



DATA AND INFORMATION GOVERNANCE: **Information Security Policy**

This policy has been adopted by the Board of Directors of Pathfinder Multi Academy Trust and is applicable across all schools that make up the Trust. In line with the MAT's Scheme of Delegation, this Policy must be duly applied by each Local Governing Committee and the Headteacher of each school that is part of Pathfinder Multi Academy Trust.

Where there are specific details or any discretions in the policy that apply to an individual school or Local Governing Committee this has been made clear within the wording of the policy.

This policy will be reviewed formally by the MAT Board of Directors in line with the agreed timetable for policy review or sooner as events or legislation changes require.

Date Adopted: **February 2021**

Date for Review: **February 2023**

Contents

Introduction	3
Scope	3
Access Control	3
Manual Filing Systems	
Electronic Systems	
Software and Systems Audit Logs	
Data Shielding	
External Access	
Physical Security	4
Clear Desk Policy	
Alarm System	
Building Access	
Internal Access	
Visitor Control	
Environmental Security	5
Back Ups	
Fire Proof Cabinets	
Fire Doors	
Fire Alarm System	
Systems Security	6
Software Download Restrictions	
Phishing Emails	
Firewalls and Anti-Virus Software	
Cloud Computing	
Shared Drives	
Communications Security	7
Sending Personal Data by post	
Sending Special Category Data by post	
Sending Personal Data and Special Category Data by email	
Exceptional Circumstances	
Using the BCC function	
Surveillance Security	7
Remote Working	
Storage	
Private Working Area	
Trusted Wi-Fi Connections	
Encrypted Devices (including USBs) and Email Accounts	
Data Removal and Return	

Introduction

The Information Security Policy outlines the Pathfinder Multi Academy Trust's (PMAT) organisational security processes and standards. The policy is based upon the sixth principle of the GDPR which states organisations must protect the personal data, which it processes, against unauthorised loss by implementing appropriate technical and organisational measures. This policy has been written using the security framework recommended by ISO: 27000:1 (internationally recognised information security standard).

This policy should be read in conjunction with the other policies in PMAT's Data and Information Governance framework with particular focus on the Acceptable Use Policy and the Information Security Incident Reporting Policy.

Scope

All policies in the Information Governance policy framework apply to all PMAT employees, any authorised agents working on behalf of PMAT, including temporary or agency employees, and third party contractors.

Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;,
- Information or data stored electronically, including scanned images;,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;,
- Information stored on desktop computers, portable computing devices including mobile phones, tablets, cameras and laptops;,
- Speech, voice recordings and verbal communications, including voicemail;,
- Published web content, for example intranet and internet;,
- Photographs and other digital images.

Access Control

Each School will maintain control over access to the personal data that it processes.

These controls will differ depending on the format of the data and the status of the individual accessing the data. The School will maintain an audit log detailing which individuals have access to which systems (both electronic and manual). This log will be maintained by each schools School Business Manager/Office Manager or equivalent.

Manual Filing Systems

Access to manual filing systems (i.e. non-electronic systems) will be controlled by a key management system. All files, that contain personal data, will be locked away in lockable storage units, such as a filing cabinet or a document safe, when not in use.

Keys to storage units will be locked in a pin-operated key safe or lockable key safe. The Office Manager will be responsible for giving individuals access to the key safe. Access will only be given to individuals who require it to carry out legitimate business functions. Where

pin operated key safes are used, the pin will be changed every three months or whenever a member of staff leaves the organisation, whichever is sooner.

Electronic Systems

Access to electronic systems will be controlled through a system of user authentication. Individuals will be given access to electronic filing systems if required to carry out legitimate functions. A two tier authentication system will be implemented across all electronic systems. PMATs two tier system will comprise of a unique username and password.

Individuals will be required to change their password every 90 days and user names will be suspended either when an individual is on long term absence or when an individual leaves employment of the School.

Users must ensure that their electronic devices and software do not store PMAT passwords allowing other users to access our systems without authentication.

Software and Systems Audit Logs

PMAT will ensure that all software and systems have inbuilt audit logs so that the PMAT can ensure it can monitor what employees and users have accessed and what changes may have been made. Although this is not a preventative measure it does ensure that the integrity of the data can be assured and also deters individuals from accessing records without authorisation.

