Mayfield School

Acceptable use of the Internet, Data Security and E-Safety Policy

September 2018

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this **information is sensitive** and could be used by another person or criminal organisation to cause harm or distress to an individual. The **loss of sensitive information** can result in media coverage, and **potentially damage the reputation of the school**. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Mayfield School works to the recommendations set out in WMnet E-Safety Framework, this framework complimenting the BECTA ICT Self Review Framework and OfSTEDs Self Evaluation Framework.

It is currently working towards the roll out of encryption technologies across all of its ICT hardware and software.

The policy will be amended if new technologies are adopted or Central Government change the guidance in any way.

Protecting Pupils

The school will never publish photographs of, or name, individual children without prior parent/carer consent. It will only publish back or side on photographs only even if parents/carers consent, whether this be on the school website, on Bgfl or on other internet sites.

The school will comply with LA Policy on acceptable use of the internet, as set down in the Birmingham LA Policy document. The copyright of material will be respected by all users of the school network.

The school will exclusively use the filtered service provider BGfL for internet access.

Pupils must only access the internet while under direct supervision from a member of staff.

Internet Access and Use

Under no circumstances whatsoever should sites containing inappropriate or undesirable information to be accessed. If a member of staff becomes inadvertently connected to such a site, he or she should disconnect immediately and notify their line manager who must notify the Head Teacher. Any inappropriate material discovered must be reported immediately.

Deliberate access to inappropriate materials by any user will lead to the incident being logged; investigation by the Head Teacher/ LA: disciplinary procedures being invoked; possible immediate suspension which may lead to dismissal and involvement of police for very serious offences

Staff should be aware that the computer will maintain a history of sites visited.

Personal use by staff of the internet is not permitted.

Account Security

General Security Overview

The School gives relevant staff only access to its Management Information System, with a unique ID and password.

It is the responsibility of everyone to keep passwords secure.

Staff should be aware of their responsibility when accessing school data. If they are unclear then they should ask and not wait until the next routine refresher training.

Staff have access to the relevant guidance documents and this policy is in the staffroom policy folder and also upon request from the school office.

The school has identified Senior Information Risk Owner (SIRO) and Asset Information Owner(s) (AIO) in school. The SIRO is the Head Teacher and all other leadership team members, therapists and assistants, office staff and teachers are AIOs as they hold pupil specific data and information.

School keeps all school related data secure. This includes all personal, sensitive, confidential or classified data.

Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible they should keep it locked out of sight.

Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.

It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used.

Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent.

Password Security

Password security is essential for staff, particularly as they may be able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone.

Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username. They are also expected to use a personal password and keep it private and only use their own password and log-in to the systems. Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures. Staff should change temporary passwords at first logon. Staff should not record passwords or encryption keys on paper or in an unprotected file.

Staff should only disclose their personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished

Pupils are not allowed to deliberately access on-line materials or files on the school network, of their, teachers or others.

Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically.

Individual staff users must also make sure that workstations are not left unattended and are locked.

In our school, all ICT password policies are the responsibility of the Governing Body and all staff and pupils are expected to comply with the policies at all times.

Zombie Accounts (Old Accounts)

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school’s systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access. The school will ensure that all user accounts are disabled once the member of the school has left as prompt action on disabling accounts will prevent unauthorized access

Email Specific Issues and Advice

General

Access to e-mail will be provided only through the LA filtered service.

The school will use an additional e-mail filter system [sophos] to help ensure that file attachments containing viruses cannot be sent or received

Although all mailboxes will be password protected to ensure confidentiality users should be aware that all e-mails will be scanned by LA software to ensure that improper use is monitored. The school also uses forensic software to capture information for LA and SIRO.

Passwords should be changed regularly and where necessary a record kept.

Managing e-Mail

The school may give staff their own e-mail account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.

Under no circumstances should staff contact pupils, parents or conduct any school business using personal school e-mail addresses. Contact with parents and pupils using home ICT equipment falls beyond the scope of this policy but within the safeguarding and professional standards frameworks of LA workers and therefore should not happen.

All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper

Staff sending e-mails to external organizations are advised to cc. the Head Teacher, line manager or designated account

E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

Delete all e-mails of short-term value

Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending, reading or receiving business related e-mail is not permitted. Personal email accounts using such providers should not be accessed using school ICT.

E-mail should not be left running while staff are away from their desk, to prevent unauthorised access. When staff have to leave a desk e-mail should be shut down and re-opened once again.

Sending e-Mails

Use your own school e-mail account so that you are clearly identified as the originator of a message

If you are required to send an e-mail from someone else's account, always sign on through the 'Delegation' facility within your e-mail software so that you are identified as the sender (if available within your software)

Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate

Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments

An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail

School e-mail is not to be used for personal advertising

Receiving e-Mails

Check your e-mail regularly

Activate your 'out-of-office' notification when away for extended periods

Use the 'Delegation' facility within your e-mail software so that your e-mail can be handled by someone else while you are not at work (if available within your software)

Never open attachments from an untrusted source; Consult your network manager first.

Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

The automatic forwarding and deletion of e-mails is not allowed

e-mailing Personal, Sensitive, Confidential or Classified Information

Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible

Where your conclusion is that e-mail must be used to transmit such data:

Obtain express consent from your manager to provide the information by e-mail

Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary

Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone)

Do not identify such information in the subject line of any e-mail

Request confirmation of safe receipt

Compliance Officers and Monitoring

Compliance

Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff who is familiar with information risks and the school's response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities:

- they own the information risk policy and risk assessment
- they appoint the Information Asset Owner(s) (IAOs)
- they act as an advocate for information risk management

The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support SIROs in their role.

The SIRO in this school is the Head Teacher.

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Schools should identify an Information Asset Owner. For example, the school's Management Information System (MIS) should be identified as an asset and should have an Information Asset Owner. In this example the MIS Administrator or Manger could be the IAO.
The role of an IAO is to understand:

- what information is held, and for what purposes
- what information needs to be protected (e.g. any data that can be linked to an individual, pupil or staff etc including UPN, teacher DCSF number etc)
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

Although these roles have been explicitly identified, the handling of secure data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask the Head Teacher. Authorised persons include the Head Teacher, Deputy Head Teacher, Link2ICT approved staff, LA Statutory Safeguarding Officers, Police(upon request to Head Teacher), school ICT staff (upon instruction of Head Teacher)

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT will therefore unavoidably be included in any business communications that are monitored, intercepted and/or recorded.

Breaches, Incidents and Actions

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Senior Information Risk Owner (SIRO). Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the SIRO.

Complaints and/ or issues relating to eSafety should be made to the Head Teacher.

The School Response to Incidents

All `incidents' must be reported both to the system manager and the Head Teacher who will take appropriate action.

The LA (Learning and Culture IT) will be informed and if appropriate sanctions may be put in place.

Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Head Teacher or Deputy

Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the Local Authority Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed off through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen

Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e
Data Protection Act 1998
http://www.ico.gov.uk/what_we_cover/data_protection.aspx
Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal

The school's disposal record will include:

Date item disposed of

Authorisation for disposal, including:

verification of software licensing

any personal data likely to be held on the storage media? *

How it was disposed of eg waste, gift, sale

Name of person & / or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate