JMAT
020

John Milton Academy Trust

ICT Policy

(GDPR Compliant)

History of Document

Issue No	Author/Owner	Date Written	Reviewed by Trust on	Comments
001	CEO	June 2018	20th July 2018	

Contents

This policy applies to each school in the Trust and is directed to all staff working in the school - teaching and support (both permanent and temporary) and also to visitors or volunteers who may use ICT equipment or require access to the system.

There are separate documents for students and parents/carers.

1. Rationale

The information communication technology (ICT) facilities and information resources in all schools remain the property of the school and the Trust and not of particular individuals or teams. By following this policy all staff will help ensure that ICT facilities are used:

- legally;
- securely;
- effectively;
- in a spirit of co-operation, trust and consideration for others;
- without adverse consequence for the school and Trust;
- correctly, so that the systems and technology can be maintained.

Although this policy relates to all ICT facilities and services provided by schools in the Trust, special emphasis is placed on email and the internet. All employees, governors, volunteers, trainees and any other users of the schools' IT facilities are expected to adhere to the policy.

2. Disciplinary Measures

2.1 Deliberate and serious breach of the statements and expectations in this policy may lead the school to take disciplinary measures in accordance with the Trust's Disciplinary Policy.

The Trust accepts that ICT – especially the internet and email system – is a valuable business tool. However, misuse of this facility can have a negative impact upon employees, other personnel connected with the school, business productivity and the reputation of the organisation.

2.2 In addition, all of the organisation's phone, internet and email related resources are provided for business purposes. Therefore, the organisation maintains the right to monitor the volume of internet and network traffic, together with the email systems. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

3. Security Measures

3.1 As a member of staff using IT equipment and services, you are responsible for your own activity

3.2 All members of staff using IT equipment and services must adhere to the following:

3.2.1 Do not disclose personal system passwords or other security details to other employees, volunteers or external agents, and do not use anyone else's log-in; this compromises the security of the school system. If someone else gets to know your password, ensure that you change it or seek assistance from the Network Manager or IT Technician;

3.2.2 If you leave your PC or workstation unattended for any reason, you should lock the screen to prevent unauthorised access. If you fail to do this, you will be responsible for any misuse of it (including a data breach) while you are away. Logging off is especially important where members of the public, visitors or students may have access to the screen in your absence.

3.3 Any pen drives or other storage devices used on the school's network should be approved and only those that are the property of the school should be used. Please see paragraph 7 for more detail.

3.4 Do not attempt to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify contents of any sort. If you do not have access to the information or resources you feel you need, contact your line-manager.

4. Use of Email

4.1 When to use email:

4.1.1 Use email in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use. However:

4.1.2 Use the phone for urgent messages (email is a good backup in such instances). Use of email by employees is permitted and encouraged where such use supports the efficient and effectiveness of the school. In some cases, the systems and processes in the school may require telephone contact or a face-to-face contact and not email;

4.1.3 However, when using email, employees and volunteers must ensure that they:

4.1.3.1 comply with current legislation;
4.1.3.2 use email in an acceptable way (including frequency and necessity);
4.1.3.3 do not create unnecessary risk or embarrassment to the reputation of the school or Trust;
4.1.3.4 adopt a professional tone at all times, using appropriate and acceptable language;
4.1.3.5 do not use email to discuss or raise contentious or difficult issues.

Employees and volunteers who do not comply with the expectations above may be deemed to be engaging in unacceptable conduct.

