Management of Information Systems and Social Media Policy

Part of the Passmores Co-operative Learning Community Trust

Passmores Academy

June 2018

Aim of the Trust

To provide unique and enriching opportunities for all.

The information systems policy covers the use of IT systems to support learning, the use of telephones, email and the internet by staff, and the use of online tools provided by The Passmores Co-operative Learning Community Trust. This policy consists of three sections:

- Acceptable use of IT equipment
- Use of telephones, email and internet by staff
- Safe use of online resources and Social Media

This policy is linked to the Staff Discipline Policy.

1. Acceptable use of IT equipment

Principles

The Passmores Co-operative Learning Community Trust is committed to safeguarding its IT infrastructure to ensure it can be used in the most effective manner to support teaching and learning processes. Ensuring the safety and integrity of the Trust's IT infrastructure is the responsibility of all staff. The Trust encourages staff to fully use the IT infrastructure and to make use of portable IT equipment offsite to support them in their work. The Trust encourages this use in a responsible and professional manner. Portable computers include for example laptops, tablets and other portable IT devices.

As a user of IT services of the Trust you have a right to use its computing services; that right places responsibilities on you as a user which are outlined below. If you misuse Trust computing facilities in a way that constitutes a breach or disregard of this policy, consequences associated with that breach mean you may be in breach of other Trust regulations.

Ignorance of this policy and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements. Staff are advised of this policy during their induction and of the Trust's requirement for them to adhere to the conditions therein.

For the purposes of this policy the term "computing services" refers to any IT resource made available to you, any of the network borne services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the Internet). Staff who

connect their own IT to the Trust's network and the services available are particularly reminded that such use requires compliance to this policy.

Purposes

- To protect the Trust's networks and equipment
- To protect the Trust's data
- To protect the Trust and its employees from activities that might expose them to legal action from other parties

Guidelines Password security

Access to all systems and services is controlled by a central computing account and password. Staff are allocated their User ID and initial password as part of their induction with the Trust. Issuance and continued use of your User Account is conditional on your compliance with this policy. User ID's and passwords are not to be shared or revealed to any other party. Those who use another person's user credentials and those who share such credentials with others will be in breach of this policy.

Initial default passwords issued to any user should be changed immediately following notification of account set up using the password criteria below:

#Minimum 7 characters
#Capital letter
#Lower case letter
#Number
#Special character like the asterisk or currency symbol

Passwords should be routinely changed (every month is recommended) and should be changed immediately if the user believes or suspects that their account has been compromised.

General Conditions

In general, use of Trust "computing services" should be for your study, research, teaching or the administrative purposes of the Trust. Modest use of the facilities and services for personal use is accepted so long as such activity does not contravene the conditions of this policy.

- Your use of the Trust's computing services must at all times comply with the law.
- Your use of the Trust's computing services must not interfere with any others' use of these facilities and services.

- You are not entitled to use a computer that you have not been authorised to use.
- You must not access any program or data which has not been specifically authorised for your use.
- You must not use or copy any data or program belonging to other users without their express and specific permission.
- You must not alter computer material belonging to another user without the user's permission.
- You must not use computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.
- You must not use computing services for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such. (There may be certain legitimate exceptions for educational purposes which would require the fullest disclosure and special authorisation from the Principal).
- You must not use the computing services to conduct any form of commercial activity without express permission.
- You must not use the computing services to disseminate mass (unsolicited) mailings.
- You must not install, use or distribute software for which you do not have a licence, and which is not first authorised by the IT Department for installation.
- You must not use any peer-to-peer file sharing software.
- You must not post or subscribe to newsgroups, on-line discussion boards or email list groups from the Trust's facilities, unless specifically related to Trust activities.
- You must not use any form of network monitoring which will intercept data not specifically intended for you unless this activity is a part of your normal job responsibilities or has been specifically authorised by the Principal or Trust Board.
- You must not play computer games of any nature whether preinstalled with the operating system or available online.

Data Security

The Trust holds a variety of personal data some of which is classified under GDPR as sensitive personal data about students, staff, local governors, volunteers and trustees. If you have been given access to this information, you are reminded of your responsibilities under data protection law.

