on-line 'friend' with any of the pupils or parents. Remember you should not publish anything that you haven't agreed to put your name to. If you do not want any comments to be associated publicly with yourself then do not do so at all.

Social media - You must give proper consideration to the fact that the same professional ethical obligations apply to all staff in their conduct in online and offline environments. It is important that personal and professional uses are not confused. Therefore, even when you are using social media channels for personal use, you should consider whether you will be associated with activities which may be visible online and which, in the future, could be viewed by other professionals. Information you share, may be accessible to a much wider audience than intended.

Electronic Information Security Declaration

By signing the acceptance form you are agreeing that you have fully understood and accept the terms and conditions and all the instructions of the school Electronic Information Security Policy.
Please contact the Heed teacher if you are not sure of any policies and terms and conditions of use.

Signature……..
Name……..
Date……