Data Shielding

PMAT does not allow employees to access the personal data of family members or close friends. Employees should declare, upon employment, whether they are aware of any family members or friends who are registered at our Schools/Trust.

Where appropriate, the School will then keep paper files in a separate filing cabinet (with access restricted to minimal employees) and any electronic files will be locked down so that the declaring employee cannot access that data.

Employees who knowingly do not declare family and friends registered at our Schools may face disciplinary proceedings and may be charged with an offence under Section 170 of the Data Protection Act 2018 (unauthorised access to information).

External Access

On occasions the School will need to allow individuals, who are not employees of the School, to have access to data systems. This could be, for example, for audit purposes, to fulfil an inspection, when agency staff have been brought in, or because of a Partnership arrangement with another School. The Chief Operating Officer or the Chief Finance Officer is required to authorise all instances of third parties having access to systems.

An access log, detailing who has been given access to what systems and who authorised the access, will be maintained by the School.

Physical Security

The School will maintain high standards of Physical Security to prevent unauthorised access to personal data. The following controls will be maintained by all our Schools:

Clear Desk Policy

Individuals will not leave personal data on desks, or any other working areas, unattended and will use the lockable storage units provided to secure personal data when not in use.

Alarm System

Schools will maintain a security alarm system at its premises so that, when the premises are not occupied, an adequate level of security is still in operation.

Building Access

External doors to the premises will be locked when the premises are not occupied. Only authorised employees will be key holders for the building premises. The Headteacher will be responsible for authorising key distribution and will maintain a log of key holders.

Internal Access

Internal areas, which are off limits to pupils and parents, will be kept locked and only accessed through pin numbers or keys. Pin numbers will be changed every six months or whenever a member of staff leaves the organisation. Keys will be kept in a key safe.

Visitor Control

Visitors to the School will be required to sign in a visitor's book and state their name, organisation, car registration (if applicable) and nature of business. Schools will follow PMAT's visitors to schools process and where applicable will ensure that visitors are escorted throughout the School and not permitted access to restricted areas without employee supervision.

Visitor books will be locked away at the end of the working day and kept for current financial year + six years.

Environmental Security

As well as maintaining high standards of physical security, to protect against unauthorised access to personal data, PMAT must also protect data against environmental and natural hazards such as power loss, fire, and floods.

It is accepted that these hazards may be beyond the control of School but the School will implement the following mitigating controls:

Back Ups

PMAT will back up their electronic data and systems every evening. Backups are stored off site. Any external arrangements will be governed by a data processing agreement. Should PMAT's electronic systems be compromised by an environmental or natural hazard then the School will be able to reinstate the data from the backup with minimal destruction.

Fire Proof Cabinets

The School will aim to only purchase lockable data storage cabinets that can withstand exposure to fires for a short period of time. This will protect paper records, held in the cabinets, from any minor fires that break out on the building premises.

Fire Doors

Areas of the premises which contain paper records or core electronic equipment, such as server boxes, will be fitted with fire doors so that data contained within those areas will be protected, for a period of time, against any fires that break out on the premises. Fire doors must not be propped open unless automatic door releases are installed.

Fire Alarm System

The School will maintain a fire alarm system at its premises to alert individuals of potential fires and so the necessary fire protocols can be followed.

Systems Security

As well as physical security PMAT also protects against hazards to its IT network and electronic systems. It is recognised that the loss of, or damage to, IT systems could affect the School's ability to operate and could potentially endanger the lives of its Pupils.

The School will implement the following systems security controls in order to mitigate risks to electronic systems:

Software Download Restrictions

Employees must request authorisation from Vital before downloading software on to the School's IT systems. Vital will vet software to confirm its security certificate and ensure the software is not malicious. Vital will retain a list of trusted software so that this can be downloaded on to individual desktops without disruption.

Phishing Emails

In order to avoid PMAT's computer systems from being compromised through phishing emails - employees are encouraged not to click on links that have been sent to them in emails when the source of that email is unverified. Employees will also take care when clicking on links from trusted sources in case those email accounts have been compromised. Employees will check with Vital if they are unsure about the validity of an email.

