

Security Measures



ST JOHN PAYNE CATHOLIC SCHOOL

Approved by	FGB
Date Approved	10/06/2020
Version	2
Review Date	June 2021 and annually

Description of Security Measures employed to safeguard the processing of Personal Data

1. Organisational

a. Policies & Documented Procedures

Policies relating to information governance issues are drafted by employees with detailed knowledge of legal requirements and the Organisation's processes. All policies have documented review dates and ownership is assigned. Reviews are held ahead of the expiry date or sooner where there is an identified issue. All policies follow a governance route for approval. Key policies are published to the organisation's website for transparency.

b. Roles

The organisation has a named Data Protection Officer who is Lauri Almond. This Officer executes the role by reporting the outcome of statutory process to Mr T Coen who acts as the organisation's Senior Information Risk Owner.

c. Training

The organisation regularly reviews our employee roles to ensure that training and awareness messages are appropriate to the nature and sensitivity of the data processing undertaken. Induction processes ensure new employees receive appropriate training before accessing personal data, and all other employees receive refresher training annually. All training received is documented for evidence purposes.

d. Risk Management & Privacy by Design

The organisation identifies information compliance risks on its risk register. Risks are assigned clear ownership, rated against a consistent schema, appropriate mitigations are identified and are annually reviewed.

e. Contractual Controls

All Data Processors handling personal data on behalf of the organisations have given assurances about the compliance of their processes; either through procurement assurances/ evidence, contractual agreement controls, risk assessments or supplementary statements.

f. Physical Security

All employees or contractors who have access to our premises where personal data is processed are provided with Identity Cards which validate their entitlement to access. The organisation operates processes which ensure only those individuals who have an entitlement to access premises are able to. Access to physical storage holding sensitive personal data is further restricted either through lockable equipment with key or code control procedures or through auditable access to specific rooms/ areas of buildings.

g. Security Incident Management

The organisation maintains a security incident process which, with the support of appropriate training, defines what constitutes a breach of these security measures to facilitate reporting of incidents. The process covers investigation of incidents, risk rating and decisions over whether to notify an incident to the Information Commissioner's Office (ICO) within the statutory timescale. Incidents are reported to senior leaders and actions are consistently taken and lessons learned implemented.

2. Technical

a. Data at Rest

i. Use of Hosting Services

Some personal data is processed externally to the organisation's managed environment by third parties in data centres under agreed terms and conditions which evidence appropriate security measures. The location of the data storage centres complies with data protection and GDPR requirements.

ii. Firewalls

Access to the Organisation's managed environment (RM education) is protected by maintained firewalls. Business needs to provide access through the firewall go through a strictly documented change control process which include risk assessment and approval.

iii. Administrator Rights

Enhanced privileges associated with administrator accounts are strictly managed. Administrator activities are logged and auditable to ensure activity can be effectively monitored.

iv. Access Controls

Access permissions to personal data held on IT systems is managed through role based permissions. Managers of appropriate seniority inform IT professionals of additions, amendments and discontinuation of individual accounts within permission groups. Managers are periodically required to confirm that current permissions for which they are the authoriser and employees associated with these permissions are accurate.

v. Password Management

We do not currently have any restrictions set on passwords for length or complexity. We do not force password changes after a certain number of days as it is not proven to be more secure and in cases can lead to less security due to people writing down their new passwords.

vi. Anti-Malware & Patching

The school is running corporate level Anti-Malware with Trend Micro Cloud solution. This also encompasses Antivirus and Anti-ransomware both on site and on our cloud services such as Office 365. The servers and desktops are all connected to Windows Server Update Service and receive security update patches as soon as they are available.

vii. Disaster Recovery & Business Continuity

As part of the organisation's business continuity plan, there is provision to ensure effective processes are in place to both safeguard personal data during a service outage incident and to re-establish secure access to the data to support data subject rights in ongoing service provision. Offsite backups are on secure encrypted servers in redundant UK data centres. Local backups are onto both tape which is securely stored in a different building to the servers and hard drives in the server room.

b. Data in Transit

i. Secure email

The organisation has access for all staff to an Office 365 mailbox. The mailboxes outbound sent traffic is encrypted. The organisation has access to secure email software for communicating with some third parties where licensing agreements permit this. Sensitive data will be sent using such tools where available using Egress system. Where software is not available a system of password protecting sensitive data in email attachments is employed.

ii. Secure Websites

The organisation has access to third party websites which allow for secure upload of personal data. The organisation uses these facilities to fulfil statutory obligations to report personal data to other public authorities.

iii. Encrypted Hardware

Devices which store or provide access to personal data are secured by password access. Remote access to computers on-site which can access personal data is encrypted end to end. It is against policy for external hard drives or memory sticks to contain sensitive or personal data.

iv. Hard-Copy Data

The removal of personal data in hard-copy form is controlled by organisational policy which requires employees to take steps to conceal the data and appropriately secure the data during transport.

These security measures are reviewed annually and approved as accurate and appropriate by the organisation's governance process.