Malton School

A Specialist Science School

1547

Stronger For Being One

Information Security Policy

Document Status		Staff Responsible	Governor Committee
Date of Approval	01/04/2019	Operations Director	Full Governors
Date of next review	01/04/2022	Operations Director	Full Governors

Introduction

In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom. This Information Security Policy outlines the School's 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 the School's Information Governance policy framework with particular focus on the Acceptable Use Policy and the Data Breach Policy.

Scope

All policies in the Information Governance policy framework apply to all School employees, any authorised agents working on behalf of the School, 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 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

The 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 The IT Manager.

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.

Access will only be given to individuals who require it to carry out legitimate business functions. All keys and school property will be retrieved from any individual who leaves the organisation.

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. The two tiers will be user and unique Password.

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

Software and Systems Audit Logs
The School will ensure that all software and systems have inbuilt audit logs so that the School 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
The School 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 the School. 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 the School 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 Operations Director is required to authorise all instances of third parties having access to systems. If the above individual is not available to authorise access then access can also be authorised by the Headteacher. Any access for third parties working in partnership with the school will only be provided in accordance with any defined contractual agreements between the school and the relevant third parties.

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 the School:

Office Access
Any staff who work from their own office will ensure that the office door is locked if the space is left unattended. All staff who interact with personal data will take reasonable steps to ensure that such personal data is not left unattended in an unlocked area or in a situation where students, visitors or other unauthorised individuals could access it.

Alarm System
The School 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 Operations Director 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. Duplicate keys will be kept in a secure location.

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 details of who they are visiting. Visitors will be escorted throughout the School and will not be allowed to access restricted areas without employee supervision.

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

Environmental Security

As well as maintaining high standards of physical security, to protect against unauthorised access to personal data, the School 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
The School will back up their electronic data and systems every night. These backups are transmitted between the two wings of the school so that a complete data set is stored in each wing at all times. Should the School's electronic systems be compromised by an environmental or natural hazard then whichever part of the school is affected, the School will be able to reinstate the data from the backup stored in the opposite wing with minimal destruction to data and disruption to work.

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 the School 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 The IT Manager before downloading any unapproved software onto any School's IT systems or devices. The IT Manager will vet software to confirm its security certificate and ensure the software is not malicious. The IT Manager will retain a list of trusted software so that this can be downloaded on to individual desktops/I-pads without disruption.

Phishing Emails
In order to avoid the School'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 The IT Manager if they are unsure about the validity of an email.

Firewalls and Anti-Virus Software
The School will ensure that the firewalls and anti-virus software is installed on electronic devices and routers. The School will update the firewalls and anti-virus software when updates are made available.

Cloud Computing
The school does permit unauthorised usages of cloud storage. The only authorised storage is restricted to the use of OneDrive and Google drive, as these services data centres are in the EU. Users who utilise cloud storage providers must ensure NO personal data is stored in these services.

Shared Drives
The School 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. For example a HR folder in the shared drive will only be accessible to employees responsible for HR matters. The IT Manager will be responsible for giving shared drive access rights to employees. 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. The School 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 using a secure email transmission portal such as Egress Secure Email method.

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

The School operates CCTV at its premises.

Due to the sensitivity of information that could collected as a result of this operation, the School has a separate policy which governs the use of CCTV.

Remote Working

It is understood that on some occasion employees of the school will need to work at home or away from the school premises. If this is the case then the employees will take all reasonable steps to ensure the safeguarding of personal data, especially when working at home or in public spaces.

Trusted Wi-Fi Connections

Employees will only connect their devices to trusted Wi-Fi connections. This is because such connections are susceptible to malicious intrusion. Dongles provided by the school can be used to work remotely, but again, only with due regard to the safeguarding of personal data.

Firewall and Antivirus software are maintained on all school devices by the school. This is done to ensure that if a school device is used on home Wi-Fi the configuration of the Firewall and Antivirus software are able to support this.

Encrypted Devices and Email Accounts

Employees will only use School 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 School issued device.

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

Data Removal and Return

Employees will only take personal data away from the School 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 and will ensure that such data is returned to school for appropriate filing or destruction as soon as is practical.

End of Document