Royds

Information Security Policy

Aspiration: Dream Big
If your dreams don't scare you, they aren't big enough!

Resilience: Be Determined
Resilience is a skill, not an ability. It can be learnt.

Respect: Communicate with Kindness
Manners cost nothing but mean everything.

Initiative: Solve Problems
Every problem is a gift – without problems we would not grow.

Reflective: Never Stop Learning
Never stop learning because life never stops teaching.

Approved 16th April 2018

1. Introduction

The school is committed to its obligations for information security under the General Data Protection Regulations (GDPR) for both electronic and paper records. The GDPR specifies that organisations must put appropriate technical and organisational measures in place to safeguard personal data. The Information Security policy outlines the school's approach to achieving this. It should be read in conjunction with other data security policies.

The objectives of this policy are to:

1. establish suitable levels of information security for all school information systems.
2. mitigate risks associated with data breaches e.g. theft, loss, misuse, damage or abuse of these systems.
3. ensure users are appropriately educated and are aware of the school's obligations and need to comply with the GDPR.
4. outline the principles to ensure the school has safe and secure information system environment for users.
5. ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
6. protect the school from liability or damage through the misuse of IT facilities.
7. maintain an appropriate level of security to safeguard confidential information.

The school's security measures seek to ensure:

- only authorised people can access, alter, disclose or destroy personal data.
- those people only act within the scope of their authority.
- if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.

2. Security Environment and Arrangements

The GDPR dictates that organisations must have an appropriate culture of information security to safeguard personal data. The school has designed information security and arrangements to support this. Security measures are appropriate to:

- the nature of the information in question.
- the harm that might result from its improper use, or from its accidental loss or destruction.

In addition to physical and technological security measures, the school has incorporated appropriate management and organisational measures.

2.1 Organisational Controls

The following organisational controls are in place:

- co-ordination between key people in school e.g. the Business Manager, Network Manager and Student Records Manager working closely to ensure the security of key MIS.
- access to premises or equipment given to anyone outside of the school is closely controlled.
- business continuity arrangements that identify how to protect and recover any personal data are in place through appropriate back-ups.

- periodic information compliance audits to ensure that the organisation's security measures remain appropriate and up to date.

2.2 Staff Training and Awareness

Staff have received appropriate data and information security training. The training enables them to:

- identify personal data and understand the importance of protecting it .
- understand school security measures and controls to safeguard personal data.
- familiarising staff with the school's data security policy.
- understand the school's obligations under the GDPR.

Regular refresher training is in place.

2.3 Physical Security Arrangements

The security arrangements for school records and IT storage facilities have been reviewed and the following controls are in place:

- paper records are kept in secure areas and, as far as possible, in locked cabinets.
- there are suitable locks and physical security arrangements in areas where paper records or servers are stored.
- there are appropriate secure disposal arrangements in place across the site using either locked secure disposal bins or shredders.

2.4 Technical Security Arrangements

The school has extensive technical security measures in place to secure the school network infrastructure such as:

- appropriate firewalls and filtering systems.
- password security.
- encryption.

Staff training covers the importance of controls such as encryption, locking IT equipment and not downloading to personal devices.

3. Responsibilities

All members of Royds School, governors, agency staff working for the school or third parties will be users of school information. This carries with it the responsibility to abide by this policy and its principles and relevant legislation, supporting policies, procedures and guidance:

- No individual should be able to access information to which they do not have a legitimate access right.
- No individual should knowingly contravene this policy, nor allow others to do so.

Many members of the school will have specific or overarching responsibilities for preserving the confidentiality, integrity and availability of information. These include:

- Headteacher
- Data Protection Officer
- IT staff.

- Safeguarding Team
- Personnel and Student administration staff
- Safeguarding Team
- Medical and other welfare staff
- SENCO and SEN staff
- Data and Examinations staff.

This includes ensuring that:

- data is appropriately stored.
- the risks to data are appropriately understood and either mitigated or explicitly accepted.
- that the correct access rights have been put in place, with data only accessible to the right people,
- ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms in place.
- information systems both manual and electronic support the school's work.

4. Information Classification

The school's Information Asset Register (IAR) documents all of the school's processing activities to ensure GDPR compliance. Within this, processing activities and data collected are classified according to the sensitivity of the information involved. This is used to inform the information security measures applicable to each processing activity.

The following principles are in place:

- Staff are trained and understand the classification system and security measures required for each level.
- Staff have the lowest level of access to information required to enable them to carry out their role.
- Information has appropriate safeguards based on the classification level.
- Staff understand the importance of reporting data breaches.
- It is possible that information classification may vary at different times e.g. public exam results are embargoed from public release until a date specified by the examination board however the Senior Leadership Team have access to them prior to this.

School security classifications are as follows:

Security Level	Definition	Examples	Security Arrangements
Confidential	Normally accessible only to identified members of school staff. Records will normally be held in an encrypted or suitably secure state outside of the school building or systems.	▪ GDPR-defined Special Categories of personal data including racial / ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health condition, sexual life and biometric information. ▪ Medical information for students and staff unless the data subject or their parent / carer have requested it is shared. ▪ Safeguarding and child protection information. ▪ Large series of personally identifying data (>1000 records) including elements such as name, address, telephone number.	▪ Subject to significant scrutiny in relation to appropriate exemptions/ public ▪ interest and legal considerations. ▪ Password protection, tiered access. ▪ Secure disposal
Restricted	Normally accessible only to specified members of school staff.	▪ GDPR-defined Personal Data: information that identifies living individuals including home address, age, telephone number, schools attended, photographs. ▪ Draft reports, papers and minutes. ▪ Student data analysis ▪ SEN information	Subject to significant scrutiny in relation to appropriate exemptions / public interest and legal considerations.
Internal Use	Normally accessible only to members of school staff or governors.	▪ Internal correspondence, ▪ Final reports, papers and minutes ▪ Information held under license	Subject to scrutiny in relation to appropriate exemptions/ public interest and legal considerations
Public	Accessible to all members of the public.	▪ Annual accounts, minutes of statutory and other formal committees, pay scales etc. ▪ Information available on the LSE website or through the LSE's Publications Scheme.	Freely available on the website or through the school's FOI Publication Scheme

5. Suppliers

All school suppliers, contractors and third parties will abide by the school's Information Security Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance. This includes:

- when accessing or processing LSE assets, whether on site or remotely
- when subcontracting to other suppliers.

6. Cloud Providers

Under the GDPR, a breach of personal data can lead to significant fines. The school's IAR documents where cloud services are used. The school retains responsibility as the data controller for any data it puts into the service. This means the school can be fined for any data breach, even if this is the fault of the cloud service provider. Similarly, it is the school's responsibility to contact Information Commissioner's Office concerning any breach, as well as any affected individual, if required.

The school has put third party data sharing contracts or agreements in place with all third party suppliers who data is shared with. This enables the school to ensure it can judge the appropriateness of a cloud service provider's information security provision.

7. Compliance, Policy Awareness and Disciplinary Procedures

Royds School fosters a culture of data security and awareness. Any security breach of the school's information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems. The loss or breach of confidentiality of personal data is an infringement of the General Data Protection Regulation, contravenes the school's Data Protection Policy.

The loss or breach of confidentiality of contractually assured information may result in financial penalties or criminal or civil action against the school. It is crucial that all users of the school's information systems adhere to the Information Security Policy and its supporting policies as well as the information classification arrangements. All current staff, students and other authorised users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines. Any security breach will be handled in accordance with all relevant school policies, including the appropriate disciplinary policies.

Royds