Maiden Erlegh Trust

PROTOCOL FOR ACCEPTABLE USE OF DIGITAL TECHNOLOGY FOR STAFF

Initial approval:	May 2019
Review frequency:	Every three years
Date(s) reviewed:	August 2010, August 2023, April 2024

Contents

Rationale

Computer, web-based and telephone services are increasingly important in the delivery of many of the Trust's services. Due to this dependence, the value and confidentiality of information processed, and current legislation, it is imperative that certain procedures and best practices are adhered to by all staff.

If in any doubt about the application of this protocol you should contact your line manager in the first instance, or a member of the local SLG.

At Maiden Erlegh Trust, we know that schools hold personal data on students, 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 also result in media coverage, and potentially damage the reputation of the Trust. This could make it more difficult for us to use technology to benefit students.

Data is processed across the Maiden Erlegh Trust for the educational benefit and wellbeing of all our students and staff. The Trust has an ongoing process for refining its compliance with regard to UK General Data Protection Regulations (UK GDPR) and Data Protection Act 2018 (DPA 2018), policies and procedures will be reviewed at an appropriate stage.

Everybody in the Trust 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.

All users must read and sign an Acceptable Use Agreement to demonstrate that they have understood the Trust's Acceptable Use Protocol.

Aims

The aims of this protocol are:

Promote the professional, ethical, lawful and productive use of the School's ICT systems and infrastructure;
Define and identify unacceptable use of the School's ICT systems and external systems;
Educate users about their data security responsibilities;
Describe why monitoring of the ICT systems may take place;
Define and identify unacceptable use of social networking sites and school devices; and
Specify the consequences of non-compliance.

This policy applies to staff members, governors and all users of the School's ICT systems who are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by staff and monitoring by the Trust of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to the Head of Trust Operations.

Scope

The protocol applies to all employees, governors, visitors, students, and contracted staff of Maiden Erlegh Trust using the following types of IT facilities whether working in or out of school:

Internet, including the website and Online Applications.
Email.
Hardware provided by the Trust and/or owned by third parties but brought onto school premises.
Management information systems.
Telephones of all types
Bring Your Own Devices (BYOD).

All equipment that constitutes the Trust's ICT systems is the sole property of the Trust.

Personal equipment can be connected to or used with the Trust's ICT systems, with permission from Head of Trust Operations or School Business Manager. It is important that if personal devices are connected, then school owned data is not downloaded or saved on personal devices.

Users must not try to install any software on the ICT systems on school owned devices. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

The Head of Trust Operations & Business Mangaers are responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptops/desktop computers or ICT equipment may be removed at any time and without prior warning for regular maintenance, reallocation or any other operational reason. Maintenance includes but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

E-Safety

E-safety is a whole-Trust issue and responsibility and forms part of our safeguarding duties. Elements of e-safety run through the entirety of this protocol.

We know that some people will use the internet to harm children and/or young people e.g. by sending hurtful or abusive texts and emails, enticing them to engage in sexually harmful conversations or actions online, webcam filming, photography, or face-to-face meetings.

There is a 'duty of care' for all staff to educate students on the risks of using the internet (including social network sites) and on how to use these media safely. They also have a duty to refer any potentially unsafe behaviour Designated Safeguarding Lead as soon as they become aware of it.

Cyber-bullying by staff/students will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures**.**

We also educate staff/students on how individuals and groups use the internet and social media to groom and radicalise them, and how to protect themselves from these risks.

It is important, however, that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential.

Internet

The primary uses of school internet provision are for communication and to enhance educational resources. These take priority over any other uses.
Personal use of the internet is subject to management discretion and the following conditions:

That the use is legal.
That the use does not impinge on other members of staff's work or that of students.
That it generally takes place outside of normal school hours.
That the use is not connected to any business or profit-making venture.

Misuse of the internet may in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material or using any of the following facilities will amount to gross misconduct (this list is not exhaustive):

- accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the School and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil and whether for the employee or for the School);
- downloading or disseminating material in breach of copyright;
- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Disciplinary proceedings will be taken against any member of staff who uses the internet for illegal or obscene purposes, or for any purpose contrary to this protocol. Further guidance for staff can be found in the Code of Conduct, a copy of which can be obtained from the IntraMET. Staff should also refer to their Union's Code of Conduct.