Personal data means data which relates to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive personal data means personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Where there is a requirement to access personal data outside of the Trust's systems, this data **MUST** only be accessed through "OneDrive" which is part of the Office365 package.

You are **NOT** permitted to remove "personal or sensitive" data and download onto laptops, ipads, memory sticks, personal phones and cds/dvds or your personal or school emails. If you do need to take data outside the Trust, that is classified under **"personal or sensitive data"** this should only be with the authorisation of the Trust's IT and Network Manager or the Data Protection Officer.

As part of this you should perform a risk assessment on the implications of it falling into the wrong hands, and take appropriate steps to mitigate against this. This will almost certainly include encrypting the information, and checking the data protection statements of any recipients of the data.

There are a variety of methods of remote access to systems available which allow you to work on data in-situ rather than taking it outside the Trust, and these should always be used in preference to taking data off-site. The IT Department offers a variety of information and support to help you keep data secure. If you are uncertain about any aspect of data security, you must contact them for advice.

Anti-Virus and Firewall Security

All personal computers are installed with current versions of virus protection and firewall software by the IT Department. Users are not to alter the configuration of this software unless express permission has been obtained from the IT Department. This software is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

Users must ensure that they are running with adequate and up-to-date anti-virus software at all times. If any user suspects viral infection on their machine, they should inform the IT Department immediately. If the IT Department detects a machine behaving abnormally due to a possible viral infection, it will be disconnected from the network until deemed safe.

Physical Security

The users of IT equipment should always adhere to the following guidelines:

- Treat equipment safely, in the same manner as a reasonable person would.
- Keep liquids away from IT equipment.
- Do not place heavy objects on IT equipment.
- Do not drop IT equipment or objects onto it.
- Any portable computer must be securely locked away when not in use.
- Portable computer security is your responsibility at all times.
- Do not leave the portable computer unattended in a public place or within the Trust.
- Do not leave the portable computer on view inside your car. It should be locked away in your car's boot out of sight.
- Extra reasonable care must be taken to prevent the loss of USB sticks which contain confidential Trust data.
- Staff supervising students using IT equipment should ensure students take reasonable care of such equipment.

Remote Access

Remote access to the Trust network is possible where this has been granted by the IT Department.

Remote connections are considered direct connections to the Trust network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy.

All connection attempts are logged.

Monitoring and Logging

Activities regarding network transactions may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised systems personnel and kept for no longer than necessary, normally 30 days, and in line with current data protection guidelines.

Such records and information are sometimes required - under law - by external agencies and authorities. The Trust will comply with such requests when formally submitted.

Breaches of This Policy

Incidents which are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of user related activity and evidence.

It is not possible to provide an exhaustive list of potential ways in which a user may contravene this policy but in general such breaches will be categorised into one of three levels of severity and each level of breach will carry with it a possible range of sanctions, consequences and/or penalties. In the event a portable computer is damaged or lost as a result of non-compliance with this policy or as a result of other negligent action, then you may be required to make a full or partial contribution towards any reparation/replacement costs, at the discretion of the Trust.

Minor Breach

This level of breach will attract a formal verbal warning which will be held recorded for 12 months. In general, this category will relate to behaviour or misuse of computer facilities that can be characterised as disruptive or a nuisance. Examples of this level of non-compliance would include:

- Taking food and/or drink into IT facilities where they are forbidden.
- Sending nuisance (non-offensive) email.
- Behaving in a disruptive manner.

Not all first offences will automatically be categorised at this level since some may be of a significance or impact that elevates them to one of the higher levels of severity.

Moderate Breach

This level of breach will attract more substantial sanctions and/or penalties. Examples of this level of non-compliance would include:

- Repeated minor breaches within the above detailed 12-month period.
- Unauthorised access through the use of another user's credentials (username and password) or using a computer in an unauthorised area.
- Assisting or encouraging unauthorised access.
- Sending abusive, harassing, offensive or intimidating email.
- Maligning, defaming, slandering or libelling another person.
- Misuse of software or software licence infringement.
- Copyright infringement.
- Interference with workstation or computer configuration.

