Policy and Procedure: Staff Agreement for Acceptable Use of ICT (including Internet, email and social media policy)

Version:	v 1.0
Author:	Alan Evans, Director of Finance and Operations Mel Wellard, Head of Governor Services
Date:	8 September 2016
Date of Board Approval:	to be confirmed
Review date:	September 2019

Eastern Multi-Academy Trust and its Academies, (referred to as "The Trust") hold and use information that is both confidential and valuable. Such information and the computer systems that store, process and transmit it must be adequately protected against any activity that could affect authorised and lawful use.

It is also important that the use of ICT resources is regulated, to ensure that the Trust complies with relevant legislation, regulatory codes of practice, its own governance arrangements and ICT & Information Security best practice. This policy has been developed to set standards and provide users with clear instructions and guidance on what constitutes acceptable and unacceptable use.

In brief, the aims of the Acceptable Use Policy (AUP) are to:

- Protect Trust staff, the Trust's equipment and the information assets held
- Prevent the abuse or misuse of computer, internet, e-mail facilities and paper files
- Prevent information security incidents and/or information loss and breaches
- Ensure compliance with legislation

This policy should be read in conjunction with the Trust's e-safety and Staff Disciplinary policy and the Teachers' Standards.

KEY MESSAGE

All staff must be aware of their obligations under this policy and take reasonable action to ensure on-going compliance.

As a condition of use, it is the responsibility of users to ensure that they keep up to date with the latest requirements of the policy

1 WHO DOES THIS ACCEPTABLE USE POLICY APPLY TO?

This policy and any references to 'the Trust' or 'users' refer to, but are not limited to, teachers and all other Trust staff, agency workers, contractors, third parties and temporary staff such as work placements.

1.1 Responsibilities of the Chief Executive and Principals

The Chief Executive and Principals will support this AUP by:

- Implementing the Policy within the Trust and ensuring that the AUP is circulated to all personnel
- Ensuring that staff understand the legal risk and security implications of improper use of Trust ICT facilities
- Promoting best practice in terms of security and data protection
- Defining within the Senior Leadership Team the acceptable level of personal use for Trust and personally owned hardware such as mobile phones and facilities such as personal email accounts etc.

The Chief Executive and Principal will ensure that the ICT facilities are configured and operated appropriately to protect the information held within or accessed by them. Guidance on the use of Cloud Services, 'Bring Your Own Device' and End User Devices (PCs, Laptops, Tablets, Smartphones, etc.) is available in *Appendix 1*

2 PRIVACY, MONITORING & FILTERING

2.1 Right to Privacy

Workplace email should not be used for private or personal purposes. Please be aware that if for any reason it is, the Trust cannot ensure privacy is maintained due to the inability to differentiate these emails during monitoring processes.

2.2 Monitoring

The Trust will not generally engage in systematic monitoring and recording activities. However, it reserves the right to do so where there is reason to believe that misuse of its information assets or computing facilities is occurring.

Nevertheless, the Trust maintains the right to examine any systems and inspect any data recorded in those systems. In order to ensure compliance with this policy, the Trust also reserves the right to use monitoring software in order to check upon the use and content of emails.

KEY MESSAGE

Any individual using the information assets or computing facilities of the Trust consents to such monitoring and recording. If apparent criminal activity is detected, monitoring logs, in conjunction with specific personal information, may be provided to the Police.

2.3 FILTERING

All Trust internet services are automatically filtered to ensure that inappropriate and unauthorised content is minimised as far as is possible without detracting from its service.

3. INTELLECTUAL PROPERTY

The Trust owns the copyright for any information produced. Copyright may also be assigned or transferred to an individual or organisation by the original owner(s). All information is stored within the ICT facilities of the Trust and may be accessed at any time where there is a need to ensure compliance with legislation and internal policy.

4. 'SENSITIVE INFORMATION'

The term 'Sensitive Information' is used in a variety of contexts and can have different meanings according to the relevant legislation or usage.

