PONTEFRACT
ACADEMIES TRUST

Information Security Policy

Trust Board Approval Date	10 December 2019
Effective Date	1 October 2019
Planned Review Date	October 2021
Web Access	Internet
Owner	Director of Operations

Information Security Policy

1.1 PURPOSE

Pontefract Academies Trust ("The Trust") is required to collect, hold, process and share information to enable it to operate. This policy is to ensure that the Trust complies with the requirements of the European Union's General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

This policy sets out the Trust organisational security processes and standards. This 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:270001:1 (internationally recognised information security standard).

1.2 SCOPE

This Policy applies to all Trust employees, agency staff, trustees, members of the governance structure, or any other third-party contractors appointed/employed by the Trust (employees). Individuals who are found to knowingly or recklessly infringe this policy may be subject to disciplinary or other appropriate action.

This Policy applies to information in all forms including, but not limited to:

- Hard copy 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 portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content for example internet and intranet; and
- Photographs and other digital images

1.3 RELATED POLICIES OR PROCEDURES

The Information Security Incident Reporting Policy should be read in conjunction with other policies and procedures that relate to conduct systems and procedures. This includes:

- Staff Code of Conduct, including safer working practice guidance
- Information Security Policy
- Information Security Incidents Reporting Policy
- Records Management Policy and Procedures
- Surveillance Policy (including CCTV)

1.4 ACCESS TO SYSTEMS

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). The School Support Manager or Office Manager will be responsible for ensuring that the log is maintained at all times.

1.4.1 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 restricted to individuals who require them to carry out legitimate business functions.

1.4.2 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. All electronic systems require authentication by username and unique password.

The Head of School will be required to inform Alamo if any user names require suspending when an individual is on long term absence or other relevant HR matter.

New/leaving employees will be informed to Alamo by the school (Office Manager, School Support Manager or Head of School) or the HR function for central trust employees.

The Trust Clerk will be required to inform Alamo of new/leaving Members, Trustees, or SPRB members.

Individuals will be required to change their password every 90 days and will meet the following complexity requirements: Be at least eight characters in length Contain characters from three of the following four categories: uppercase letters, lowercase letters, numbers from 0 to 9, non-alphabetic/numeric characters (e.g. !,$,
#, %).

1.4.3 Software and Systems Audit Logs

The Trust will require that all software and system specifications which process personal information have inbuilt audit logs so that it can monitor what employees and users have accessed systems 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 deters individuals from access to records without authorisation.

1.4.4 Access to external parties

On occasions the Trust may need to allow individuals, who are not employees of the Trust, to have access to data systems. This could be, but not exclusively for audit purposes, to fulfil an inspection, consultants, agency/supply staff, or trainees. The Head of School is required to authorise all instances of third parties having access to systems. If the Head of School is not available to authorise access, then access can also be authorised by their Deputy or Assistant. The Director of Operations/Finance and Estates can authorise access to central trust systems or trust wide systems

In all instances the Head of School, their Deputy or Assistant or Director of Operations/Finance and Estates must ensure that the external party is made aware of this policy and their responsibilities regarding information governance and confidentiality.

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

1.5 PHYSICAL SECURITY

The Trust will maintain high standards of physical security to prevent unauthorised access to personal data. The following controls will be maintained by the Trust:

1.5.1 Clear Desk and Screen Policy

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

Unattended computer terminals must be turned off or locked when unattended. An auto- lock system will be invoked after a period of 20 minutes of inactivity.

1.5.2 Alarm System

All Trust premises will maintain security alarm systems to ensure that an adequate level of security is in operation when premises are unoccupied.

1.5.3 Building Access

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

1.5.4 Internal Access

Internal areas which have restricted access will be kept locked and only accessed through pin pads or keys.

1.5.5 Visitor Control

Visitors to each school will be required to sign the visitor book or on the visitor management system. Visitors will not be permitted access to restricted areas without employee supervision.