Severe Breach

This level of breach will attract more stringent sanctions, penalties and consequences than those above, and access to computing facilities and services may be withdrawn (account suspension) until the disciplinary process and its outcomes have been concluded. Examples of this level of breach would include:

- Repeated moderate breaches.
- Theft, vandalism or wilful damage of/to IT facilities, services and resources.
- Forging email i.e. masquerading as another person.
- Loading, viewing, storing or distributing pornographic or other offensive material.
- Unauthorised copying, storage or distribution of software.
- Any action, whilst using Trust computing services and facilities deemed likely to bring the Trust into disrepute.
- Attempting unauthorised access to a remote system.
- Attempting to jeopardise, damage circumvent or destroy IT systems security.
- Attempting to modify, damage or destroy another authorised user's data

- Disruption of network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing or network flooding activities.

Process

An investigation will be carried out, in confidence, by Trust Leadership under the direction of the Principal. That investigative report will be passed to the staff member's line manager, to be considered within the Trust's disciplinary procedures. Each set of disciplinary procedures provide for an appeal stage.

2. Use of telephones, email and internet/apps by staff

Principles

The provisions of this policy apply to all members of staff, whether or not they have access to, or sole use of, a telephone or e-mail/the Internet on a personal computer. Although access to such facilities does not form part of the benefits provided to staff, it is recognised that there are occasions when employees might legitimately make private use of these facilities. This policy is intended to make clear what constitutes legitimate use. It is intended not to place employees under unjustifiable scrutiny, but to give them a high measure of security and confidence about their use of e-mail, telephones and the Internet.

This policy has been designed to safeguard the legal rights of members of staff under the terms of both the General Data Protection Regulation and the Human Rights Act.

Purposes

To provide guidance on inappropriate use of Trust telephones, email and internet facilities. To clarify when the Trust may monitor staff usage of these facilities.

Guidelines:

Use of telephones

There will be occasions when employees need to make short, personal telephone calls on Trust telephones in order to deal with occasional and urgent personal matters. Where possible, such calls should be made and received outside the employee's normal working hours or when they do not interfere with work requirements.

The use of Trust telephones for private purposes, which are unreasonably excessive or for Trust purposes which are defamatory, obscene or otherwise inappropriate, may be treated as gross misconduct under the appropriate disciplinary procedure.

Where the Trust has grounds to suspect possible misuse of its telephones, it reserves the right to audit the destination and length of out-going calls and the source and length of in-coming calls. This would not normally involve the surveillance of calls but in certain rare circumstances where there are reasonable grounds to suspect serious misconduct, the Trust reserves the right to record calls.

Use of email

As with telephones, it is recognised that employees can use e-mail for personal means in the same manner as that set out for telephones above. E-mail should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter or memorandum is equally unacceptable in an e-mail communication.

Employees should be careful that before they open any attachment to a personal e-mail they receive, they are confident that the content is in no sense obscene or defamatory to avoid contravening the law. Equally, if an employee receives an obscene or defamatory e-mail, whether unwittingly or otherwise and from whatever source, s/he should not intentionally forward the e-mail to any other address, unless specifically requested to do so by an investigator appointed by the Trust.

Any other use of e-mail for either personal or Trust purposes to send or forward messages or attachments which are in any way defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure. Where the Trust has reasonable grounds to suspect misuse of e-mail in either scale of use, content or nature of messages, it reserves the right to audit the destination, source and content of e-mail to and from a particular address.

The Trust also reserves the right to access an employee's e-mail account in her/his unexpected or prolonged absence (e.g. due to sickness) in order to allow it to continue to undertake the employee's normal role. In normal circumstances the employee concerned will be contacted before this is done, in order to provide him/her with prior knowledge.

Change to email use for your own device or devices removed from site - GDPR

If you choose to have your school emails on your own personal device, your device must be password protected. To access your emails, you will need to access them through Office365 using a web browser or by downloading the Microsoft outlook app.

On your device there will be a "mail" app that is pre-installed on your device. This MUST NOT be used to access your school emails, if you use this "mail" app to view school emails the data becomes stored on your device.

Under the new General Data Protection Regulation, this can be deemed as a data breach. It is your responsibility, if you choose to access your emails, and not that of the school. This means that you MUST either gain access through the Microsoft Outlook app, Office 365 or choose not to access your emails outside of school if you feel this would mitigate the risk to you.

