Rydes Hill Preparatory School & Nursery
P59– Data Breach Policy

CHILDREN'S MISSION STATEMENT

Think deeply, live wisely, love generously

MISSION STATEMENT

IN OUR SCHOOL WE WILL TRY TO:

- ❖ Rydes Hill Preparatory School and Nursery is a Catholic school where children learn how to live in loving relationship with God and each other.
- ❖ Christian virtues of love and justice, faith and courage, hope and perseverance are fostered.
- ❖ Pupils and staff comprise individuals of different faiths and beliefs but the Rydes Hill community aspires to unity within the life of the school on shared moral values.
- ❖ The importance placed on the development of individual talents is at the heart of what the school stands for and all are encouraged and challenged to be the best they can be.

Written By :	Martin Halsall - Bursar	March 2022
Reviewed By :	Sarah Norville – Headmistress	23rd May 2022
Approved By :	SLT	24th May 2022
Governor Review By :	N/A	

Contents

Revision History

Revision	Paragraph Number	Revision
May 2022		New Document

Abbreviations, Acronyms and Definitions

Abbreviation / Acronym	Definition
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office

Introduction

1. The School is committed to keeping individuals' personal data secure and has policies, staff training and appropriately designed system security in place to achieve this. However, as there is always the risk that a data breach may occur, this policy sets out the procedure and considerations for dealing with such breaches.
2. Under the UK GDPR, all data breaches that occur within the School must be recorded on the School's Data Breach register. Those breaches that are deemed likely to result in "a risk to the rights and freedoms of natural persons" must be reported to the Information Commissioner's Office (ICO) within 72 hours of the School being aware of the breach. Where the breach is deemed likely to result in "a high risk to the rights and freedoms of natural persons" the individuals affected should be notified without undue delay.
3. This policy explains:
   - what is meant by a data breach;
   - what data breaches need to be reported to the ICO and potentially to individuals;
   - the procedure that should be followed upon discovering a breach;

What is meant by a data breach?

4. A personal data breach is a security incident that has affected the confidentiality, integrity or availability of personal data. Data breaches can be a result of both accidental and deliberate causes. It is classed as a personal data breach whenever any personal data is:
   - lost;
   - destroyed (except planned deletions in line with the School's retention policy);
   - corrupted;
   - disclosed (if someone accesses the data or passes it on without proper authorisation); or
   - made unavailable (and this unavailability has a significant negative effect on individuals).

   Examples of personal data breaches include:

   - sending personal data to an incorrect recipient;
   - displaying personal data of pupils on a screen to other pupils;
   - the theft or loss of computing devices which contain personal data;
   - the alteration of personal data without permission;
   - unauthorised access to personal data on systems or paper.

What data breaches need to be reported and to where?

5. All data breaches that occur within the School need to be reported to the Privacy Officer at bursar@rydeshill.com Any data breaches that occur at one of the School's third party data processors that impact personal data from the School also need to be reported to the Privacy Officer. All data breaches must be investigated and documented in the School's internal Data Breach Register by the Privacy Officer, in accordance with the procedure laid out in this policy.

6. If a data breach is likely to result in discrimination, damage to reputation, identity theft or fraud, financial loss, loss of confidentiality or any other significant economic or social disadvantage then it should be reported to the ICO within 72 hours of the School being aware of the breach. Breaches can be reported to the ICO using their personal data breach helpline, 0303 123 1113. Breaches will be reported to the ICO by the Privacy Officer.

7. When reporting a breach to the ICO, the following information should be provided:

   - a description of the nature of the personal data breach including:
     - the categories and approximate number of individuals concerned; and
     - the categories and approximate number of personal records concerned.
   - the name and contact details of the privacy officer;
   - a description of the likely consequences of the personal data breach; and
   - a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

8. If it is not possible to investigate the breach fully within 72 hours, it is allowable to provide the information to the ICO in phases, the initial notification happening within the first 72 hours.