Maiden Erlegh Trust uses filtering technology and takes all precautions to ensure that users only access appropriate material. It is not possible to guarantee that unsuitable material will be inaccessible, however. The Trust cannot accept liability for the material accessed, or any consequences of such access.

Staff will preview any recommended sites before use but any inadvertent/unintentional use of the Internet (for example, accessing an inappropriate website) must be reported immediately to the member of SLG responsible for ICT.

Staff should refrain from downloading large files during school hours unless vital for their lessons as this may affect the quality of service for other users.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

Staff may only create blogs, wikis, or other Web 2 spaces in order to communicate with students using Google Applications. If they wish to use other mediums to create user groups or discussion forums in the name of the Trust, they must get approval from the Headteacher.

A log is kept of all websites where registration of some kind is necessary for access by students or staff and checking of the compliance of such sites with appropriate legislation is the responsibility of the member of staff initially giving access. The member of staff should also check that the site used is on the list.

All users must observe software and electronic resources copyright at all times. It is illegal to copy or distribute Trust software or illegal software from other sources.

Social networking

Please see Trust Social Media Policy - here.

Email

Emails sent via the Trust network or in the context of Trust activities should not be considered private. As such they must not be used for any illegal, defamatory, or obscene purpose.

Care must be exercised when sending an email as they may commit the Trust to a binding contractual obligation notwithstanding any disclaimer which may be attached to the email.

Where email is provided, it is for academic and professional use with reasonable personal use being permitted. Personal use should be limited to short periods during recognised break times and comply with this Acceptable Use policy. The Trust's email system can be accessed from both the Trust computers and via the internet from any computer. Wherever possible, all Trust related communication must be via the Trust email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the School/Trust does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g., sensitive or personal information) will only be sent using a secure method including:
- Email encryption;
    - A secure upload portal (where by the recipient will be required to log in to retrieve the email/documentation sent);
    - Password protection on sensitive documents. The sender must ensure that the password is sent separately to the intended recipient (i.e., in a separate email or over the phone).
- Emails should not contain children's full names in the subject line and preferably, not in the main body of the text either. Initials should be used wherever possible.
- Access to school/setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g., confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).

Staff will be encouraged to develop an appropriate work life balance when responding to email. Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.

School email addresses and other official contact details will not be used for setting up personal social media accounts.

Where possible, emails must not contain personal opinions about other individuals e.g., other staff members, children or parents. Descriptions of individuals must be kept in a professional and factual manner.

Presentation

This disclaimer is automatically added to all externally sent emails.

This email and any attachments to it may be confidential and are intended solely for the use of the individual to whom it is addressed. Any views or opinions expressed are solely those of the author and do not necessarily represent those of Maiden Erlegh Trust.
If you are not the intended recipient of this email, you must neither take any action based upon its contents, nor copy or show it to anyone.
Please contact the sender if you believe you have received this email in error.
This email was sent by Maiden Erlegh Trust, registered office at Silverdale Road, Earley, Reading, RG6 7HS.
Registered in England and Wales with company number 07548754


Please consider the environment before printing this email

Email safety

The Trust gives all staff and students their own email account to use for their work. This is to minimise the risk of receiving unsolicited or malicious emails 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, if necessary, email histories can be traced. Staff should only send emails to students via their school accounts, even where students use other accounts to communicate with them.

Under no circumstances should staff contact parents or conduct any school or Trust business using personal email addresses.

It is recommended that all communication with parents is made via Bromcom Parent Portal (My Child At School) so that the communication is logged.

Never open attachments from an untrusted source; consult ICT support first.

Staff must inform the member of SLG in charge of ICT if they receive an offensive email.

Sending emails

Sending emails is not always the best way to communicate. For example, long email exchanges including multiple contributors are not efficient means of communication and certainly not of decision-making. Staff should consider other means of communication where they need the input from different people.

Keep the number and relevance of email recipients to the minimum necessary, particularly those being copied.