Key Points to remember:

- Your device should automatically lock if left inactive for a period of time
- DO NOT use the "mail" app that is preinstalled on the device
- Set your device to receive automatic updates. Downloading the latest "patches" or security updates should cover all vulnerabilities.
- Ensure anti-virus software is installed on laptops and computers and kept up-to-date

Change to email use when communicating outside of school

All emails that are sent outside of the PCLC Trust must be encrypted if they contain personal or sensitive data.

The step by step guide to encryption can be found on the school desktop entitled "Encryption Video", alternatively please see the IT department for support.

Key points to remember:

- When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - eg "Dave" - the auto-complete function may bring up several "Daves". Make sure you choose the right address before you click send.
- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.

Use of the Internet

The primary reason for the provision of Internet access is for the easy retrieval of information for educational purposes, or to make use of learning resources, or to make legitimate authorised purchases to enhance the ability of its staff to undertake their Trust role. However, it is legitimate for employees to make use of the Internet in its various forms in the same way as email above as long as it is not used to view or distribute improper material such as text, messages or images which are derogatory, defamatory or obscene.

Unauthorised use of the Internet, which is unreasonably excessive for personal use or for purposes which are defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure. The Trust reserves the right to audit the use of the Internet from particular personal computers or accounts where it suspects misuse of the facility.

Use of Social Media

Social media can be defined as websites and applications that enable users to create and share content or to participate in social networking, resulting in a number of different activities.

These activities can include, but are not limited to:

- Maintaining a profile page on social / business networking sites such as Facebook, Twitter or LinkedIn.
- Writing or commenting on a blog, whether it is your own or the blog of another person / informational site.
- Taking part in discussions on web forums or message boards.
- Leaving product or service reviews on business websites or customer review Websites.
- Taking part in online polls.
- Uploading multimedia on networking sites such as Instagram and Tumblr.
- Liking, re-tweeting and commenting on posts of your own, another person or other social media account.

As with all personal internet use, employees using social media sites must observe the specific requirements of the school's E-Safety Policy.

Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against employees and the Trust. It may also cause embarrassment to the Trust and other parties connected to the school or bring such parties into disrepute.

Any such, action would likely be addressed under the Disciplinary Policy and could result in dismissal.

Employees must ensure content or links to other content does not interfere with their work commitments

- Pupils must not be discussed on social media sites.
- Photographs or videos of pupils or their homes must not be posted on social media sites.
- Employees should not post information on sites, e.g. photographs and videos that could bring the Trust into disrepute.
- Employees must not represent their own views/opinions as being those of the Trust.
- Potentially false or defamatory remarks towards the Trust, employees, pupils, pupils' relatives, and partner organisations should not be posted on social media sites.
- Employees must not either endorse or criticise service providers used by the Trust or develop on-line relationships which create a conflict of interest.
- When posting on social media sites, employees must observe the requirements of the Equality Act and the Human Rights Act and must not use any offensive, obscene, derogatory, or discriminatory language which may cause embarrassment to Trust, employees, pupils, pupils' relatives and partner organisations.
- Employees must not divulge any information that is confidential to the Trust.
- Employees must not upload, post, forward or post a link to any pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
- Employees must not upload, post, forward or post a link with regards to any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or material in breach of copyright or other intellectual property rights, or which invades the privacy of any person.

Employees should be mindful when placing information on social media sites that this information is visible to a large audience and could identify where they work and with whom, thereby increasing the opportunity for false allegations and threats. In addition, it may be possible through social media sites for children or vulnerable adults to be identified, which could have implications for their security.

Furthermore, there is the scope for causing offence or unintentionally causing embarrassment, for example if pupils find photographs of their teacher which may cause embarrassment and/or damage to their professional reputation and that of the Trust.

In addition, it may be possible for other social media site users to identity where employees live, which could have implications for individual security.

Therefore, first and foremost consideration should be given to the information posted on social media sites and employees are advised to use appropriately the security settings on such sites in order to assist in limiting the concerns above.

Using Apps on your device

If you have apps installed on your device, you must ensure that your device is password protected and it is strongly recommended that you do not access school based apps in a public place where they can be seen by another individual, this is a "data breach" and you would be liable. For example, the SIMS Teacher App which will contain both personal and sensitive data.