In the context of this Acceptable Use Policy, 'Sensitive Information' includes any information which requires protection from unauthorised or unwanted loss or disclosure. This will typically include, but is not limited to:

- Personal Data (including pupil records, staff records, appraisals, disciplinary cases, etc.);
- Sensitive Personal Data (for example, health records);
- Bank and Payment Card information;
- Commercial data, leases, contracts, etc.;
- Information marked as 'OFFICIAL – SENSITIVE';
- Any information where loss or disclosure could lead to damaging consequences for an individual or group of individuals; damage the reputation of the Trust, compromise ICT security or cause the Trust to not fulfil its statutory obligations.

Section B

Statements and procedures

5 GENERAL PRINCIPLES

The Trust's ICT Facilities must only be used by those authorised to do so. Any user who requires access to Trust ICT Facilities must first:

- Be authorised to do so

- Read, understand and accept all relevant Trust policies, including this Acceptable Use Policy
- Sign and return the confirmation of Acceptable Use Policy – shown in Annex 1

No user must deliberately or knowingly use the Trust's ICT facilities to view, copy, create, download, share, store, print, e-mail, transfer or otherwise access any material which:

- is sexually explicit or obscene
- is racist, sexist, homophobic or in any other way discriminatory or offensive
- contains content where the possession, transmission or sharing of would constitute a criminal offence
- promotes any form of criminal activity
- brings the Trust into disrepute or exposes it to legal action

It is unacceptable to use the Trust's ICT facilities to:

- Conduct any non-approved business
- Undertake any activities detrimental to the reputation of the Trust
- Make offensive or derogatory remarks about anybody on social media or otherwise via the Internet or e-mail
- Create, transmit, download or share information which would breach copyright, confidentiality or any other applicable legislation
- Impersonate or attempt to impersonate another individual or organisation
- Attempt to gain access to information or information systems any user is unauthorised to access
- Attempt to bypass internet filtering or any monitoring functions
- Attempt to conceal a user's identity by using anonymising software or services
- Deliberately or knowingly undertake activities that corrupt or destroy Trust data, disrupt the work of others, deny network resources to them or violate the privacy of other users

5.1 Trust Representation and Conduct

- When using the computing facilities of the Trust you must act in accordance with any Trust policies to help the Trust maintain a reputation for quality and integrity.
- Employees, who are aware of any impropriety, breach of procedure, unlawfulness or maladministration, should report this to the Chief Executive, Principal or line manager. where it asks the user to save their password;
- The user must not store their username, password or other credentials within any website including web based email accounts such as Yahoo or Gmail;
- The user must not attempt to access or make use of any username or email address that is not their own;
- The user must not attempt to impersonate anyone else;
- The user must not leave their PC unlocked and ensure that they lock their PC before leaving their desk.

KEY MESSAGE

Communicating with both current and former pupils via social networking sites and via other non-Trust related mechanisms such as personal emails and text messaging can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.

Communication between pupils and adults, by whatever method, should take place within clear explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, emails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to pupils including email, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. Email or text communications between an adult and a child/young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

7 USE OF TRUST ICT EQUIPMENT

Any equipment supplied to a user (for example, Laptops, PCs, Smartphones, Tablets) remains the property of the Trust at all times, with the user assuming temporary "custodianship".

Do's

- Make sure that at all times that this equipment is used appropriately, securely, for the purpose for which it was issued to you, without reconfiguration and in compliance with relevant legislation such as the Computer Misuse Act 1990 and Data Protection Act 1998;
- On leaving the Trust, the user must ensure that all ICT equipment is returned;
- Before the user stores any films, music or other media on ICT equipment, they must ensure that they are aware of their responsibilities under current Intellectual Property Legislation. Report the loss or theft of ICT Equipment to your Trust

7.1 Laptop, Tablet and Smartphone Users (for use on Trust premises and offsite remote working)

All Trust ICT equipment is subject to information security risks, but the portability of laptops, tablets and smartphones makes them particularly vulnerable to damage, loss or theft, either for their re-sale value or the information they contain. When outside of secured premises, there is an increased risk to any laptops or portable devices that a user may carry as part of their role.

Do's

- Users must keep ICT equipment in their possession within their sight whenever possible. ICT equipment should never be left visibly unattended unless it is suitably secured (for example in a secure office)
- Extra care should be taken in public places such as airports, railway stations or restaurants
- The user must ensure that the device is regularly connected and logged onto the network to receive its security updates at least monthly
- Any data saved to the device is not backed up centrally. The user should avoid saving data to the device wherever possible. However, where this is necessary for operational reasons the user must ensure that data on the device is backed up to the network storage areas for the Trust as soon as is practical.

