

DATA BREACH POLICY AND PROCEDURE

To be used following an actual or suspected data breach

| | |
|----------------------------------|------------------|
| Person responsible: | Business Manager |
| Date approved by governing body: | March 2023 |
| Review cycle: | Annually |
| Date of policy review: | March 2024 |

Data Breach Policy and Procedure

The policy should be read in conjunction with the following documents: ICT Policy, Data Protection Policy, Online Safety Policy, Information and Records Retention Policy, Information Security Policy, IT Password Policy, Staff Acceptable Use Policy.

1 Introduction

- 1.1 St Rose's understands the importance of keeping personal data secure and of effectively dealing with data breaches. This is essential for maintaining the trust of staff, students, and their parents when St Rose's uses their information.
- 1.2 This policy and procedure is to be used by St Rose's Data Breach Response Committee in the event of a data breach at St Rose's (or a suspected data breach). The Committee is comprised of the senior members of staff (named at section 3.1 below) who will deal with different aspects of a data breach.
- 1.3 This policy complies with the Data Protection Act 1998 and the General Data Protection Regulation (GDPR).
- 1.4 All staff should receive training on how to recognise a data breach and St Rose's Information Security Policy contains guidance for staff on this issue.
- 1.5 St Rose's is required to report certain breaches to the Information Commissioner's Office (ICO) and to data subjects under the General Data Protection Regulation. There are strict timescales for reporting breaches which are outlined in section 6.
- 1.6 St Rose's also has responsibilities to report certain incidents to other regulators. Section 6 below covers these reporting obligations.
- 1.7 **Immediate action following a data breach.**

- Inform all members of the Data Breach Response Committee if the breach is serious, minor breaches will be reported to the DPO and their response will be noted on the Data Breach Register.
- Identify what personal data is at risk.
- Take measures to prevent the breach from worsening e.g. changing password/access codes, removing an email from students' inboxes which was sent by mistake.
- Recover any of the compromised personal data e.g. use back-ups to restore data.
- Consider whether outside agencies need to be informed as a matter of urgency e.g. the police in the event of a burglary or Children's Services where the breach may lead to serious harm being caused to a student.
- Consider whether any affected individuals should be told about the breach straight away. For example, so that they may act to protect themselves or because they would find out about the breach from another source. Please note this is different to the mandatory notification to individuals covered at 6.6 - 6.10 below which does not need to be an immediate notification.

2 What is a data breach?

2.1 A data breach is a breach of security which leads to any of the following:

- 2.1.1 the loss of personal data;
- 2.1.2 the accidental or unlawful destruction of personal data;
- 2.1.3 the disclosure of personal data to an unauthorised third party;
- 2.1.4 the unlawful or accidental alteration of personal data; or
- 2.1.5 unauthorised access to personal data.

2.2 Personal data is information:

- 2.2.1 from which a person can be identified (either from the information itself or when combined with other information likely to be used to identify the person); and
- 2.2.2 which relates that person.

2.3 The following are examples of personal data held by St Rose's:

- 2.3.1 names and contact details of students, parents and staff;
- 2.3.2 financial information about parents and staff;
- 2.3.3 student exam results;
- 2.3.4 safeguarding information about a particular family;
- 2.3.5 information about student behaviour and attainment; and
- 2.3.6 a student or staff member's medical information.

2.4 If staff are in any doubt as to whether an incident constitutes a data breach they must speak to St Rose's Business Manager, IT Manager or Principal immediately.

2.5 Please see Appendix 1 for examples of data breaches.

3 Roles and responsibilities

3.1 The following staff form St Rose' Data Breach Response Committee (the **Committee**) and will have certain responsibilities:

| <u>Role</u> | <u>Responsibility</u> |
|--------------------|--|
| Business Manager | <p>The Business Manager will chair the Committee and is responsible for co-ordinating St Rose's response to any breach. In addition, the Business Manager will lead on any physical security measures which are required at St Rose's site to contain the breach. The Business Manager is responsible for notifying and liaising with St Rose's Data Protection Officer, IT Manager and insurers as required.</p> <p>The Business Manager will lead on any employee welfare or disciplinary issues in consultation with the Principal.</p> <p>The Business Manager will be responsible for ensuring the security of St Rose's IT infrastructure. In addition, for taking any possible technical measures to recover personal data or to contain a data breach.</p> |
| The Principal | <p>The Principal will be responsible for any communications with students and parents and for any student welfare or disciplinary considerations.</p> |
| The Vice Principal | <p>The Vice Principal will deputise for the Principal or Business Manager as appropriate and will assist in particular with communications with students and parents.</p> |
| Chair of Governors | <p>The Chair of Governors will be responsible for liaising with the Board of Trustees as appropriate. If there is a serious breach it must be reported to the Trustees and the Congregations Finance and H/R Manager.</p> |