4.2 Unacceptable behaviour

In addition to the situations identified in 3.1, unacceptable behaviour will also include:

4.2.1 Sending confidential information to external locations without appropriate safeguards in place; (See paragraph 5 of this document for more details)

4.2.2 Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal;

4.2.3 Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment or bullying;

4.2.4 Using copyrighted information in a way that violates the copyright;

4.2.5 Hacking into other employee's or another organisation's system, or unauthorised use of a password / mailbox.

4.2.6 Broadcasting unsolicited personal views on social, political, religious or other non-business related matters.

4.2.7 Transmitting unsolicited commercial or advertising material.

4.2.8 Undertaking deliberate activities that waste employee's effort or networked resources.

4.2.9 Deliberately or recklessly introducing any form of computer virus or malware into the corporate network.

4.3 Confidentiality

Always exercise caution when committing confidential information to email since the confidentiality of such material cannot be guaranteed. The school and Trust reserves the right to monitor electronic communications in accordance with applicable laws and policies. The right to monitor communications includes messages sent or received by system users (employees, governors, temporary users and temporary employees) within and outside the system as well as deleted messages. See paragraph 5 for more detail.

4.4 Important points on email use

4.4.1 When publishing or transmitting information externally be aware that you are representing the school and Trust and could be seen as speaking on their behalf. Make it clear when opinions are personal. If in doubt, consult your line manager;

4.4.2 Check your inbox at regular intervals during the working day. Keep your inbox fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical);

4.4.3 Keep electronic files of electronic correspondence and only retain what you need to. Do not print it off and keep paper files unless absolutely necessary;

4.4.4 Treat others with respect and in a way in which you would expect to be treated yourself (e.g. do not send unconstructive feedback, argue, or invite colleagues to make public their displeasure at the actions / decisions of a colleague or what you may consider to be the failings of a particular system of approach);

4.4.5 Do not forward emails warning about viruses (they are invariably hoaxes and the Network Manager will probably already be aware of genuine viruses – if in doubt, contact the IT team for advice;

4.4.6 Do not open an email unless you have a reasonably good expectation of what it contains, and do not download files unless they are from a trusted source. For example, do open **report.doc** from a colleague you know but do not open **explore.zip** sent from an address you have never heard of, however tempting. Alert IT Support if you are sent anything like this unexpectedly; this is one of the most effective means of protecting the school and Trust against email virus attacks.

4.5 Email signatures

Keep these short and include your name, title, phone / fax number(s) and website address.

5. Use of the Internet

5.1 Use of the Internet by employees is permitted and encouraged where such use supports the vision and objectives of the school and Trust and is in line with the employee's role and job description.

5.2 Use of the Internet

When using the Internet, employees must ensure that they:

5.2.1 comply with current legislation;

5.2.2 use the internet in an acceptable way;

5.2.3 do not create unnecessary business risk to the organisation by their misuse of the internet.

5.3 Unacceptable Behaviour

The following is deemed unacceptable use or behaviour by employees or anyone else using the school systems:

5.3.1 Visiting internet sites that contain obscene, hateful, pornographic or other illegal material

5.3.2 Using the computer to perpetrate any form of fraud, or software, film or music piracy;

5.3.3 Using the internet to send offensive or harassing material to other users;

5.3.4 Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;

5.3.5 Hacking into unauthorised areas;

5.3.6 Creating or transmitting defamatory material;

5.3.7 Undertaking deliberate activities that waste employees effort or networked resources;

5.3.8 Deliberately or recklessly introducing any form of computer virus into the school or Trust's network

5.4 Chat rooms / instant messaging (IM)

The use of chat rooms and instant messaging is permitted for business use only. This use must have been agreed in advance with the Headteacher.

5.5 Webmail

The use of webmail (e.g. Hotmail, MSN, Google Mail) is not permitted in the organisation unless it forms part of an employee's role and job-description and has been previously agreed with the headteacher.

5.6 Obscenities / pornography

Do not write, publish, look for, bookmark, access or download material that might be regarded as obscene or pornographic. Such actions are likely to be illegal and will be regarded as a serious breach of this policy.

5.7 Copyright

5.7.1 Take care to use software legally and in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

5.7.2 Be aware of copyright law when using content you have found on other organisations' websites. The law is the same as it is for printed materials.

6. Confidentiality

6.1 If you are dealing with personal, sensitive and / or confidential information, then you must ensure that extra care is taken to protect the information.