Don'ts

- If a device is secured either with an encryption password or a 'lock screen' password, the user must not share your encryption / lock screen password with anyone or write this down.

7.2 Personal use of Trust Equipment and ICT Facilities

Any personal use must not, in any way, distract staff from the effective performance of their duties. Improper or inappropriate personal use of the Trust's e-mail and Internet systems may result in disciplinary action.

Trust devices contain or enable access to Trust data and systems. Personal use of Trust ICT equipment does not extend to other family members, friends or any other person, unless they are formally authorised to do so.

7.3 Secure Disposal of Trust ICT Equipment

Trust equipment which is broken, no longer fit for purpose or to be used/donated for other purposes should be returned to the IT department where it will be securely wiped (where applicable) and disposed in-line with EE regulations.

Don'ts

- The user must not sell or donate Trust equipment to staff, charities or any other third-parties without the explicit authorisation of the Chief Executive or Principal.

8 USE OF PERSONAL AND NON TRUST ICT EQUIPMENT

The use of non-Trust and personal ICT equipment to undertake Trust business brings both opportunities and risks. The potential for an increase in flexibility and convenience must be balanced against the need to keep personal and sensitive information secure.

- The user must only use their personal hand held/external devices (mobile phones/USB devices etc.) to undertake Trust business in school if permission has been gained. Employees must understand that, if they do use their own devices in school, they will follow the rules set out in this agreement, in the same way as if they were using Trust equipment
- Users must keep personal phone numbers and email accounts private and not use their own mobile phones or email accounts to contact pupils
- Users must only use a Trust mobile phone to undertake Trust business when on a Trust trip other than in emergencies

9 SHARING, SENDING AND STORING INFORMATION

9.1 Information Classification

During the course of its business the Trust sends and receives large quantities of data. Not all of this will be personal or sensitive, but if a user handles (creates, sends, receives, etc.) such data, then they need to be aware of how to look after it.

Some information may be labelled with a 'classification' (e.g. Sensitive, Confidential) which identifies how sensitive it is. However, much of the information a user handles will not be labelled.

KEY MESSAGE

You will need to use your professional judgement, in conjunction with available guidance, practice and processes to ensure that you are aware of the sensitivity of the information you work with. Any sensitive information must be handled (sent, stored, etc.) appropriately)

9.2 Using e-mail to send sensitive information

Do's

- You must use appropriate technology to encrypt or otherwise protect e-mail containing sensitive information if you are sending it outside of the Trust.

9.3 Using Removable Media to store sensitive information

Removable Media can be a convenient way to store and share information.

Do's

- Ensure that all files on the removable media are also stored on Trust shared drives or within ICT Systems - removable media can be lost or damaged;

Don'ts

- Do not store sensitive information on removable media that is not encrypted (for example, standard USB Memory Sticks, CDs, tapes and SD cards);

KEY MESSAGE

Removable media includes:

- CDs and DVDs
- USB memory sticks and external hard drives
- Memory cards (e.g. SD cards) and SIM cards
- Digital cameras, MP3 players
- Backup tapes, audio cassettes

9.4 Cloud Services

The terms 'Cloud Services' or 'The Cloud' cover a number of technologies which provide access to software, applications, data and ICT infrastructure (typically) over the Internet. For example, services such as Dropbox offer file storage; Office 365 allows access to e-mail and Microsoft Office applications.

The UK Government and the Information Commissioner's Office have issued guidance about the use of 'Cloud'. Links to this guidance can be found in Appendix 1.

Do's

- Make use of Cloud-based technologies approved by the Trust for sharing information and collaborating;

Don'ts

- A user must not store any sensitive Trust information in a Cloud Service which has not been formally assessed and approved by the Trust for that purpose.

KEY MESSAGE

Remember that the General Principles outlined in Section 5 of this document apply when you are using the internet, email or social media

10 INTERNET, EMAIL AND SOCIAL MEDIA POLICY

The internet, e-mail and social media are all important channels used by the Trust to share, publicise and access information.