3.2 The Committee will form as soon as possible once a data breach has been identified.

4 Containment and recovery

4.1 As soon as a data breach has been identified or is suspected, steps must be taken to recover any personal data and to contain the breach. For example, St Rose's may need to:

4.1.1 change any passwords and access codes which may have been compromised;

4.1.2 if appropriate in all the circumstances, tell employees to notify their bank if financial information has been lost (or other information which could lead to financial fraud) and offer credit protection;

- 4.1.3 limit staff and/or student access to certain areas of St Rose's IT network;
 - 4.1.4 use back-up tapes to restore lost or damaged data;
 - 4.1.5 take any measures to recover physical assets e.g. notifying the police or contacting third parties who may have found the property;
 - 4.1.6 notify its insurers; and
 - 4.1.7 act to mitigate any loss.
- 4.2 The Committee should decide what action is necessary and which member(s) of the Committee will be responsible for the different aspects of the containment and recovery. Where appropriate the Committee will delegate tasks to other members of staff with the relevant expertise.
- 4.3 An interview will be held with the member of staff concerned in the breach and this conversation recorded on the document in Appendix 6.
- 4.4 The Committee should seek assistance from outside experts if appropriate to effectively contain the breach and recover any personal data. For example, legal advice, reputation management advice or specialist technical advice.

5 **Establishing and assessing the risks**

- 5.1 The next stage in the process of dealing with a data breach is to establish and assess the risks presented by the breach. To assist with this process, the Committee should document the answers to the questions contained in Appendix 2 in as much detail as possible.
- 5.2 The table in Appendix 2 should be copied into a new document in order to retain a record of this process.

6 **Notification**

Notification to the Information Commissioner's Office

- 6.1 From 25 May 2018 St Rose's will be required to report a data breach to the ICO unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. The exercise which was documented under section 5 above should be used to determine if a notification to the ICO is required.
- 6.2 "Risk to the Rights and freedoms of individuals" should be interpreted broadly. Please see row 5 of Appendix 2.
- 6.3 Any decision to not notify the ICO should be documented. It is possible that if another data breach occurs in the future that the ICO will ask why any previous breaches were not reported and the ICO is likely to ask to see evidence of any decision to not notify.
- 6.4 If St Rose's decides to notify the ICO then this must be done without undue delay and where feasible within 72 hours of having become aware of the breach.
- 6.5 **Content of the notification**
- 6.5.1 The ICO has set out procedures for notifications on their website (ico.org.uk) which should be followed.
- (a) However, St Rose's should also prepare a letter to the ICO in addition to following the ICO's procedures on the website in all but the most minor

breaches because this provides the opportunity to present what has happened in a way that is advantageous to St Rose's.

- (b) St Rose's may need to send this letter after the initial notification to incorporate any subsequent action taken by St Rose's which may act in mitigation against ICO enforcement action.

6.5.2 The notification must contain as a minimum:

- (a) a description of the nature of the data breach including where possible:
 - (i) the categories and approximate number of data subjects concerned; and
 - (ii) the categories and approximate number of personal data records concerned.
- (b) the name and contact details of the Data Protection Officer who can provide more information to the ICO if required;
- (c) a description of the likely consequences of the data breach;
- (d) a description of the measures taken or proposed to be taken by St Rose's to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

6.5.3 If it has not been possible to submit the notification to the ICO within 72 hours of becoming aware of the breach, the notification must explain the reason for this delay. For example, that St Rose's has been instructed by the police to postpone the notification to the ICO.

6.5.4 If it is not possible to provide all of the information at the same time, St Rose's should provide the information to the ICO in phases without further undue delay. For example, St Rose's could make an initial notification within the 72-hour period with a more detailed response the following week once St Rose's has more information on what happened.

6.5.5 The initial notification should include points such as the possible cause of the breach and how St Rose's plans to deal with the breach including mitigation actions.

6.5.6 The more detailed response should set out as clearly as possible the steps St Rose's has taken to prevent a reoccurrence. The ICO is less likely to take enforcement action if it considers that St Rose's has already taken steps to address what went wrong.