6.2 If sending personal, sensitive and / or confidential information via email, then the following protocols should be used. If there is any doubt as to the information being sent or the appropriate level of protection required, please check with the headteacher or data contact:

6.2.1 Personal, sensitive and / or confidential information should be contained in an attachment;

6.2.2 In appropriate cases the attachment should be encrypted, and / or password protected (eg where this information is being sent to external agencies)

6.2.3 Any password or key must be sent separately;

6.2.4 Before sending the email, verify the recipient by checking the address, and if appropriate, telephoning the recipient to check and inform them that the email will be sent;

6.2.5 Do not refer to the information in the subject of the email.

7. The School System

7.1 Keep master copies of important data on the school's network server and not solely on your PC's local C: Drive or portable disks. If data is not stored on the network server, it means it will not be backed up and is, therefore, at risk.

7.2 Ask for advice from the network manager or ICT Technician if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disk space very quickly and can bring the network to a standstill.

7.3 Be considerate about storing personal files on the school's network;

7.4 Do not copy files that are accessible centrally into your personal drive or area unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disk space unnecessarily.

8. Removable Media

8.1 If storing or transferring personal, sensitive, confidential or classified information using removable media you must first ensure that you have permission. You should always:

8.1.1 Consider if an alternative solution already exists;

8.1.2 Only use removable media provided by the school;

8.1.3 Encrypt and password protect;

8.1.4 Store all removable media securely;

8.1.5 Removable media must be disposed of securely by the network manager

9. Personal use of ICT facilities

9.1 Social media

For the purposes of this policy, social media websites are regarded as web-based and mobile technologies which allow parties to communicate instantly with each other or to share data in a public forum. They include websites such as Facebook, Twitter, Google+ and LinkedIn. They also cover blogs and image sharing websites such as YouTube and Flickr. This is not an exhaustive list and you should be aware that this is a constantly changing area.

9.1.1 Employees and volunteers are only permitted to make reasonable and appropriate use of social media websites if this is in line with their role, job description or work responsibilities. Employees should ensure that usage outside directed time is not excessive and does not interfere with work duties.

9.1.2 Access to particular social media websites may be withdrawn in the case of misuse.

9.1.3 Inappropriate comments on social media websites can cause damage to the reputation of the organisation if a person is recognised as being an employee or volunteer or refers to someone who can be identified as such from any comment. It is, therefore, imperative that you are always respectful of the organisation's service as a whole including all staff, colleagues, students and parents/carers

9.1.4 Employees and volunteers should not give the impression that they are representing, giving opinions or otherwise making statements on behalf of a School or the Trust unless appropriately authorised to do so. Personal opinions must be acknowledged as such, and should not be represented in any way that might make them appear to be those of the Trust or any teams or groups within the School or Trust. Where appropriate, an explicit disclaimer should be included, for example: '*These statements and opinions are my own and not those of X.'*

9.1.5 Any communications that employees or volunteers make in a personal capacity must not:

9.1.5.1 bring the school or Trust into disrepute, for example by criticising clients, colleagues or partner organisations;

9.1.5.2 breach Teacher Standards or expectations identified in the Staff Handbook or other policies

9.1.5.3 breach copyright, for example by using someone else's images or written content without permission;

9.1.5.4 do or write anything which might be viewed as discriminatory against, or harassment towards, any individual, for example, by making offensive or derogatory comments relating to: age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation;

9.1.5.5 use social media to bully another individual;

9.1.5.6 post images that are discriminatory or offensive (or which have links to content which is designed to support a derogatory comment or view)

With respect to all aspects of social media, the school and Trust maintains the right to monitor usage where there is suspicion of improper use.

NB: Use of social media outside school which falls into these categories (whether or not accessed through school equipment) will also be subject to investigation and, where appropriate, disciplinary action will be taken.