9. If a data breach is highly likely to result in discrimination, damage to reputation, identity theft or fraud, financial loss, loss of confidentiality or any other significant economic or social disadvantage then it should be reported to the ICO within 72 hours of the School being aware of the breach and to the individuals whose data was involved without undue delay. The ICO can give guidance as to whether a data breach has reached this higher category and requires individuals to be notified.

10. In notifying individuals of a data breach the following information must be given:

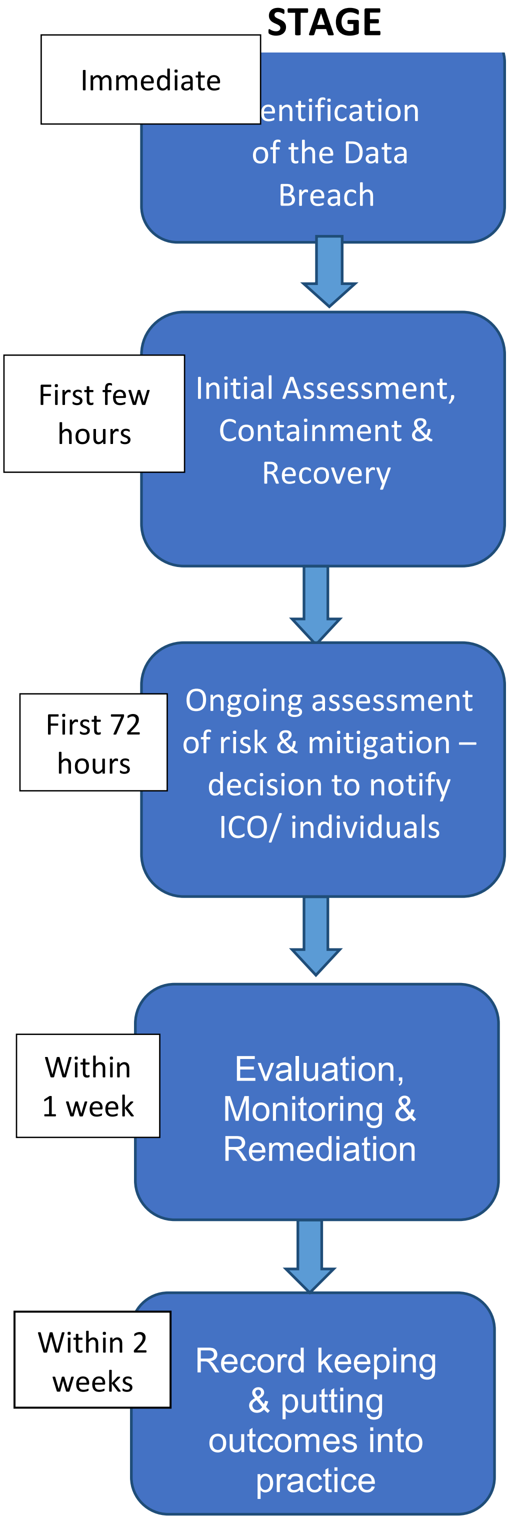
    - a description of the nature of the personal data breach, including the name and contact details of the privacy officer;
    - a description of the likely consequences of the personal data breach; and
    - a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures the School has taken to mitigate any possible adverse effects and any action that they can take themselves to mitigate these effects.

11. Where it is decided that a breach does not need to be notified to the ICO (and individuals) the rationale for not notifying must be documented and included in the breach register.

12. Where a report is made to the ICO, the School should subsequently notify the Charity Commission and, if appropriate, the Fundraising Regulator.

The procedure to be followed on discovering a breach

This procedure identifies the process that the School will follow in investigating a breach, taking appropriate action to mitigate the breach and prevent similar breaches happening again in the future and, where necessary, notifying the ICO (and individuals). All the actions and information relevant to each stage need to be documented and recorded in the School's breach register (file of breach investigations), regardless of whether a breach is notified to the ICO or not.