Contacting affected individuals

6.6 St Rose's is required by the GDPR to report a data breach to the individuals whose data has been compromised (known as data subjects) where the breach is likely to result in a high risk to the rights and freedoms of individuals. It may not always be clear which individuals should be notified, for example, parents may need to be notified rather than their children.

6.7 St Rose's should use the exercise at section 5 above to assist with this decision. A notification does not need to be made where:

- 6.7.1 St Rose's had taken measures so that the data compromised was unintelligible to any person not authorised to access it (e.g. it was encrypted); or

- 6.7.2 St Rose's has managed to contain the breach or take mitigating action so that any high risk to individuals is no longer likely to materialise (e.g. an unencrypted memory stick has been recovered before anyone was able to access the data held on it).
- 6.8 If St Rose's decides not to notify individuals this decision must be documented.
- 6.9 If a notification is sent this must be done so without undue delay. St Rose's should work with the ICO in determining when is the most appropriate time to notify the individuals. Other outside agencies, such as the police, may also have a view regarding the timing of this notification.
- 6.10 The ICO may advise or require St Rose's to notify individuals. In addition, the ICO has the authority to require a more detailed notification to be given to individuals. The ICO is given these powers under the GDPR.
- 6.11 Content of the notification to individuals
- 6.12 The notification to individuals must include the following as a minimum:
- 6.12.1 the name and contact details of the Data Protection Officer who can provide more information;
 - 6.12.2 a description of the likely consequences of the data breach; and
 - 6.12.3 a description of the measures taken or proposed to be taken by St Rose's to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- 6.13 In addition, St Rose's must consider if any additional information would be helpful to data subjects. For example, instructions on measures which they can take to protect their data now or in the future.
- 6.14 The notification must be drafted in clear language. If directed at students, the notification should be age appropriate.
- 6.15 The Committee should decide what is the most appropriate method of communication for the notification. Factors to consider include the urgency of the notification. For example, it may be appropriate to telephone individuals followed up with an email.

Notification to the police

- 6.16 St Rose's should consider whether the police need to be notified about the data breach because it is possible that a criminal offence has been committed. However, there is no legal obligation to notify the police. The following are examples of breaches where a criminal offence may have been committed:
- 6.16.1 theft e.g. if a laptop has been stolen;
 - 6.16.2 burglary;
 - 6.16.3 if a staff member has shared or accessed personal data where this was not required as part of their professional duties e.g. a staff member shares information about a student with famous parents with the local press;
 - 6.16.4 St Rose's computer network has been hacked (e.g. by a student or a third party).
- 6.17 Action Fraud is the national fraud and cybercrime reporting centre. It can be contacted on 0300 123 2040 or using www.actionfraud.police.uk.

7 Internal Breach Register

- 7.1 St Rose's is required to keep a register of all data breaches including those which do not meet the threshold to be reported. Staff should be trained to report all data breaches to allow St Rose's to meet this requirement.
- 7.2 The Business Manager is responsible for keeping this register up to date.
- 7.3 The Trustees need to be informed of any serious data breach.

8 Evaluation

Evaluation of St Rose's security measures

- 8.1 St Rose's is obliged under the GDPR to implement technical and organisational measures to protect personal data. St Rose's regularly evaluates the effectiveness of both its organisational and technical measures.
- 8.2 Organisational measures include:
 - 8.2.1 policies for staff on their data protection obligations, including when working away from St Rose's site;
 - 8.2.2 guidance for staff on how to use specific computer applications and software securely; and
 - 8.2.3 data protection training for staff.
- 8.3 Technical measures include:
 - 8.3.1 the use of encryption;
 - 8.3.2 limiting access to certain areas of St Rose's IT network;
 - 8.3.3 firewalls and virus protection; and
 - 8.3.4 the use of backups.
- 8.4 The Committee should establish how the existing measures could be strengthened and what additional measures should be put in place to guard against future data breaches. The Committee should consider both breaches of a similar type to that which has occurred and the risk of security breaches more broadly.
- 8.5 The Committee may delegate this task to one or more appropriate members of staff. The Committee should consider whether legal and/or technical advice is required.
- 8.6 This exercise should be undertaken promptly because the actions taken by St Rose's to improve its practices will likely be taken into account by the ICO when considering if enforcement action should be taken against St Rose's.
- 8.7 Key points to consider include:
 - 8.7.1 Would improvements in the training given to staff have prevented the breach or lessened the severity of the breach?
 - 8.7.2 Can measures be taken to speed up the process of staff reporting breaches?
 - 8.7.3 Does St Rose's Information Security Policy need to be revised?
 - 8.7.4 Are changes required to St Rose's IT system?