Staff sending emails to external organisations, parents or students are advised to retain a copy of such emails for their records. (Please see the note about MCAS below) All emails should

be written and checked carefully before sending, in the same way as a letter written on school headed paper. All emails should only be retained according to the Trust's retention policy.

Staff do not have to divulge their direct email address to parents or outside agencies and so, staff should not copy other colleagues into external emails without their permission.

Emails pertaining to students should be copied to the student communications log area of their record file.

In order to respect staff wellbeing there is no expectation that staff will be using the email system after 6.00pm weekdays or at weekends.

Emails should not be sent to stakeholders outside normal working hours, unless in an emergency.

Should you wish to send a message to all staff that is too urgent for the staff briefing/bulletin, you must request permission from a member of SLG.

Do not send or forward attachments unnecessarily and never on an urgent info from SLG email. Whenever possible, send the location path to the shared drive rather than sending attachments.

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

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

A personal reply to all staff email should not be "reply to all".

Emailing Personal, Sensitive, Confidential or Classified Information

If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, it is the member of staff's responsibility to:

Consider the potential harm of that data falling into the wrong hands.
Assess whether the information can be transmitted by other secure means before using email.

Where your conclusion is that email must be used to transmit such data exercise caution when sending the email and always follow these checks before releasing the email:

- Verify the details, including accurate email address, of any intended recipient of the information.
- Do not copy or forward the email to any more recipients than is absolutely necessary.
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone). Whilst there is a retrievable option it is not 100% effective.
- Do not identify such information (including the name of any individual) in the subject line or body of any email. We recommend you use a security classification: - Request confirmation of safe receipt.

It is strongly recommended that you send the information as an encrypted and password protected document attached to an email and provide the encryption password by a separate contact with the recipient(s).

There is a system for sending secure emails and the details of how to use this is available from ICT support.

General use of Trust equipment and network

Every user of IT is responsible for their activity, and activities they manage, on the Trust's IT equipment or network.

Information and communications held on Trust systems, hardware or used in relation to Trust business may be subject to The Freedom of Information Act or Subject Access Request and staff must ensure that all their contributions are professional.

Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files, or data. This is an offence under the Computer Misuse Act 1990.

Privately owned ICT equipment should not be used on a school network without reference to the Trust's Bring Your Own Device Protocol (info later in this document).

Any equipment issued to staff remains the property of the Trust and must be returned upon request. It is an expectation that Trust equipment issued to staff will be primarily for use in school/Trust office with the appropriate use at home. Staff are expected to bring in their devices every day and the appropriate updates applied.

Staff must report the loss, theft, or damage of any Trust equipment to IT immediately in line with the Trusts Breach procedures.

NB: The network and all internet use is monitored at a high level for all users both staff and students, and this includes all words typed and records are kept which are outside any browser history. All staff are made aware of this at their induction and at the beginning of the academic year.

Data backup and housekeeping

All files must be stored in the appropriate area on SharePoint/One Drive/Google Suite in order that files are backed up regularly. The Trust cannot be responsible for data/files only held on local computers. Staff should not save multiple copies of the same document or file.

Staff should not use the Trust platforms to store personal files of any description.

All staff are responsible for ensuring that they undertake regular housekeeping on their areas (including their email account) and that documents are archived appropriately at the end of each academic year.

If necessary, the Trust reserves the right to remove files/documents where it is necessary to create space without prior notice to staff.

No personally or sensitive material, or work related files should be stored on hard drives, USB sticks or any other devices.

Physical security

Portable equipment (including laptops, smartphones, digital cameras) must be stored securely when not in use. When carrying portable equipment in a vehicle, it must be stored out of sight in the boot at all times or the insurance is void.

Computer viruses

The Trust's PCs and network are protected against viruses.

All files downloaded from the Internet, received via email or on removable media (e.g., CDROMS, memory sticks or images from digital cameras) will be checked for any viruses using school provided anti-virus software. USB memory sticks and external hard drives cannot be connected to the network without explicit permission.

Staff must never interfere with any anti-virus software installed on Trust ICT equipment.