10.1 e-mail

Do's

- If users receive e-mail not intended for them, notify the sender and then delete the original.

Don'ts

- Users must not use, disclose, distribute, copy, print or forward any information contained in an e-mail which has been sent to you in error;
- If a user receives an e-mail from an unknown source ('Spam' e-mail) they must not open any attachments or click on any links. They should neither forward the e-mail nor reply to the sender (as this may attract further e-mails).

10.2 Social Media

Although this Acceptable Use Policy applies to the use of Trust facilities, it is important to note that the use of Social Media outside of work can affect the workplace. For example, comments posted on Social Media may be seen by work colleagues, and a private disagreement may 'spill over' into the workplace;

Do's

- Follow the General Principles outlined in Section 5 of this document.

Don'ts

- A user must not use social networking sites to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages.
- A user must not befriend pupils on social networking sites. (Staff should consider carefully the implications of befriending parents or ex-pupils);
- A user should not post information and photos about themselves, or Trust-related matters, publicly that they wouldn't want employers, colleagues, pupils, parents and other Trust stakeholders to see;

11 SECURITY INCIDENTS

Security Incidents, for example the theft of a laptop, a computer virus or a successful hacking attack could compromise the security of Trust data. A successful compromise may:

- affect business operations and lead to financial loss or reputational damage
- be a threat to the personal safety or privacy of an individual;
- need to be reported to the UK Government, the Information Commissioner's Office, the Police or a number of other organisations.

Do's

- as a user ensure report all security incidents to the Trust

Don'ts

- Don't ignore a security incident assuming that someone else will report it

Section C

Additional Information & Guidance

APPENDIX 1 – Guidance

Information Commissioner's Office
Guidance on the use of Cloud Computing
Bring Your Own Device Guidance

UK Government
End User Device Guidance
Bring Your Own Device Guidance

CURRENT LEGISLATION

- The Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Computer Misuse Act 1990
- Copyright Design and Patents Act 1988
- Protection of the Children Act 1978

APPENDIX 2 – Examples of Security Incidents

- Damage to or theft/loss of information (either manual or electronic)
- The finding of confidential information/records in a public area
- Poor disposal of confidential waste
- Unauthorised access to information
- Unauthorised disclosure of confidential information to a third party (in any format including verbally)
- Transfer of information to the wrong person (by email, fax, post, or phone)
- Receiving of information (such as by email or fax) meant for someone else
- Sharing of computer IDs and passwords

- Loss or damage to paper based files containing sensitive or personal identifiable information
- Loss of computer equipment due to crime or an individual's carelessness
- Loss of computer media e.g. CD, USB stick
- Corrupted data
- Access to inappropriate websites in breach of policy
- Theft
- Fraud
- A computer virus
- Successful hacking attack

APPENDIX 3 – Passwords: Good Practice

- **Choose a password that cannot easily be guessed – avoid using the names of children, partners, pets, car registration numbers or favourite football/rugby teams. This is information that could relatively easily be uncovered by social engineering techniques, looking at the electoral register, etc.**

- **Some passwords are easy to discover or 'crack' using simple techniques known as Dictionary or Brute Force attacks:**

- **Avoid using a word with a number or symbol at the end. E.g. Password1 or Warrington! – these are very easy to discover using simple tools or techniques;**

- **Don't use a lot of repeating letters or numbers, these again are easy to discover: Joe111111;**

- **If you want to use a word to make the password easy to remember, you could replace letters with numbers and symbols: for example F1$h&Ch!ps**

Annex 1 – Staff Agreement

Staff Obligations in relation to the Acceptable Use of ICT -

To ensure that members of staff are fully aware of their professional responsibilities when using ICT systems and equipment, staff are required to sign this document.

Members of staff must read and understand the Trust's e-safety and social media policy (contained with the Acceptable Use of ICT policy) prior to signing.

I understand that the Trust's ICT equipment is the property of the Trust whether used on or off the premises.

I understand that the Trust's ICT systems and services must be used in accordance with Trust policies whether used on or off the premises.