9.2 Other personal use

9.2.1 The use of school laptops or devices for leisure or personal purposes (e.g. sending and receiving personal email, personal phone calls, playing computer games and browsing the internet) is permitted so long as such use does not:

9.2.1.1 incur specific expenditure for the school or Trust;

9.2.1.2 impact on the performance of an employee's job or role

9.2.1.3 break the law;

9.2.1.4 bring the School or Trust into disrepute;

9.2.1.5 undermine, or make derogatory comments or references to staff, colleagues, students or parents/carers

9.2.1.6 detrimentally affect the network performance by using large amounts of bandwidth (for instance by downloading / streaming of music or videos)

9.2.1.7 impact on the availability of resources needed (physical or network) for business use

9.2.2 Any information contained on the school system in any form is for use by the employee or volunteer for the duration of their period of work and should not be used in any way other than for proper business purposes. Nor should such information be transferred into any other format (e.g. loaded onto a memory stick / pen drive), unless necessary for business use. If information does have to be transferred, an encrypted pen drive should be used and the headteacher should be made aware.

10. Portable and Mobile ICT Equipment

This section covers items such as laptops, mobile devices and removable data storage devices. Please refer to paragraph 7 of this document when considering storing or transferring personal or sensitive data.

10.1 Use of any portable and mobile ICT equipment must be authorised by the headteacher and network manager before use.

10.2 All activities carried out on the school or Trust's systems and hardware will be monitored in accordance with the general policy.

10.3 Employees and volunteers must ensure that all data belonging to the school or Trust is stored on the school or Trust's network and not kept solely on a laptop. Any equipment where personal data is likely to be stored must be encrypted.

10.4 Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting your journey.

10.5 All locally stored data, including diary entries, should be synchronised with the central organisation network server on a frequent basis.

10.6 Portable and mobile ICT equipment must be made available when requested for anti-virus updates and software installations, patches or upgrades.

10.7 The installation of any applications or software packages must be authorised by the school, fully licensed and only carried out by the network manager or designated technician.

10.8 In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

10.9 Portable equipment must be transported in a protective case if one is supplied.

11. Remote Access

11.1 Laptops and mobile devices must have appropriate access protection, i.e. passwords and encryption, and must not be left unattended in public places.

11.2 PINs that are used should not be easily guessed, e.g. do not use your house or telephone number and do not choose consecutive or repeated numbers.

11.3 Avoid writing down or otherwise recording any network access information where possible. Any information that is written down must be kept in a secure place and disguised so that no other person is able to identify what it is.

11.4 Protect the schools and Trust's information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access and printing is from a non-office environment

11.5 Users of laptops and mobile devices are advised to check their car and home insurance policies for the level of cover in the event of equipment being stolen or damaged. Appropriate precautions should be taken to minimise the risk of theft or damage.

11.6 Care should be taken when working on laptops in public places (e.g. trains) so that any employee, student or parent/carer details are not visible to other people.

12 Electronic monitoring

12.1 In your professional role, you may find that you have access to electronic information about the activity of colleagues. Any such information must not be used by unauthorised individuals to monitor the activity of individual employees in any way (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files, etc.) without their prior knowledge. Exceptions are:

12.1.1 In the case of a specific allegation of misconduct, when the headteacher, or HR Manager can authorise accessing of such information when investigating the allegation;

12.1.2 When technicians cannot avoid accessing such information while fixing a problem, but this will only be carried out with the consent of the individual concerned.

13 Online purchasing

Any users who place and pay for orders online using personal details do so at their own risk and the school accepts no liability if details are fraudulently obtained whilst the user is using the School or Trust's equipment.

14 Care of equipment

Do not rearrange the way in which equipment is plugged in (computers, power supplies, phones, network cabling, modems etc.) without first contacting the network manager or designated technician.

15 Agreement

All employees, volunteers, contractors or temporary employees who have been granted the right to use the school or Trust's ICT systems are required to sign this agreement confirming their understanding and acceptance of this policy.

Signed:		**Signed:**	
Line Manager:		**Employee [/volunteer]:**	
Date:		**Date:**	