Staff are required to connect their device routinely to the school network in order to ensure that the anti-virus software is updated. Where this has not happened (e.g.: due to an absence) staff must go to IT Support to ensure it is updated before they recommence using the machine.

If staff suspect there may be a virus on any school equipment, they must stop using the equipment and contact IT Support immediately.

Staff leavers

If a member of staff leaves the Trust any data held on their OneDrive may be either deleted or transferred to a relevant colleague (or their manager) via an approval process.

Visitors

Visitors are not allowed to plug their hardware into the school network points (unless special provision has been made through ICT Support). Should you wish a visitor to have access to the guest network you must speak with ICT Support at least TWO working days ahead of their arrival.

Data projectors

Staring directly into the projector beam should be avoided at all times.

Standing facing into the beam should be minimized. Users especially students should have their backs to the beam as much as possible. Where interactivity is not required a remote control should be used.

Staff teaching in a room during the last lesson of the day are expected to turn the projector off. Should a teacher use a room after school they should turn it off after their session.

Staff should use the remote control to switch on/off the projector and where this is missing, they should not stand on a chair.

Heads of Department are responsible for ensuring all projectors in their classrooms have a full accessory kit, including remote controls. They must replace them immediately if lost out of their department budgets. Turn It On also review this every term.

Systems and Access

Staff are responsible for all activity on Trust systems carried out under any access/account rights assigned to them, whether accessed via Trust IT equipment or your own PC.

Staff must not allow any unauthorised person to use Trust IT facilities and services that have been provided to them.

Data security

Any attempt to bypass the Trust's or other network security systems, including the introduction of viruses or applications of a destructive nature could lead to disciplinary action or prosecution.

Staff must be conversant with the Trust's Data Protection Policy.

Apply security classification labelling to all data (see email section) and be aware that this may change over time.

Staff must not provide 2 Factor Authentication on behalf of other staff members or persons.

Senior Information Risk Owner (SIRO) and Information Asset Owner(s) (IAOs)

The SIRO/IAO is a shared responsibility between the Business Manager and the local SLG. They are responsible for:

- The information risk policy and risk assessment.
- Determining what information is held, and for what purposes.
- Determining what information needs to be protected.
- Determining who has access to the data and why.
- Determining how information is retained and disposed of.

Although these roles have been explicitly identified, the handling of secured 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.

Passwords

Passwords must not be disclosed to anyone. If an individual suspects that their password has become known to someone else, they must change the password immediately.

Staff will have to change their password to include both a number and a special character. The password will last 90 days before being prompted to change again.

Screen displays

Staff must keep their screen display out of direct view of any third parties when they are accessing personal, sensitive, confidential, or classified information (e.g.: when using IWB in classrooms).

Unattended PCs

PCs must not be left unattended whilst logged on to any system. If an individual leaves his/her PC for any duration of time, the computer should be shut down or a password system invoked by the use of a screen saver. Staff should lock their PC when moving away from it by pressing the Windows Key + L. All staff PCs will lock themselves after 10 minutes of inactivity.

In a bid to help work life balance and be green, all PCs and laptop logged on to the network and not being used after 6.30pm will automatically be shut down. This is set to 9.30pm for Parent Evening or other necessary events.

Zombie Accounts

All user accounts are disabled once the member of the Trust has left. The account will be disabled at 3.50pm on the last term day that the member of staff is in school. This may only be extended with specific permission of the Headteacher of the appropriate school. Business Managers must inform TIO that staff are leaving.

Taking of Images and Film

Photographs, videos, and students work bring our Trust to life, showcase our student's talents, and add interest to publications both online and in print that represent the Trust. We acknowledge the importance of having safety precautions in place to prevent the misuse of such material.

Staff must remember that, under UK GDPR and DPA 2018 images of students and staff will not be displayed in public, either in print or online, without consent.

The Trust is careful to ensure that images published on the Trust website cannot be reused or manipulated through watermarking and browser restrictions. Only images created by or for the Trust will be used in the public domain and students may not be approached or photographed while in school or doing school activities without the Trust's permission.