Firewalls and Anti-Virus Software

PMAT will ensure that the firewalls and anti-virus software is installed on electronic devices. PMAT will update the firewalls and anti-virus software when updates are made available and when advised to do so by Vital. PMAT will review its firewalls and anti-virus software on an annual basis and decide if they are still fit for purpose.

Cloud Computing

Employees must only use cloud systems managed and authorised by the Pathfinder Network.

Shared Drives

The School maintains shared drives on its servers. Whilst employees are encouraged not to store personal data on the shared drive it is recognised that on occasion there will be a genuine business requirement to do so.

The shared drive will have restricted areas that only authorised employees can access. Our IT providers will be responsible for configuration of access to these drives. Shared drives will still be subject to the School's retention schedule.

Communications Security

The transmission of personal data is a key business need and, when operated securely is a benefit to the School and pupils alike. However, data transmission is extremely susceptible to unauthorised and/or malicious loss or corruption. PMAT has implemented the following transmission security controls to mitigate these risks:

Sending Personal Data by post

When sending personal data, excluding special category data, by post the School will use Royal Mail's standard postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject.

Sending Special Category Data by post

When sending special category data by post the School will use Royal Mail's 1st Class Recorded postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject. If the envelope contains information that is thought to be particularly sensitive then employees are advised to have the envelope double checked by a colleague.

Sending Personal Data and Special Category Data by email

The School will only send personal data and special category data by email if using a secure email transmission portal.

Employees will always double check the recipient's email address to ensure that the email is being sent to the intended individual(s).

Exceptional Circumstances

In exceptional circumstance the School may wish to hand deliver, or use a direct courier, to ensure safe transmission of personal data. This could be because the personal data is so sensitive usual transmission methods would not be considered secure or because the volume of the data that needs to be transmitted is too big for usual transmission methods.

Using the BCC function

When sending emails to a large number of recipients, such as a mail shot, or when it would not be appropriate for recipients to know each other's email addresses then School employees will utilise the Blind Copy (BCC) function.

Surveillance Security

**ONLY APPLICABLE IF YOU OPERATE CCTV/PHONE RECORDING
(DELETE AS APPROPRIATE)**

The School operates CCTV at its premises.

Due to the sensitivity of information that could be collected as a result of this operation, the School has a separate policy which governs the use of CCTV. This policy has been written in accordance with the ICO's Surveillance Code of School.

Remote Working

It is understood that on some occasion employees of PMAT will need to work at home or away from our premises. If this is the case then the employees will adhere to the following controls:

Storage

If employees are working at home they will ensure that they store any personal data and PMAT equipment safely to prevent loss or theft.

Employees must not keep personal data or PMAT equipment unsupervised at home for extended periods of time (for example when the employee goes on holiday).

Employees must not keep personal data or PMAT equipment in cars if unsupervised.

Private Working Area

Employees must not work with personal data in areas where other individuals could potentially view or even copy the personal data (for example on public transport).

Employees should also take care to ensure that other household members do not have access to personal data and do not use PMAT equipment for their own personal use.

Trusted Wi-Fi Connections

Employees will only connect their devices to trusted Wi-Fi connections and will not use 'free public Wi-Fi' or 'Guest Wi-Fi'. This is because such connections are susceptible to malicious intrusion.

When using home Wi-Fi networks, through personal devices, employees should ensure that they have appropriate anti-virus software and firewalls installed to safeguard against malicious intrusion. If in doubt employees should seek assistance from Vital.

Encrypted Devices (including USBs) and Email Accounts

Employees will only use PMAT issued encrypted devices to work on Personal Data. Employees will not use personal devices for accessing, storing, or creating personal data. This is because personal devices do not possess the same level of security as a PMAT issued device.

Employees will not use Personal email accounts to access or transmit personal data. Employees must only use PMAT issued, or PMAT authorised, email accounts.

Data Removal and Return

Employees will only take personal data away from our premises if this is required for a genuine business need. Employees will take care to limit the amount of data taken away from the premises.

Employees will ensure that all data is returned to our premises either for re-filing or for safe destruction. Employees will not destroy data away from the premises as safe destruction can not be guaranteed.