I understand that it is a disciplinary offence to use any Trust ICT system, services or equipment for a purpose not permitted by the Trust. This includes (but is not limited to)

- conducting illegal activities,
- accessing or downloading pornographic material,
- political purposes,
- gambling,
- soliciting for personal gain or profit,
- managing or providing a business service using the Internet,
- advertising,
- revealing or publicising proprietary or confidential information,
- representing personal opinions as those of the Trust, or saying to speak on behalf of the Trust,
- making or posting indecent remarks or proposals,
- sending chain letters,
- using software in violation of its copyright,
- Illegal downloading from torrent sites (copyright music and films etc.)
- intentionally interfering with the normal operation of Trust Internet services,

Learning Platform services, Management Information System, hardware or software.

(Staff are permitted to browse the internet and undertake activities such as online shopping during non-contact time (teachers) or designated breaks (support staff)).

I understand that my use of Trust systems, software, Internet and email is monitored and recorded to ensure policy compliance. Where the Trust believes that unauthorised use of equipment, systems or services may be taking place, it may delete inappropriate materials and may take disciplinary action. Where the Trust believes that equipment, systems or services may be being used for unlawful or criminal purposes this may be referred to the appropriate agency.

I understand that ICT includes a wide range of systems, includes but it not limited to: - mobile phones, PDA's, digital cameras, email and social networking. ICT use may also include personal ICT devices with the permission of the Principal if used for Trust business.

I understand that I must not communicate with current students of the Trust via public social networking sites (e.g. Facebook, Twitter, Instagram) and that if contact with students is required, I must use Trust-owned equipment or facilities (e.g. the email facility on the Learning Platform or a phone provided by the Trust).

I understand that my use of social networking sites (e.g. Facebook, Twitter, Instagram) should be for personal use only; however should there be a requirement to use Social Media for Trust purposes then my usage will be consistent with my professional role. All communication with parents of students at the Trust should be conducted using Trust-owned equipment or facilities (e.g. the email facility on the Learning Platform or a phone provided by the Trust).

I understand that my use and storage of photographic images or video recordings of pupils taken in Trust or on Trust activities should be with parental/student consent.

I understand that any official Trust blogs, wikis, discussion boards etc. should be hosted on the Trust's website or Learning Platform.

I will respect and abide by all copyright and intellectual property rights.

I will respect system security and I will not disclose or share any login, password or security information to anyone other than an authorised system manager.

I will ensure that all Trust electronic communications that I make are compatible with my professional role and Trust policies and will not use inappropriate humour, graphics or images.

I will seek to ensure that I check my email inbox each working day and deal with emails promptly.

I will seek to produce appropriate distribution lists and/or give appropriate subject descriptions to internal emails to prevent colleagues from having to deal with emails that

do not concern them.

I will maintain my user area(s) in good order whether on a laptop or on networked computers or other devices.

I will ensure that students are appropriately supervised when using ICT equipment and remind them that their ICT activity is routinely monitored.

I will take all steps necessary for the protection of both IT and information whilst it is in my possession and I will also ensure that I either log off my computer or apply the screen lock should I need to leave the computer for any reason.

I will ensure that personal data is stored securely and is used appropriately, whether in Trust, taken off the Trust premises or accessed remotely. I will ensure that personal or confidential information is not stored on any computers not belonging to the Trust or on removable media, such as memory sticks, CDs, DVDs except for the purpose of transfer of data from one Trust's computer to another Trust's computer. I will ensure that no personal data is copied unless there is a specific requirement to do so.

I understand that computers provided by the Trust for use away from the Trust premises may be used for personal purposes provided that any usage does not constitute a breach of this or any other Trust policy or Code of Conduct.

I will not install any software or hardware without authorisation by the Principal or Trust's Director of Finance and Operations.

If using a computer provided by the Trust away from Trust premises, I will ensure that appropriate physical security measures are in place to safeguard the equipment. I will also ensure that any anti-virus protection software is updated prior to leaving the Trust.

I will report any information breach and/or security incidents of concern relating to the inappropriate use of ICT systems or equipment to the ICT Coordinator, e-Safety coordinator, the Designated Child Protection coordinator or Principal.

I have read, understood and accept the obligations outlined above for Acceptable Use of ICT.

Name: ……..……. Signed: ……..…… Date: ……

Please sign and return to Sandra Harvey