The Trust follows general rules on the use of photographs and videos of students:

Parental/student consent will be obtained and cover the use of images in:

- All Trust publications
- On the Trust website
- In newspapers as allowed by the Trust
- In videos made by the Trust or in class for Trust projects.
- Electronic and paper images will be stored securely without naming the student (with the exception of exam requirements).
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the students (ie a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only.

Students are reminded regularly (and during all off-site visits) that they should not record images of the others without their permission.

Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs or videos that are taken of them, or they are being asked to participate in.

Any photographers that are commissioned by the Trust will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the students.

Staff must never use personal digital equipment, such as mobile phones and cameras, to record images of students, staff, or governors without their express permission, this includes when on field trips.

Staff who do not wish their image to be used for Trust purposes should inform the SLG of the appropriate school in writing.

On admission to the school, all parents are asked to give permission to use images and videos of their child, as well as their work, for promotional purposes in Trust documents, displays or website/VLE materials. A list of students whose parents have not given consent can be obtained from the Main Office and is recorded on Bromcom.

Where images/work may be used external areas, i.e., exhibitions, media appearances etc then express permission will be collected separately.

Telephones (landlines and mobiles)

Telephones must not be used for any illegal, defamatory, or obscene purpose.

Personal use of telephones is acceptable, subject to the following:

- It is infrequent and kept as brief as possible and do not cause annoyance to others.
- That the use is legal
- That the use does not impinge on the work of others.
- That the use is not connected to any business or profit-making venture.
- That personal calls on landlines are limited to emergencies and other unforeseen events at the discretion of the line manager.
- Personal mobile phones should only be used discretely whilst on the school site and not in a way as to disturb others.

Health and safety – before using mobile phones in vehicles, staff should refer to the latest guidance from Health & Safety and appropriate legislation.

Disciplinary proceedings will be taken against any member of staff who uses the telephone systems for illegal or obscene purposes, or for any purpose contrary to this protocol. Staff must familiarise themselves with the Code of Conduct with regard to telephone answering and the contacting of parents which can be found in the staff handbook.

Report immediately any abusive or threatening telephone calls to a senior member of staff.

Where you have a mobile phone in school, whether a Trust or personal device, should be PIN code protected and should not be left unattended, including in vehicles.

Report the loss or theft of any Trust mobile phone equipment immediately

Trust SIM cards must only be used in Trust provided mobile phones

Staff will be required to reimburse the Trust for the cost of any personal use on your school mobile phone. This includes call charges incurred for incoming calls whilst abroad**.**

File Storage

Staff members have their own personal area on the network (OneDrive), as well as access to shared network drives (SharePoint). Any school related work should be stored on one of these drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area for example, copyright music files.

Monitoring

The Trust reserves the right to examine the content of any network work area or documents created or stored using the Trust's ICT equipment at any time. This can be done as part of our general monitoring of the use of the network, but also as part of our safeguarding monitoring. This also applies to any digital device used in school or connected to the network in any way.

High level monitoring takes place of computer/internet use by students, staff, and guests. This is done by authorised staff and may take place without any prior notice.

Disciplinary proceedings will be taken against any member of staff who uses the network or email system for illegal or obscene purposes, or for any purpose contrary to this protocol.

Authorised staff may also, without prior notice, access the email or voicemail 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 authorised ICT and SLG staff and comply with the Data Protection Act 2018, UK GDPR, 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 Trust ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Please note that the Trust reserve the right to ask a member of staff for access to their mobile and/or personal device(s) phone where the Trust thinks there may have been a use of the device which contravenes the Behaviour Policy.

Please see Annex 2 for NetSupport DNA Monitoring statement provided by the School Improvement Director: Culture and Safeguarding and Trust IT Network Manager.

