Radnor House
SEVENOAKS
celebrating every individual

Data Breach Policy

Policy Statement

Radnor House Sevenoaks holds large amounts of personal and sensitive data. Every care is taken to protect personal 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 the school and all staff. This policy must be read in conjunction with the School's Data Breach Response Plan (internal procedural document for staff), Data Protection Policy, Data Privacy Notices, and Records Management Policy including Data Retention Timescales.

Purpose

This Policy sets out the course of action to be followed by all staff at the school if a Data Breach occurs. The General Data Protection Regulations explain that:

' A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.'

Managing a Data Breach

If a member of staff becomes aware that a data breach may have or has occurred they WILL take the following steps **immediately**:

Notify the Business Manager, IT Service Manager or Compliance Officer and their own line manager. This can be done in person, or by email setting out the nature of the incident, the date it occurred, those involved and the type of data potentially accessible/accessed/disclosed. If notified in person, the details must be confirmed by email immediately after this has been done. The Business Manager will, in liaison with any other relevant member of staff, on receipt of the above notification, immediately establish whether a data breach is still occurring. If so, they will ensure that steps are taken immediately to minimise the effect of the data breach and notify the police and/or the School's insurers, where appropriate.

If the breach occurs or is discovered outside of normal working hours, an email should be sent to the Business Manager and their line manager as soon after discovery as possible.

The Business Manager will, in liaison with the Compliance Officer and I.T. Services Manager and any other relevant member of staff, on receipt of the any notification of a data breach, whether by a member of staff or by a contractor, such as an IT provider, immediately seek to establish the likelihood and severity of the resulting risk to individuals' (the data subjects involved in the breach) rights and freedoms. This will be done by conducting a Data Breach Risk Assessment within 24 hours of the breach occurring.

This will 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
- Its sensitivity
- What protections were in place (eg. 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 (such as pupils, staff members, suppliers) and whether there are wider consequences to the breach

Following the conclusion of the risk assessment process, if it IS likely that there may be a risk to the Data Subject's individual rights and freedoms, then the Business Manager MUST notify the Information Commissioners Office (ICO) without undue delay and, where feasible, **not later than 72 hours of having become aware of the data breach.** A copy of any notification to the ICO should be emailed to the Finance and Operations Director.

If it is considered unlikely that the data breach will result in a risk to the rights and freedoms of individuals then there is no necessity to notify the ICO. The school will keep a record of the basis on which the assessment of the risk was made.

Reporting to the ICO

When reporting a data breach to the ICO, the notification must provide:

- A description of the nature of the data breach including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned;
- The name and contact details of the Business Manager or other contact point where more information can be obtained;
- 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 data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

In the event that it has not been possible to fully investigate the data breach within 72 hours of having become aware of it, the notification should explain that not all the relevant details are yet available and when it is expected that this information will be available.

The ICO helpline can offer advice about whether data subjects need to be informed of the data breach. If they consider that the data breach is likely to result in a high risk to the rights and freedoms of individuals, then those individuals must be notified as soon as possible. The Business Manager will keep a record of the basis on which the assessment of the risk was made. This notification to the data subjects involved should describe, in clear and plain language, the nature of the data breach and, at least:

- A description of the likely consequences of the data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects

Ongoing Evaluation, Monitoring and Remediation

As well as recording details on the Data Breach Risk Assessment, a clear record will also be made of the actions taken to mitigate the effects of the breach after the event, to seek to ensure that it does not happen again. This

could include staff training to improve future performance, procedural changes or technological development (this list is not exhaustive).

The school will also take appropriate steps to recover data and minimise risk including:

- Informing people/agencies such as the police, banks, relevant contractors and server administrator
- Reporting and attempting to recover lost equipment
- Informing the school's marketing department with a view to managing a press release about the data breach
- Informing staff about the data breach and to warn them of possible 'blagging attempts'
- Accessing back-ups to replace lost or damaged data
- If the data breach included entry codes or passwords, then these must be changed immediately and involved users informed

Once the data breach has been contained, a full report will be sent by the Compliance Officer to the Finance and Operations Director setting out both the causes of the data breach and the effectiveness of the school's response. The review should include the following considerations:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie including identifying any further potential weak points within the existing security measures
- Whether methods of transmission are secure and the sharing of data limited to the minimum necessary
- Staff awareness
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security
- Whether any changes to systems, policies and procedures should be undertaken

If systemic or ongoing problems are identified, then an action plan will be drawn up to remedy these, which will be monitored by the Compliance Officer.

If the data breach warrants a disciplinary investigation, this will be carried out in accordance with the school's Staff Disciplinary Policy.

Staff Training

The school will ensure that staff are aware of the provisions of its Data Protection Policy and other associated policies and their requirements regarding the handling of personal data including the procedures contained in this Policy. Such training is part of staff induction and ongoing training and supervision.

Signed

Fraser Halliwell
Head
Aug 2022