Roding Valley High School

General Data Protection Regulation (GDPR)

Security Measures

⚠ Data Protection is everyone's responsibility ⚠

This document is an outline of the Organisational and Technical Security measures deemed appropriate by Roding valley High School's Data Controller for the nature of the personal data processed by the Controller and any Data Processor acting on its behalf.

Description of Security Measures Employed to Safeguard the Processing of Personal Data

Section One: Organisational

Policies & Documented Procedures

Roding Valley High School as part of the CLP Trust subscribes to the Information Governance Service – IGS and all policies relating to information governance are drafted by IGS and then personalised to fit with the school's information governance processes 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 school's website for transparency.

Roles

Roding Valley High School has the following staff assigned to Information Governance Roles:

- **Data Protection Officer:** Laurie Almond - IGS. This Officer executes the role by reporting the outcome of statutory process to our SIRO
- **SIRO**: Mrs Sharon Jenner – Headteacher acts as the schools Senior Risk Owner
- **Data Protection Lead:** Mr Marius Vermaak – Assistant Headteacher who ensures the school complies with all data protection policies and procedures and manages the administration of data protection matters, reporting to the SIRO.

Training

Roding Valley High School 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.

Risk Management and Privacy by Design

Roding Valley High School 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.

Contractual Controls

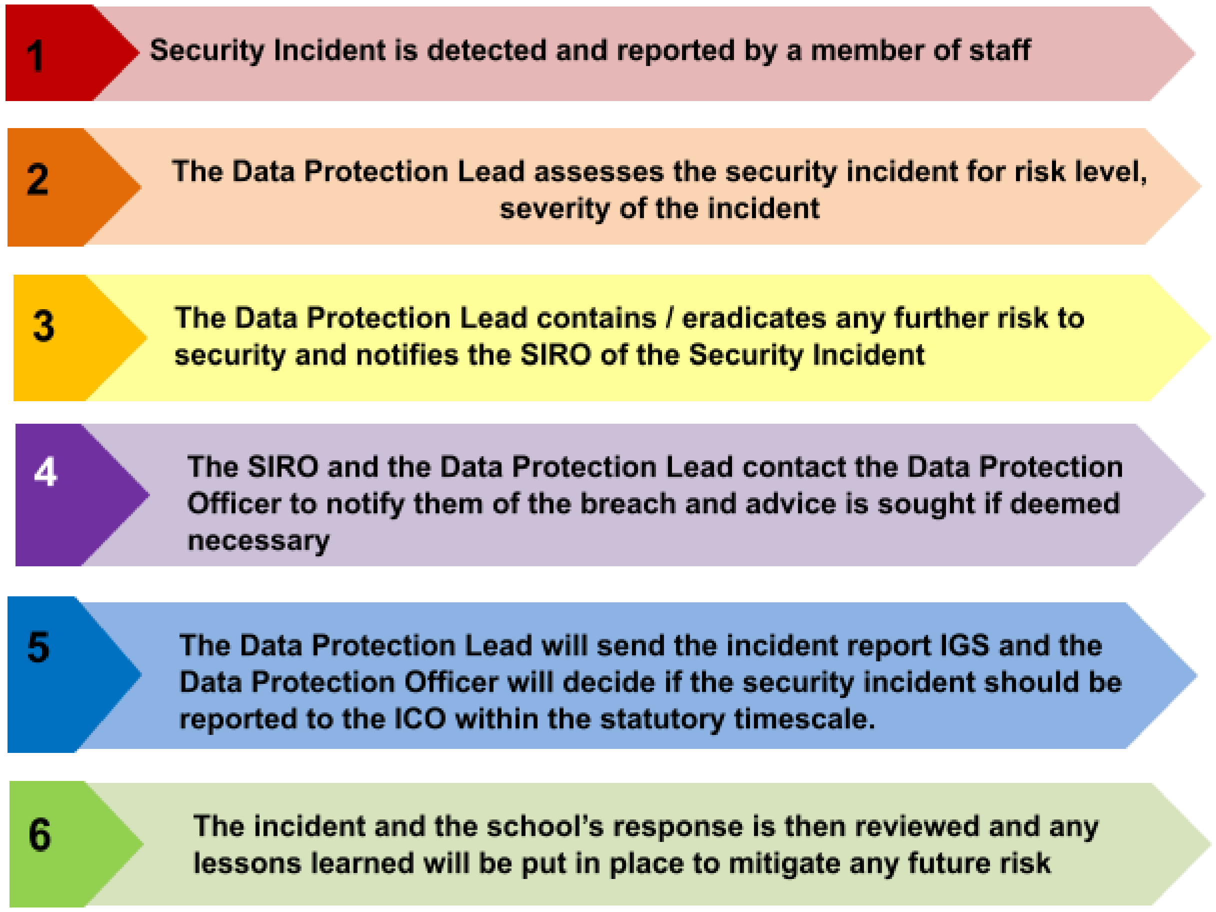
All staff are classed as Data Processors and are handling personal data on behalf of the school and are subject to contractual obligations or other legally binding agreements.