Monitoring the use of telephone, e-mail and the Internet.

It is not the Trust's policy, as a matter of routine, to monitor an employee's use of the Trust's telephone or e-mail service or of the Internet via the Trust's networks. However, as has been stated, where there are reasonable grounds to suspect an instance of misuse or abuse of any of these services, the Principal or Trust Board may grant permission for the auditing of an employee's telephone calls, e-mail or the Internet.

Once approved, the monitoring process will be undertaken by designated staff acting, for operational purposes, under the direction of the Principal. These staff are required to observe the strictest confidentiality when undertaking these activities and they will monitor only to the extent necessary to establish the facts of the case. They will make their reports directly to the Principal/Trust Board or their delegated representative to enable Human Resources to advise the appropriate line manager/head of faculty the actions that may need to be taken in any particular case. When monitoring is approved, the case for continued monitoring shall be reviewed on a regular basis with a view to terminating monitoring in as short a period of time as possible.

3. Safe use of online resources and social media

Principles

This applies wherever access to The Passmores Co-operative Learning Community Trust Management Information Systems (MIS) are provided. This applies to all online resources provided by The Passmores Co-operative Learning Community Trust, for example Capita SIMS. This policy applies whenever information is accessed through The Passmores Co-operative Learning Community Trust MIS, whether the computer equipment used is owned by The Passmores Co-operative Learning Community Trust or not. The policy applies to all those who make use of The Passmores Co-operative Learning Community Trust's MIS resources.

Security

This Policy is intended to minimise security risks. These risks might affect the integrity of The Passmores Co-operative Learning Community Trust's data, the authorised MIS user and the individuals to which the MIS data pertains. In particular, these risks arise from:

- The intentional or unintentional disclosure of login credentials.
- The wrongful disclosure of private, sensitive, and confidential information.
- Exposure of The Passmores Co-operative Learning Community Trust to vicarious liability for information wrongfully disclosed by authorised users.

Data Access

- This policy aims to ensure all relevant aspects of the General Data Protection Regulations are adhered to.
- This Regulation aims to promote best use of the MIS system to further the communication and freedom of information between The Passmores Co-operative Learning Community Trust and parents/carers and students.

Guidelines

The Passmores Co-operative Learning Community Trust's online systems are provided for use only by persons who are legally responsible for student(s) currently attending the Trust.

Access is granted only on condition that the individual formally agrees to the terms of this policy.

The authorising member of Trust staff **must** confirm that there is a legitimate entitlement to access information for students, the names of whom must be stated on the Online Usage Policy Declaration.

A copy of the form will be held by the Trust for audit purposes.

Personal Use

Information made available through the MIS system is confidential and protected by law under the General Data Protection Regulations. To that aim:

Users must not distribute or disclose any information obtained from the MIS to any person(s) with the exception of the student to which the information relates or to other adults with parental/carer responsibility.

Best practice is not to access the system in any environment where the security of the information contained may be placed at risk.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **Data Protection Officer**:

Ms. Tina Sparrow, Passmores Co-operative Learning Community Trust

Email: gdpr@pclc.co.uk or alternatively, contact the main school office on 01279 770800.

COPYRIGHT CONSIDERATIONS

Respect all copyrights and do not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner. This includes all software, music, video and books.

All software and media must be appropriately licensed and vetted by the school's IT Network Manager before use. You should consult with IT Support before purchasing new software to ensure that any technical issues are fully considered. Both the individual and the school may be subject to legal action if illegal software/media is used.

By signing below, you acknowledge that you have read and understood this policy and that any breach may be subject to disciplinary procedures, at the Principal's discretion.

You have the right to refuse for your image to be used in PCLC media and communications. If you wish to exercise this right, please make the HR department aware.

Declaration

Please only sign if you have fully read the Management of Information Systems and Social Media Policy. By signing the acceptance form you are agreeing that you have fully understood the terms and conditions and all the instructions/policies of The Passmores Co-operative Learning Community Trust Computing Services.

Please contact The Network Manager or the Data Protection Officer at The Passmores Co-operative Learning Community Trust if you are not sure of any policies and terms and conditions of use.

Declaration

Print Name_____

Signature_____

Date_____

This declaration will be stored in your staff file in the HR department.