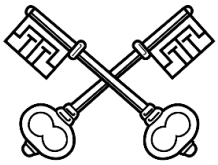

RADLEY

Data Breach Policy

January 2024

Data Breach Policy

Data Protection - Data Breach Procedure for Radley College

Radley College holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Radley College and all school staff, governors, volunteers and contractors, referred to herein after as 'staff'.

Procedure (all staff)

This breach procedure sets out the course of action to be followed by all staff at Radley College if a data protection breach takes place.

- Staff member should notify their Head of Department without undue delay after becoming aware of a personal data breach. In the case of IT related breaches the IT systems manager should be contacted immediately (out of work hours use the IT emergency number)
- Heads of Departments should then inform the IT Systems Manager and the Bursar.
- The notification referred to above should at least:
    - Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
    - Describe the likely consequences of the personal data breach;
    - Describe any measures you have already implemented (please get advice before doing this in almost all cases)
    - In the case of compromised user passwords change the passwords immediately

Note: In the case of a personal data breach, we may be required to inform the ICO no later than 72 hours after having become aware of it.

Types of Breach

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored.
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Poor data destruction procedures.
- Human error.
- Cyber-attack.
- Hacking.
- Leaving paper documents in unlocked office or classroom.
- Losing anything that contains personal data.

Managing a Data Breach (for SMT and IT staff)

In the event that the school identifies or is notified of a personal data breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the IT Systems Manager and Bursar.
2. IT Systems Manager and Bursar (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff.
3. Bursar (or nominated representative) must consider informing Council as soon as possible, it is the school's responsibility to take the appropriate action and conduct any investigation. This would be appropriate where it is believed the breach is likely to be notifiable to the Information Commissioner's Office ("ICO").
4. Bursar (or nominated representative) must also consider whether the police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the school's legal support should be obtained.
5. IT Systems Manager and Bursar (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:
    - Attempting to recover lost equipment.
    - Contacting the relevant departments, so they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the IT Systems Manager and Bursar (or nominated representative).
    - The use of back-ups to restore lost/damaged/stolen data.
    - If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
    - If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the IT systems Manager or Bursar (or nominated representative) to fully investigate the breach. The IT systems Manager or Bursar (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- It's sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the ICO. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Bursar (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the ICO must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the school is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the school's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the IT systems Manager or Bursar (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported at the next available Senior Management Team and Council meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Head of HR for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The Bursar should ensure that staff are aware of the school's Privacy Statement and Data Processing Procedures and their requirements including this Data Breach Policy. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the school's Privacy Statement and Data Processing Procedures, they should discuss this with their Head of Department.