DATA BREACH POLICY

Under the GDPR and the Data Protection Act 2018, all organisations acting as data controllers must report security breaches involving personal data to the relevant supervisory authority if the breach is likely to result in a risk to individuals' rights and freedoms.

Such breaches must be reported without undue delay and, where feasible, within 72 hours of becoming aware of the breach. In some instances, you may need to report the breach without undue delay to the data subject to enable them to act to protect their fundamental rights and freedoms. There is also a requirement to keep a record of such breaches.

While the GDPR is in relation to 'personal data', breaches involving any kind of data should also be reported internally and to appropriate personnel in accordance with this policy.

This policy should be considered in conjunction with:

- The internal data security policy.
- The management and retention of records policy.
- Personnel record keeping policy.
- The privacy notices.
- The ICT policies.

Responsibilities

All employees, workers, governors, and consultants are responsible for reporting any data breaches they discover, or are responsible for, and for assisting in investigations where required.

Data breaches must be reported to the data protection officer (DPO) to consider what actions need to be taken with management and IT to address the incident, including whether to report the incident to the Information Commissioner's Office (ICO) and any affected individuals.

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data. Broadly, it can be defined as a security incident that compromises the confidentiality, integrity or availability of personal data.

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored.
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error.
- Unforeseen circumstances, such as a fire or flood.

- Hacking attack.
- ‘Blagging’ offences where information is obtained by deceiving the organisation that holds it.

However, the breach has occurred, there are four important elements to any breach management plan:

- Containment and recovery.
- Assessment of ongoing risk.
- Notification of breach.
- Evaluation and response.

What are the school’s responsibilities?

We process personal data on behalf of our pupils, their parents or guardians and all personnel connected within the school, including our staff and volunteers. Under the GDPR, we are classed as a ‘data controller’ and we are therefore responsible for ensuring compliance with the various laws in place to protect individual privacy rights. We have privacy notices in place for the various categories of individuals whose data we process.

Where we engage third parties to process personal data on our behalf, such as payroll, we must also ensure that they process our data in a way that is compatible with the GDPR to ensure that the personal data is not compromised in anyway. We have set up arrangements to ensure that any third parties we engage, known as ‘data processors’, are GDPR compliant and have in place appropriate breach protocols and notification requirements.

While this policy is largely focused on personal data and our obligations under the GDPR, internal data and commercially sensitive data must likewise be protected and secure. Data breaches relating to any sort of data should be reported to the DPO.

What to do if you suspect there has been a data breach regarding personal data?

Data breaches could involve anyone’s personal data that we process at the school. Do not investigate the matter yourself. Complete an incident form and pass it to the DPO. Please see appendix 1 for the data breach incident form. Due to the legal requirements of reporting personal data breaches within 72 hours, or such reasonable time, it is crucial that breaches are addressed immediately. Do not ignore them because the consequences may be worse, and can include substantial fines and penalties as well as personal repercussions for you.

Subject to the Data Protection Act 2018 section 68, where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the data subject should be informed of the breach without undue delay. Not all data breaches have to be reported to the ICO. You can take a self-assessment to help determine whether it is necessary to report to the ICO. This is available at https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/.

If the breach involves the compromising of servers/IT security systems, you should also contact the IT department, so that immediate action can be taken to limit any damage/exposure.

What happens next?

Data breaches, whether they involve personal data or not, will be considered in line with our data breach protocol (appendix 2). You may be required to assist with the investigation process and/or help resolve any security incidents as part of your role.

APPENDIX 1

DATA BREACH INCIDENT FORM

Description of the data breach	
Time and date the breach was identified and by whom	
Who is reporting the breach: name/job title	
Contact details: telephone/email	
Classification of data breached • Personal data • Internal data • Confidential data • Highly confidential data • Commercial data	
Volume of data involved	
Confirmed or suspected breach?	
Is the breach contained or ongoing?	
Who has been informed of the breach?	
Any other information	

APPENDIX 2

DATA BREACH PROTOCOL

This protocol sets out what we need to do in the event of a data breach. Stage one below is covered by the data breach policy. However, stages two to four will be carried out by the DPO with appropriate support from other personnel, such as IT support.

The data breach protocol comprises four stages

- Incident report to the DPO.
- Containment and recovery/investigation and assessment of data breach.
- Consideration of reporting requirements to ICO/individual.
- Evaluation and response, record of breach kept, consideration of any additional security measures needed.

Stage one – incident report

Any data breaches must be reported to the DPO immediately in line with the data breach policy above.

Stage two – containment and recovery/investigation and assessment

Containment and recovery

Depending on the type of breach incident, it may be appropriate to take immediate steps to contain the threat or recover the data. Consult with IT and management.

The requirement to report breaches to individuals in high risk cases may require the DPO to notify individuals whose personal data has or may have been compromised of the situation straightaway. This consideration should be kept under constant review throughout the process.

Any 'data processor' breaches by any of the third parties we engage should also be reported to us to enable us to take appropriate action.

Investigation and assessment

Investigating the incident will involve:

- Considering the incident report.
- Discussing matters with appropriate personnel and obtaining relevant reports/statements.
- Finding out what has happened and what data is affected.
- Consideration of whether the data is high risk, commercially sensitive or includes personal data/special categories of personal data.
- Keeping a timeline/log and updating the developments of the breach.

- Consideration of whether, in the case of personal data, the breach affects the fundamental rights and freedoms of the data subject with regard to:

    - Any resulting 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.

    - The severity of the breach generally.

Stage three – breach reporting
Given the length of time that incidents have to be reported by, it may be appropriate to report the incident without having fully investigated the issues. Matters may develop, and a log should be kept as they do.

If the breach does impact on the rights and freedoms of the data subject(s), report the breach to the ICO if appropriate at https://ico.org.uk/for-organisations/report-a-breach. A self-assessment can be carried out by the DPO to consider whether the breach requires reporting to the ICO https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/.

Notify any data subject of the personal data breach if appropriate where there is a high risk and without undue delay. This will allow the data subject to mitigate any immediate risks of damage. Notification should include:

- Details of the personal data breach.
- Details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the breach including any measures to mitigate any possible adverse effects.

Consideration must be given to whether our insurers need to be informed.

Stage four – evaluation and response
The final breach report should include a summary of the facts of the breach, its effects and the remedial action we have taken. Consideration of whether the issue is human error or not and how reoccurrence can be prevented.

Review of the measures in place – administrative, technical and organisational.

A record must be kept of all breaches.