MAIDEN ERLEGH TRUST

ACCEPTABLE USE OF DIGITAL TECHNOLOGY

FOR STAFF

May 2019 (review May 2021)

MAIDEN ERLEGH TRUST

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 GDPR and 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.

Contents

1. Aims

The aims of this protocol are:

- **To ensure users of IT facilities are clear about what is acceptable and what is unacceptable.**
- **To reduce security threats.**
- **To encourage effective and positive use of resources.**
- **To shield the school against potential liability.**

2. 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

3. 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 eg: 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 to the Child Protection Lead as soon as they become aware of it.

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

We also educate 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.

4. 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 places outside of normal school hours.
- That the use is not connected to any business or profit making venture.

The Trust also specifically excludes the following uses of the Internet:

- To view content of an obscene or discriminatory nature or in violation of UK legislation.
- To download unofficial software for use on the Trust's equipment.
- To engage in on-line gambling or gaming.
- To access information to which they are not authorised.
- To spread or publish any political or threatening views or content that could cause unrest.
- To access any materials, sites or social networks which promote extremist views or calls for death of members of our armed forces, whether in this country or overseas

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 Business Manager. Staff should also refer to their Union's Code of Conduct.

Maiden Erlegh Trust, in conjunction with Wokingham LA, uses sophisticated 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

5. Social networking

At present, the Trust endeavours to deny access to most social networking sites to students via the school network, though it cannot block access via 3G/4G enabled devices, or networks run by third parties (eg: youth club).

Through the ICT and Personal, Spiritual, Moral, Social and Cultural (PSMSC) Education all students are advised to be cautious about the information given by others on social networking sites. This is reinforced through our general use of ICT across the curriculum.

Key messages are that they should:

- Not give out personal details or post images of themselves or others which may enable third parties to identify them or where they are. This may put them or others in danger.
- Pay due care when uploading images of themselves or others. Once images or words are posted online, it is extremely difficult to remove them and so.
- Set and maintain profiles to maximum privacy and deny access to unknown individuals.
- Be aware that they can never be certain who is communicating virtually with them.
- Be wary about publishing specific and detailed private thoughts.
- Never publish any material, chat or comment which might be construed as bullying, harassment, prejudicial, criminal or extremist.
- Never publish material which brings the reputation of an individual or the Trust into disrepute.
- Report any incidents of bullying, harassment, grooming or radicalisation to the school and, where necessary, to the companies running the sites and/or the police.
- Where we are made aware that a member of the school community has posted comments or images on social networking sites which are offensive, bullying or inappropriate we will deal with it in line with the relevant disciplinary policy and work with the organisations involved to endeavour get any posts removed (this includes the police where necessary).

Parents are given information about how to keep their child safe on the internet and reminded that the school cannot control what students do on the internet outside the school day.

Staff should be particularly careful when using social networking sites to ensure that any material or comments uploaded to a site does not bring the Trust into disrepute in any way.

Appropriate privacy settings should be used to prevent access to personal details. Staff must not give students access to their personal pages for their own protection (including stakeholders who have left the school but may still have contacts within it), nor should they message or respond to messages on social media by students.

Staff must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience. This includes revealing names of colleagues or partner professionals.

Any Twitter account associated with the Trust, its schools or departments should only follow educationally linked accounts. No personal accounts, will be followed. Tweets will not compromise personal or professional reputations or the reputation of the Trust. The Trust regularly reviews Twitter accounts and reserves the right to remove accounts if they contravene this policy.

Where possible messaging/commenting facilities should be turned off. Conversations should not take place on social media.

Department or private staff accounts on twitter should not follow current or ex-student accounts. Exceptions may be made for ex-students should the follow be educationally linked but this must be checked by the member of SLG in charge of ICT.

6. 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.

Personal use of email is acceptable, subject to the restrictions placed on the use of the internet.
In addition emails must not:

- Contravene the Trust's Equality Policy and Code of Conduct.
- Disclose confidential, political or threatening information, or any information that might cause unrest.
- Be "chain letters"
- Include indecent humour or images.
- Be used to distribute advertisements to staff e.g. items for sale etc, or to send personal emails containing photos and video clips.

<u>Presentation</u>

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

<u>Email safety</u>

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 SIMS InTouch 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 SIMS InTouch 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 the 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 ten 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.

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:

1. Consider the potential harm of that data falling into the wrong hands
2. 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)
- 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.

7. 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 (see separate 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 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 the Assistant Headteacher responsible for IT immediately in line with the Trusts Breach procedures.

Note that 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.**

<u>Data backup and housekeeping</u>
All files must be stored in the appropriate area on a network drive 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 on the network.

Staff should not use the network 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. Media files should be archived as soon as they are no longer used and no more than 10 photos per event and 1 short video should be stored at any one time.

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 should be stored on hard drives, USB sticks or any other devices.

How the network drives are used is contained within the document Introduction to ICT at MET.

NB: HODs and SLG are responsible for keeping portable hard drives with archived material on them securely in the department. They should never be taken off site.

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. CD-ROMS, 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 (eg: 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 home drive (N:) should be either deleted or transferred to a relevant colleague (or their manager).

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 <u>not</u> 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.

8. 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.

9. Remote Access

Staff must protect Trust information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment.

They must only use equipment with an appropriate level of security for remote access.

To prevent unauthorised access to Trust systems, keep all information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone.

10. 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.

<u>Senior Information Risk Owner (SIRO) and Information Asset Owner(s) (IAOs)</u>
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 off

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 be 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.

Staff must ensure that their password to log on to the Trust system is different to that for SIMS.

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 (eg: 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 15 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.

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.

11. 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 GDPR and Data Protection Act 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.
- 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 recorsed on SIMS.

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

12. Telephones (land-lines 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 land-lines 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.

13. 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 1998, 2018, 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 phone where the Trust thinks there may have been a use of the device which contravenes the Behaviour Policy.

14. 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.

15. 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 1994,1998, and 2018
Defamation Acts 1952 and 1996
Equalities Act 2010
Freedom of Information Act 2000
General Data Protection Regulations 2018
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
BYOD Procedure
Data Protection Policy
Introduction to ICT at MET 2019
Privacy Notice for staff

Staff Agreement

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

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 Network Logon ID *		*** USE BLOCK CAPITALS**

Staff Signature		**Date**	DD	MM	YY