Managing emerging technologies

Technology evolves constantly and new technologies are emerging all the time. The Trust will risk-assess any new technologies before they are allowed in school and will consider any educational benefits that they might have. The Trust keeps up to date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

Relevant Legislation

Line managers should be aware when managing the acceptable use of computing facilities of the following Acts and Statutory Instruments:
Communications Act 2003 (section 127)
Computer Misuse Act 1990
Copyright Designs and Patents Act 1998
Criminal Justice Act 1988
Data Protection Act 2018
Data Protection Acts 2018
Defamation Acts 1952 and 1996
Equalities Act 2010
Freedom of Information Act 2000
UK General Data Protection Regulations (UK GDPR)
Human Rights Act 1998
Malicious Communications Act 1988 (section 1)
Obscene Publications Act 1959 and 1964
Prevent Duty 2015
Protection from Harassment Act 1997
Protection of Children Act 1988
Public Order Act 1986
Race Relations Amendment Act 2000
Regulation of Investigatory Powers Act (RIPA) 2000
Sexual Offences Act 2003
Telecommunications Act 1984
The Computer Misuse Act 1990 (sections 1 – 3)

Other documents
Data Protection Policy
Privacy Notice for staff

BYOD

The Maiden Erlegh Trust (MET) recognizes the benefits that can be achieved by allowing staff to use their own electronic devices when working, whether that is at home, on campus or while travelling. Such devices include laptops, smart phones and tablets, and the practice is commonly known as 'bring your own device' or BYOD. It is committed to supporting staff in this practice and ensuring that as few technical restrictions as reasonably possible are imposed on accessing MET provided services on BYOD.

The use of such devices to create and process MET information and data creates issues that need to be addressed, particularly in the area of information security.

The Trust must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering staff to ensure that they protect their own personal information.

The Responsibilities of Staff Members

Individuals who make use of BYOD must take responsibility for their own device and how they use it. They must:

- Familiarize themselves with their device and its security features so that they can ensure the safety of the Trust's information (as well as their own information)
- Invoke the relevant security features
- Maintain the device themselves ensuring it is regularly patched and upgraded
- Ensure that the device is not used for any purpose that would be at odds with the Trust's Policy on the Use of ICT

While Trust's IT staff will always endeavour to assist colleagues wherever possible, the Trust cannot take responsibility for supporting devices it does not provide.

Staff using BYOD must take all reasonable steps to:

- Prevent theft and loss of data
- Keep information confidential where appropriate
- Maintain the integrity of data and information, including that Trust sites
- Take responsibility for any software they download onto their device

Staff using BYOD must:

- Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device
- Set up remote wipe facilities if available and implement a remote wipe if they lose the device
- Not hold any information that is sensitive, personal, or confidential on personally owned devices. Instead they should use their device to make use of the services that the Trust offers allowing access to information on the Trust services securely over the internet. More information on determining if information is 'confidential' is available.
- Where it is essential that information belonging to the Trust is held on a personal device it should be deleted as soon as possible once it is no longer required. This includes information contained within emails
- Ensure that relevant information is copied back onto the Trust systems and manage any potential data integrity issues with existing information

- Report the loss of any device containing Trust data (including email) to the DPO.
- Be aware of any Data Protection issues and ensure personal data is handled appropriately.
- Report any security breach immediately to the DPO in accordance with the AUP
- Ensure that no Trust information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of/sold/transferred to a third party

The use of camera, microphone and/or video capabilities are prohibited whilst in School unless this has been approved by SLG. If approved, any pictures, videos or sound recordings can only be used for School purposes and cannot be posted or uploaded to any website or system outside of the Trust network.

You must not use your device to take pictures/video/recordings of other individuals without their advance written permission to do so.

All staff who wish to use their own devices to access the Trust's network must sign and return the statement at the conclusion of this policy.

When in Trust sites, staff should connect their device via the Trust's wireless network for security.

When out of Trust sites, staff should access work systems on their mobile device using secure connections.

Monitoring and Access

The Trust will not routinely monitor personal devices. However, the Trust does reserve the right to:

- Prevent access to a particular device from either the wired or wireless networks or both
- Prevent access to a particular system
- Take all necessary and appropriate steps to retrieve information owned by the Trust
- All internet access via the network is logged and as set out in the Acceptable Use policy, employees are blocked from accessing certain websites whilst connected to the Trust network.