STAGE

Immediate

entification of the Data Breach

- Gather information about the breach (using form in Appendix 1) – what, when, how, where, who.
- Notify the Privacy Officer in person or by email at bursar@rydeshill.com
- Depending on the level of the breach, the privacy officer will involve relevant staff in the following stages. For the most serious breaches, a critical incident team would be formed.

First few hours

Initial Assessment, Containment & Recovery

- Determine the timescales of the breach, what data is involved and where that data has gone to.
- Identify what immediate steps can be taken to contain the data now or to recover the data.
- If a cyber breach, involve the school's IT manager.
- If people are involved, can they be contacted to give assurances
- Determine if specialists are needed: e.g. IT consultants; legal.

First 72 hours

Ongoing assessment of risk & mitigation – decision to notify ICO/ individuals

- Build up a full picture of the breach – number of individuals affected, types of personal data involved, being particularly aware of any sensitive or financial data involved.
- Identify if a crime has been committed – if so, involve the police.
- Assess the likely risk of harm to the individuals and decide whether the breach needs reporting to the ICO (and individuals).
- Determine what can be done to mitigate the risk.
- Report to ICO (and individuals) if required (using information collected in Appendix 2), otherwise document rationale for not reporting.

Within 1 week

Evaluation, Monitoring & Remediation

- Continue to monitor and assess possible consequences.
- Review internally to identify how the breach occurred, how it could have been prevented, what follow-up action is needed to prevent a similar breach happening in the future.
- Where the ICO (and individuals) have been notified, keep them informed, as appropriate, as new information comes to light and tell them what is being done to improve practices.

Within 2 weeks

Record keeping & putting outcomes into practice

- Keep a full internal record, whether or not the matter was reported to the ICO.
- Log this record against wider trends and compare with past incidents.
- Ensure any recommendations made by, or promised to, the ICO are actioned and make sure any follow-up action is implemented.
- Review policies and ensure regular (or specific) training is completed.
- Notify the Charity Commission if the breach was reported to the ICO.

Appendix 1 - Information to be gathered upon discovering a breach

To be completed by the member of staff who first becomes aware of the breach and given to the Privacy Officer (the Bursar), as soon as possible after the breach is identified. We have just 72 hours from the point that the first member of staff is aware of the breach in which to investigate the breach, assess the impact and notify the ICO if this is needed.

Please complete in as much detail as possible.

Description of the data breach. What happened, the names of the people involved, where known? When did the breach happen? Where did the breach happen? How and when did you become aware of the breach?

Whose data has been affected (lost, stolen, or shared or altered without proper authorisation)? What type of data is involved? Eg home address, email address, telephone number, assessment grades, medical details, SEN details. Was sensitive personal data involved? Eg medical / SEN / financial?

If the data has been shared, who has it been shared with who should not have seen it?

Name of Person reporting the breach ______________________________

Date of the report ____________________ Time of the report ______________

Appendix 2 - Information to be gathered in the investigation of the breach

Information to be recorded in the breach register and, where necessary, given to the ICO when notifying them of the breach.

When and how did the School become aware of the breach?
Description of the data breach. What happened? When did the breach happen? Where did the breach happen? How did it happen?
How many people’s data could be affected? Who could be impacted? (Category not names eg staff, pupils, parents/guardians). What sort of data has been breached?
What controls did you have in place that could have prevented the breach?
What has been done to contain the breach or retrieve the data?
What risk is there to the individuals whose data this has impacted? What could be the impact? What is the likelihood that individuals will suffer serious consequences as a result of the breach?

Does this breach need reporting to the ICO (and individuals, where necessary)? Give reasons.
Actions that have been taken or will be taken to mitigate the impact for the individuals affected?
What has been learned? What actions need to be taken to avoid a similar breach happening in the future?
What other organisations or regulators have been or will need to be notified? When done, by whom?

Name of Person reporting the breach to the ICO ______________________

Date of the report ______________ Time of the report ______________

Name of contact at the ICO ______________ ICO Case Number ______________