- 8.7.5 Should St Rose's document management system be made more robust? For example, should staff's ability to access certain documents be limited to a greater extent.
- 8.7.6 Does the physical security of St Rose's, particularly in areas where personal data is kept, need to be improved?
- 8.7.7 Do St Rose's remote working practices need to change?
- 8.7.8 Does St Rose's need more robust procedures around staff using their own devices for the organisation's work?
- 8.7.9 Do St Rose's' contracts with processors (e.g. a Cloud storage provider) need to be revised?
- 8.7.10 Does St Rose's need to do more robust due diligence on its processors?
- 8.7.11 If any IT services providers were contracted by St Rose's to carry out work related to information security was the service provided adequate?
- 8.8 The Committee should report the outcome of the evaluation to the Leadership and Management team before implementing any necessary changes.

Evaluation of St Rose's response to the data breach

- 8.9 When the immediate action has been taken following the data breach, St Rose's should evaluate how its initial response to the breach could have been better.
- 8.10 Key points to consider:
 - 8.10.1 Was the breach reported to the Business Manager immediately? If not, what action can be taken to speed up the process of contacting a senior member of staff?
 - 8.10.2 Were all possible measures taken to recover the data promptly?
 - 8.10.3 Could more have been done to contain the breach as quickly as possible?
 - 8.10.4 If one of St Rose's processors (e.g. an assessment software provider) was either responsible for the breach, or discovered the breach, was this notified to St Rose's without undue delay? If not, what measures can be put in place to improve this communication in the future?
- 8.11 The Committee should report the outcome of the evaluation to the Leadership and Management team before implementing any necessary changes.


9 Tactical considerations

- 9.1 St Rose's should refer to Appendix 4 which outlines tactical and supplemental considerations. For example, is any student disciplinary action required?

10 Monitoring and review

- 10.1 The Business Manager should ensure that this policy is regularly reviewed and updated as required.
- 10.2 This policy should be reviewed following any data breach at St Rose's which meets the threshold to be reported to the ICO.

**This Policy Statement is considered part of the Terms and Conditions of
Employment for all staff at St Rose's School**

.....


Chair of Governors

Date 15.3.2023

.....


Principal

Date 15.3.2023

Appendix 1 Examples of data breaches and the next steps

| Example of breach | Containment and Recovery | Establishing and Assessing the Risks | Notification | Evaluation of St Rose's's response to the data breach |
|--|--|--|---|---|
| A staff member leaves papers containing information about students' academic performance on a train. The papers were not in a locked case. | St Rose's should find out if it is possible to retrieve the papers. For example, by calling the train company's lost property department. | St Rose's should work through the questions in Appendix 2 below. | <p>If the papers are not retrieved, then this breach will need to be notified to the ICO.</p> <p>Whether a notification to the students and their parents is required will depend upon the nature of the personal data.</p> <p>St Rose's should consult section 6 of this policy.</p> | St Rose's should work through sections 8.9 to 8.11 of the policy above. |
| Ransomware locks electronic files containing personal data. | St Rose's should have a back-up of the data and should also ensure that its systems are secured (e.g. that the ransomware has been removed). | Ditto | Depends on factors such as whether St Rose's was able to recover the data and whether there is any other risk to St Rose's systems | Ditto |
| Sending an email containing personal data to the incorrect recipient. | <p>Use the recall email feature if available.</p> <p>Consider calling the unintended recipient and asking them to delete the email</p> | Ditto | Depends on the sensitivity of any personal data contained in the email, whether the unintended recipient has agreed to delete it etc. | Ditto |