1.6 ENVIRONMENTAL SECURITY

As well as maintaining high standards of physical security, to protect against unauthorised access to personal data, the Trust 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 the Trust, however, the Trust will implement the following mitigating controls:

1.6.1 Access to Servers

Access to servers will be restricted as far as is practicably possible.

1.6.2 Back Ups

Each primary school server will be backed up at least twice a week to an encrypted disk, which will be stored off site with designated officer, a secondary disk stored in the school safe. In addition to this a weekly offsite backup is also to a secure network attached storage device located at The Kings School. This is performed over the trust wide area network (WAN).

Secondary school servers have daily backups of all crucial virtual servers which are saved to a secure network attached storage device located within a physically separate building to the core infrastructure (technology block at Carleton High School & old caretaker's house at The Kings School). A single backup is replicated weekly between these two devices to ensure each school has an offsite backup.

Should the school's electronic system be compromised by an environmental or natural hazard then the school will be able to reinstate the data from the back up with minimal destruction.

Bromcom MIS (pupil management information system) is a cloud-based system and is backed up in accordance with the software agreement with Bromcom.

The Trust financial system PS Financials is held on a dedicated server located at The Kings School and is backed up daily on the cloud, it is also replicated daily to a secondary server located at Carleton High School.

1.6.3 Fire Proof Cabinets

The Trust 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.

1.6.4 Fire Alarm System

Each 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. The Trust HQ lease will include a fire alarm system maintained by the landlord.

Information Security Policy

1.7 SYSTEMS SECURITY

As well as physical security the Trust 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 Trust's ability to operate and could potentially endanger the lives of its pupils/students.

The Trust will implement the following systems security controls to mitigate risks to electronic systems:

1.7.1 Software Download Restrictions

Employees do not have administration rights to enable them to install software. Alamo will only install software onto a school/central team IT system on receipt of written instruction from the Head of School or Director of Operations/Finance and Estates. Alamo will vet software to confirm its security certificate and ensure the software is not malicious. Alamo will retain a list of trusted software so that this can be downloaded on to individual desktops without disruption.

1.7.2 Phishing Emails

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

1.7.3 Firewalls, Filtering and Anti-Virus Software

Alamo will ensure that the Trust filtering and anti-virus software is installed on all trust electronic devices. Alamo will update the filtering and anti- virus software when updates are made available. Alamo will review the Trust's filtering and anti-virus software on an annual basis and decide if they are still fit for purpose.
The Trust ISP (Talk Straight) provide a managed firewall and ensure it is configured optimally and kept up to date.

1.7.4 Cloud Computing

The Trust currently operates its email communications on Office365. Employees will not save any other records on cloud storage unless authorised to do so by their Head of School. This should be in limited or exceptional circumstances (i.e. google drive or
one drive).

Employees are able to access email communications on their personal or work mobile telephone only if it has a pin code or bio recognition and adheres and adheres to the Office365 security policy.

1.7.5 Shared Drives

The Trust maintains a shared drive 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. Shared drives will still be subject to the Trust's retention schedule.

1.7.6 Wireless Network

Alamo will ensure that the local area networks are AES/WPA2 encrypted to the highest industry standard. WiFi passwords will be restricted to Alamo second line support staff. The WiFi will be set up to only allow access onto the wireless network for Trust owned devices. Exceptions will only be permitted on the instruction of the CEO.

1.8 COMMUNICATIONS SECURITY

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

1.8.1 Sending Personal Data by post

When sending personal data, excluding special category data, by post the Trust 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. Envelopes should be marked "Private and Confidential, to be opened by the addressee only".

1.8.2 Sending Special Category Data by post

When sending special category data by post the Trust 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. Envelopes should be marked "Private and Confidential, to be opened by the addressee only".

1.8.3 Sending Personal Data and Special Category Data by email

Where personal data is emailed to another Trust email address it is automatically encrypted and therefore secure from external interception, however all files must be password protected using passwords which are secure to the parties involved in the transaction.. Where personal data is emailed external to the Trust the subject header should start with **[Encrypted]** to secure it from interception and requires authentication at the recipients end regardless of their system.