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. Roding Valley High School 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.

Security Incident Management

Roding valley High School maintains a security incident reporting process where all data breaches can be reported by way of completing and submitting a Google Form, this form is available on the GDR page of our Staff Intranet.   The following process is then followed on receipt of a submitted Security Incident:



1 Security Incident is detected and reported by a member of staff

2 The Data Protection Lead assesses the security incident for risk level, severity of the incident

3 The Data Protection Lead contains / eradicates any further risk to security and notifies the SIRO of the Security Incident

4 The SIRO and the Data Protection Lead contact the Data Protection Officer to notify them of the breach and advice is sought if deemed necessary

5 The Data Protection Lead will send the incident report IGS and the Data Protection Officer will decide if the security incident should be reported to the ICO within the statutory timescale.

6 The incident and the school's response is then reviewed and any lessons learned will be put in place to mitigate any future risk

Section Two: Technical

Data at Rest

Use of Hosting Services

Some personal data is processed externally to Roding Valley High School's managed environment by third parties in data centres under agreed terms and conditions which evidence appropriate security measures and compliance with the law.

Firewalls

Access to Roding Valley High school's managed environment is protected by maintained firewalls. Business needs to provide access through the firewall and go through a strictly change control process which includes risk assessment and approval.

Administrator Rights

Enhanced privileges associated with administrator accounts are strictly managed and limited to as few a people as possible

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.

Password Management

Roding Valley High School requires a mandatory password complexity combination of minimum length and characters.

Anti-Malware & Patching

Roding Valley High School has a documented change control process which facilitates the prompt implementation of any security updates provided by the suppliers of active software products.

Disaster Recovery & Business Continuity

Secure backup of all data done on a daily basis. In process of establishing an separate arms-length secure backup to further safeguard critical data

Penetration Testing / Vulnerability Scanning

The internet connection is via LGFL that has an extensive system of evaluating their feed and security of access.

Our network do not have any direct connection to the internet and can therefore not be accessed from any external source

Section Three: Data in Transit

Secure email

Roding Valley High School has access to secure email software for communicating with some third parties where licensing agreements permit this, such as Egress. Sensitive data will be sent using such tools where available. Where software is not available a system of password protecting sensitive data in email attachments is employed.

Secure Websites

Roding Valley High School has access to third party websites, these websites allow for secure upload of personal data. We use these facilities to fulfil statutory obligations to report personal data to other public authorities.

Encrypted Hardware

All devices that provide access to personal data are password secured. Download of data onto portable drives is disabled for all school devices. Remote access into our systems are password protected and do not allow for the download of data to an external drive

Hard-Copy Data

The removal of personal data in hard-copy form is controlled by organisational policy which requires staff to dispose of all confidential documents or documents containing personal data in one of the Secure Shredding Bins located in key areas around the school.
These bins are collected at routine intervals by a licenced secure waste collector and a record is kept of all collections. .

These security measures are reviewed annually and approved as accurate and appropriate by Roding valley High School’s governance process.

Reviewed: May 2022
Next Review: September 2023