Non-acceptable Use

Any apps or software which are downloaded onto the user's device whilst using the Trust's own network is done at the users risk and not with the approval of the Trust.
Devices may not be used at any time to:

- Store or transmit illicit materials;
- Store or transmit proprietary information belonging to the School;
- Harass others;
- Act in any way against the School's Acceptable Use policy and other safeguarding and data related policies.
- Technical support is not provided by the Trust on the user's own devices.

Data Protection and BYOD

The Trust must process 'personal data' i.e. data about identifiable living individuals in accordance with the Data Protection Act 2018 and UK GDPR. Sensitive personal data is information that relates to race/ethnic origin, political opinions, religious beliefs, trade union membership, health (mental or physical) or details of criminal offences. This category of information should be handled with a higher degree of protection at all times.

The Trust, in line with guidance from the Information Commissioner's Office on BYOD recognizes that there are inherent risks in using personal devices to hold personal data. Therefore, staff must follow the guidance in this document when considering using BYOD to process personal data.

A breach of the Data Protection Act and GDPR can lead to the Trust being fined. Any member of staff found to have deliberately breached the Act may be subject to disciplinary measures, having access to the Trust's facilities being withdrawn, or even a criminal prosecution.

Disclaimer

The Trust will not monitor the content of the user's own device but will monitor any traffic over the Trust system to prevent threats to the Trust's network.

The Trust reserves the right to disconnect devices or disable services without notification.

The employee is expected to use his or her devices in an ethical manner at all times and adhere to the Trust's policy as outlined above.

The employee is personally liable for all costs associated with his or her device.

The Trust reserves the right to take appropriate disciplinary action up to and including summary dismissal for non-compliance with this policy.

ANNEX 1: Artificial Intelligence Staff

Background

Although Data Protection law does not specifically define or discuss the guidelines for Artificial Intelligence ('AI'), the guidance from the Information Commissioner's Office and the UK government defines it as using non-human systems to imitate human intelligence.

In this time of constant development and increased usage, there is a need to provide staff with guidelines for use and to recognise an employer's right to monitor such usage. We have also set out expectation on AI usage by pupils.

Introduction

The use of AI is transforming the way individuals are working. Informed and responsible use of AI has the potential to increase efficiency and improve decision making.

With these benefits come potential risks, including data protection breaches, the protection of confidential information, ethical considerations, and compliance with wider legal obligations.

We permit all Trust schools for using AI.

We permit the use of informed and responsible use of authorised AI applications by staff, in carrying out specific and authorised tasks. This policy must be complied with when using AI to carry out such tasks.

The purpose of this policy is to set out our rules on the use of AI in the workplace and how it should be adopted by staff to ensure we maximise the benefits of AI while minimising any risks or concerns.

Where personal data is used with AI applications, an ICO risk assessment and/or data protection impact assessment ('DPIA') has been carried out to ensure transparency in how AI will be used and what mitigating steps have been taken to reduce any potential risk of harm to pupils, staff and any other data subjects whose data might be shared with the authorised systems.

This policy covers all employees, officers, consultants, contractors, volunteers, interns, casual workers and agency workers.

Pupil usage of AI

As part of this policy, staff should be aware of how the Trust permits limited pupil usage of AI applications in accordance with the AI policy for pupils. It is important to monitor pupil usage whilst in class and for homework to ensure compliance with this policy or how to monitor when reviewing homework.

For pupils, they must sign an Acceptable Use Statement to ensure appropriate usage of AI and they are reminded of the permitted usage along with an outline of what classes as AI misuse.

The school permits pupil usage of AI in the following circumstances:

- As a research tool
- Idea generation for projects
- For use with coursework or homework with the above requirements fulfilled
- Examples of AI misuse include, but are not limited to, the following:

- Copying or paraphrasing sections of AI-generated content so that the work is no longer the pupil's own;
- Copying or paraphrasing whole responses of AI-generated content;
- Using AI to complete parts of the assessment so that the work does not reflect the pupil's own work, analysis, evaluation or calculations;
- Failing to acknowledge use of AI tools when they have been used as a source of information;
- Incomplete or poor acknowledgement of AI tools; or
- Submitting work with intentionally incomplete or misleading references.

Authorised AI applications

The school allow access to the following AI applications for business purposes.