Special category data should only be sent externally by email in exceptional circumstances and where any other more secure means of communication is not appropriate. In such cases the instructions above will be followed and additional security of password protection will be added.

Where special category data is being sent internally by email, employees should be extra vigilant and always consider whether there is a genuine need to send the information in an email. Personal comments should never be included in emails, and care should be taken to ensure the accuracy of information.

In all instances, employees must always double check the recipient's email address to ensure that the email is being sent to the intended individual(s).

1.8.4 Exceptional Circumstances

In exceptional circumstance the Trust 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.

1.8.5 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 employees will utilise the blind copy (BCC) function.

1.9 TRANSFERRING AND SHARING DATA

All data transferred or shared should be done so securely and an appropriate written protocol or processing agreement in place.

1.10 SURVEILLANCE SECURITY

A number of Trust schools operate CCTV. Due to the sensitivity of information that could be collected as a result of this operation, the Trust has a separate policy which governs the use of CCTV.

1.11 REMOTE WORKING

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

1.11.1 Storage Security

When files or equipment are stored at home they should not be openly accessible to other members of the household.

Employees must always lock their computer screen when away from their computer/laptop.

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

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

1.11.2 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 school equipment for their own personal use.

1.11.3 Trusted Wi-Fi Connections

Employees will only connect their devices to trust 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 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 IT Provider.

1.11.4 Using Home Computers

When an employee is using their home computer/device to access school remote services or email then they should firstly ensure that their computer is up to date with the latest anti-virus protection.

Any information or files should not be downloaded to the home computer/device.

The employee should not leave the device unattended and should ensure they log off all Trust systems completely at the end of any session.

If an employee has the facility to print from home then this should be limited and not stored at home.

1.12 DISPOSAL OF DATA AND INFORMATION

Documents containing information which is confidential or includes personal data must be disposed of through cross shredding disposal or a certified GDPR compliant personal data shredding service. A destruction log will be completed when the final copy of personal data is destroyed. Personal data held in containers or consoles will be locked, in restricted areas with controlled access restricted to the Head of School or collection provider.

Disposal of computer equipment must be via Airedale Computers and should be stored in secure rooms/cabinets prior to disposal. In all instances Alamo will be responsible for making arrangement with Airedale Computers and retaining the audit log of disposal and forwarding a copy to the school.

1.13 INFORMATION / INTELLECTUAL PROPERTY

Any information or intellectual property held or developed on trust systems or through a contract of employment or commercial contract remains the property of the Trust.

All systems must be monitored and audited for administrative, legislative and management purposes, therefore, personal privacy cannot be guaranteed.

It may be necessary to access systems and equipment during an employee's absence to ensure business continuity and compliance with the Freedom of Information Act.

Appendix A: Schedule of Environment Security Measures

	Server Location	**Back Up location**
Carleton High School	Annex Block – locked room	Technology Block (automatic)
The King's School	ICT/Maths Block - locked room	Caretakers House (automatic)
Carleton Park	SBM Office	Disks held in the school safe *(designated officer responsible for disk rotation)*
De Lacy Primary	Server Room	Disks held in the school safe. *(designated officer responsible for disk rotation)*
Halfpenny Lane	Locked Cupboard	Disks held in the school safe. *(designated officer responsible for disk rotation)*
Larks Hill	Secure cabinet in ICT suite	Disks held in the school safe. *(designated officer responsible for disk rotation)*
Orchard Head	Server Room	Disks held in the school safe. *(designated officer responsible for disk rotation)*
The Rookeries	Old SBM Office	Disks held in the school safe. *(designated officer responsible for disk rotation)*
Central Team	Server Room – locked room	Stored on the King's School Server configuration

Firewalls are managed by Talk-Straight

Anti-virus software licence renewal is managed by Alamo and is currently provided by Sophos.

Filtering software licence renewal is managed by Alamo and is currently provided by Censornet.