Appendix 2 Establishing and Assessing the Risks Presented by the Data Breach

| | <u>Question</u> | <u>Response</u> |
|----|---|-----------------|
| 1. | Precisely what data has been (or is thought to have been) lost, damaged, or compromised? | |
| 2. | <p>Is any of the data Critical Personal Data as defined in St Rose's's [• Data Protection Policy for Staff and Information Security]? This would be:</p> <ul style="list-style-type: none"> i. information concerning child protection matters; ii. information about serious or confidential medical conditions and information about special educational needs; iii. information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved); iv. financial information (for example about parents and staff); v. information about an individual's racial or ethnic origin; and vi. political opinions; vii. religious beliefs or other beliefs of a similar nature; viii. trade union membership; | |

| | | |
|----|---|--|
| | <p>ix. physical or mental health or condition;</p> <p>x. genetic information;</p> <p>xi. sexual life;</p> <p>xii. information relating to actual or alleged criminal activity; and</p> <p>xiii. biometric information (e.g. a student's fingerprints following a criminal investigation).</p> <p>If any of these types of data are involved this makes the breach more serious.</p> | |
| 3. | Who are the affected individuals e.g. staff, parents, students, third parties? | |
| 4. | How many individuals have definitely been affected and how many potentially affected in a worst-case scenario? | |
| 5. | <p>What harm might be caused to individuals (not to St Rose's)? The individuals do not necessarily need to be those whose personal data was involved in the breach.</p> <p>Harm should be interpreted broadly, for example to include:</p> <p>(a) distress;</p> <p>(b) discrimination;</p> <p>(c) loss of confidentiality;</p> | |

| | | |
|----|---|--|
| | <p>(d) financial damage;</p> <p>(e) identity theft;</p> <p>(f) physical harm; and</p> <p>(g) reputational damage.</p> | |
| 6. | <p>What harm might be caused to St Rose's? For example, reputational damage and financial loss.</p> | |
| 7. | <p>What mitigating factors may have lessened the risks presented by the breach? The following questions may assist when considering this point.</p> <p>(a) Were any physical protections in place to limit the impact of the breach e.g. was the data contained in a locked case when it was lost/stolen?</p> <p>(b) Were any technical protections in place e.g. was the data protected by encryption?</p> <p>(c) Have measures been taken to contain the breach e.g. have banks being notified where financial information has been compromised?</p> <p>(d) Have measures been taken to recover the data e.g. has lost data been found before being seen by any unauthorised party or have back-ups been used where electronic information was lost or damaged?</p> | |

Appendix 3 External advice

Legal advice

St Rose's should consider taking legal advice in relation to the following. Please note that this is not an exhaustive list but should be used as a guide.

1. Determining whether to notify the ICO and the data subjects.
2. Drafting the notification to the ICO and the data subjects.
3. Drafting a serious incident report to the Education and Skills Funding Agency.
4. Any correspondence with other external agencies such as the Department for Education.
5. Any communications with the police.
6. The decision to notify St Rose's insurers.
7. Any communications with staff members, students and parents.
8. Any disciplinary action in relation to students or staff.
9. Establishing whether there is a risk that an affected individual might bring a legal claim against St Rose's.

Reputation management

St Rose's should consider obtaining advice regarding reputation management. This advice may be provided by solicitors or by other specialists. As above, this is not an exhaustive list but should be used as a guide.

The following circumstances in particular may require specialist advice:

1. If the data breach becomes widely known to the parental community.
2. If news of the breach becomes known outside of St Rose's community.
3. If the media report on the breach or ask St Rose's for a statement.
4. If the ICO take enforcement action which may become public knowledge.

Appendix 4 Tactical and supplemental considerations

This appendix should be completed to assist St Rose's in checking that all issues surrounding the data breach have been considered. It is not an exhaustive list but may assist the Committee when handling the consequences of the data breach.

| Supplemental issue | Considerations |
|-----------------------------|----------------|
| Student welfare | |
| Staff welfare | |
| Parental complaints | |
| Staff disciplinary action | |
| Student disciplinary action | |
| Reputation management | |
| Risks of legal claims | |
| Possible ICO action | |

Appendix 5 Data Breach Register Template

The Business Manager is responsible for keeping this register up to date.

| Date of breach | Outline of facts | Effect of the breach | Remedial action taken | Regulatory bodies informed if any e.g. ICO |
|----------------|------------------|----------------------|-----------------------|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Appendix 6 Record of meeting with staff concerned with a data breach

| GDPR Breach of Information meeting | |
|------------------------------------|--------------------|
| Name of staff member: | Name of manager: |
| Date of meeting: | People present: |
| Breach reference number | |
| Summary of Breach of Information | |
| Record of discussion | |
| Key points emerging | |
| Staff member's comments | Manager's comments |

Decision of Breach Committee regarding reporting

If reported to Data Protection Officer - date and comments

If reported to Information Commissioners Office – date and comments

Signed (staff member) Date

Signed (Data Breach Response Committee Member) Date