The listed AI applications may be updated at any time. Should staff wish to use an AI application, they must contact the Head of Trust Operations to review permission to do so.

Authorised usage of AI for staff

Authorised AI applications must only be used by staff for the following business purposes:

- Drafting internal guidance, training and presentations;
- Lesson planning
- Conducting research
- Developing code
- Providing summaries
- Idea generation

All other purposes must be authorised in advance the Head of Trust Operations or School Business Manager.

Before using any AI applications, staff will be provided training to ensure human reviewers (those who conduct monitoring of these applications) have a correct understanding and do not add any bias into the AI systems.

Data Privacy

The Trust are yet to permit or encourage the usage of AI to process personal data at this time but are aware of the data protection responsibilities to be transparent of such usage and will update the policy as and when needed.

Monitoring

We reserve the right to monitor all content on any AI applications used for business purposes. This will only be carried out by the school to comply with a legal obligation or for our legitimate business purposes, in order to:

- prevent misuse of the content and protect confidential information (and the confidential information of our pupils, staff or other stakeholders);
- ensure compliance with our rules, standards of conduct and policies in force;
- monitor performance at work;
- ensure that staff do not use AI for any unlawful purposes or activities;
- comply with legislation for the protection of intellectual property rights;

The Trust will also conduct monitoring under our IT and Communications Systems policy and Bring Your Own Device to Work policy.

Breach of this policy

Breach of this policy may, where appropriate, result in disciplinary action up to and including dismissal or termination of your employment or engagement with us.

Where disciplinary action is appropriate, it may be taken whether the breach is committed during or outside normal hours of work and whether or not use of AI is on an individual's own device or one of our devices, and whether at home, in the office or from a remote working location.

You are required to assist with any investigation into a suspected breach of this policy. This may involve providing us with access to AI applications and any relevant passwords and login details.

You must report any breach of this policy immediately to your line manager, the School Business Manager or Head of Trust Operations in the first instance. We advise referring to the Trust's current data breach policy which can be found on the IntraMET.

Related Policies

Staff should refer to the following policies that are related to this AI Staff Policy: -

Diversity, Equity and Inclusion Policy
Code of Conduct and Ethics Policy
Data Protection Policy
Privacy Policy for staff.
IT and any related communications policies

These are available on the Trust IntraMET.

Staff Agreement

I have read and understood the Staff Acceptable Use Procedure for Maiden Erlegh Trust.

I confirm that I will comply with the terms of the Bring your own Device policy when using my mobile/own device to access the Trust network.

I understand that should I be found in breach of the Acceptable Use Procedure I may be liable to disciplinary procedures and, if appropriate, the Police and local authorities may become involved.

I accept that it is my responsibility to be aware of amendments to this Acceptable Use Procedure.

Staff Name		**USE BLOCK CAPITALS**
Staff Signature		
Date *DD / MM / YY*		

ANNEX 2: NetSupport DNA Monitoring

Online safety and effective monitoring are key features of KCSiE.

NetSupport DNA is the tool used by Maiden Erlegh Trust to ensure that the internet is used safely in all our schools.

This piece of software is constantly monitoring activity on all PC's as well as internet traffic. All activity is cross referenced against a bank of URLs and a glossary of words and phrases that could be a cause for concern. These are regularly updated and reviewed by NetSupport as well our inhouse network management team.

When an alert is triggered by a pupil/student, an email is sent to the Designated Safeguarding Lead.

When an alert is triggered by a member of school staff, an email is sent to the Headteacher.

When an alert is triggered by a member of Central Services staff, an email is sent to the CEO.

All alerts will be assessed for risk and any that are judged to be safeguarding concerns will be followed up.

For online activity that contravenes the Acceptable Use Policy and/or the Staff Code of Conduct, the relevant Trust polices will be followed. This could lead to sanctions up to and including Permanent Exclusion (for a child) and Dismissal (for a member of staff). If necessary, the police and local authorities will be informed.

For questions about in-school monitoring, please contact your headteacher; for general questions about safeguarding contact the School Improvement Director: Culture and Safeguarding; and for technical questions contact the Trust IT Network Manager.