Data Breach Policy

Table of Contents

Introduction

The Leys School ("the School") processes personal data and special category data (see definitions below) relating to the School, its pupils, their parents and/or guardians ("Parents"), its staff, Governors, alumni and other third parties. As Data Controller, the School has responsibilities under the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 and other applicable legislation to ensure its security and confidentiality. Whilst every care is taken to protect data and avoid a security incident, in the unlikely event of such an occurrence, it is vital that appropriate actions are taken to minimise the associated risks as soon as possible.

If a data security breach occurs, the School's main objectives are to:

- prevent further misuse, alteration, unauthorised disclosure or loss of data;
- recover data that has been lost;
- identify risks arising from the breach;
- notify the appropriate parties in the appropriate timeframe;
- take actions to help prevent future breaches.

Purpose

The purpose of this Policy is to assist staff to:

- identify a data security breach;
- understand the main causes of data security breaches and reduce the associated risks;
- take appropriate action in the event of a data security breach.

Related Policies:

- Data Protection Policy
- Online Safety Policy

- Acceptable Use Policy for Staff
- Information Security Policy

Responsibility

The School's Senior Legal and Compliance Officer has overall day-to-day responsibility for breach notification within the School, including being the designated point of contact for personal data breaches. This responsibility may also be delegated to other members of the Compliance Department.

The School has appointed an external Data Protection Officer (DPO) who is responsible for overseeing this policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed.

The DPO's contact details are set out below: -
Data Protection Officer: Judicium Consulting Limited (Lead Contact: Craig Stilwell)
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174

Definitions

"Breach Notification Team" means the designated staff members at the School collectively responsible for carrying out an investigation into School data security breaches.

This team is made up of the following members of staff:

- Martin Priestley (Headmaster): head@theleys.net, or 01223 508903;
- Paul McKeown (Bursar): pdm@theleys.net, or 01223 508902;
- Damian Glasfurd-Brown (Director of IT): dgb@theleys.net, or 01223 508667;
- Fiona Oliver (Senior Legal and Compliance Officer): compliance@theleys.net, or 01223 854 861 who may also delegate this responsibility to the School's Compliance Officer, Avneet Marwaha who can be contacted on the same email and phone number.

"Data Controller" means a person or organisation who determines the purposes for which and the manner in which any personal data are, or are to be processed. The School is a data controller.

"Data Processor" means any person (other than an employee of the data controller) or organisation who processes data on behalf of a data controller.

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Special Category Data" are personal data revealing a person's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, genetic or biometric data, and personal data relating to criminal offences and convictions.

Types of Data Security Breach

Under the UK GDPR a personal data breach means an improper use of security leading to the accidental or unlawful destruction, misuse, loss, alteration, unauthorised disclosure of or access to, personal data.

It is important to remember that a breach can be more than just losing personal data. For clarity, please see the below definitions:

- 'Unauthorised destruction': where personal data is destroyed or deleted without an approved disposition, when the record has been approved for permanent retention, or when the record is subject to another requirement to retain the record.
- 'Damage': where personal data has been altered, corrupted or is no longer complete.
- 'Accidental loss': where the data may still exist, but the School has lost control of or access to it, or no longer has it in its possession.
- 'Unauthorised processing': includes disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data.
- 'Unlawful processing': any other form of processing which violates the law.

The most common reasons of a breach include:

- human error (for example, sending an email to the wrong recipient);
- theft or loss of data on paper or equipment on which the data is stored (e.g. a mobile device, papers, laptop or tablet);
- inappropriate access controls allowing unauthorised use or sharing of data;
- hacking or phishing scams;
- accidental loss, deletion or damage of data;
- hardware or equipment failure or software corruption;
- 'blagging' where data is obtained through deception;
- natural disasters such as a flood or fire.

Breach Prevention

All staff, Governors and third-party data processors used by the School are responsible for protecting the School's data from potential misuse, loss, unauthorised access, modification and disclosure and assisting the School in fulfilling its duties under data protection legislation. Staff must abide by the School's data protection policies and guidance and exercise a common-sense approach to data security. If in doubt, staff should always consult the Compliance or IT team for advice. A breach of this policy may amount to a disciplinary offence and be addressed in accordance with The Leys and St Faith's Schools Disciplinary Policy and Procedure. Data Processors must abide by the terms of the relevant Data Processing Agreement, or other relevant Terms and Conditions, in place.

Reporting data protection concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage all staff and adults/third parties working on behalf of the School to report any concerns and near-misses (even if they do not meet the criteria of a data breach or a data breach was narrowly avoided) that they may have to the Compliance Department or the DPO. This can help capture risks as they emerge, protect the School from data breaches and keep our processes up to date and effective.

Recognising a suspected Data Breach

When assessing whether there has been a data breach, staff and data processors should consider the following questions:

- Have any errors been made when processing data?
- Is data known, or suspected, to be missing?
- Has data been sent to the wrong recipient?
- Has there been a breach of the terms of the School's Data Protection Policy, Information Security Policy or Privacy Notices?
- For data processors, have the terms of a Data Processing Agreement or the data protection/confidentiality clauses of other Terms and Conditions in force, been breached?

Appendix 1 can be used to assist individuals in establishing whether a data breach has taken place and the potential severity of that breach. If the answer is yes to any of the above, you have identified a potential data security breach and must report it.

If in doubt, contact the Compliance Department (compliance@theleys.net).

Reporting a Data Breach

Prompt reporting of a data breach improves the School's capability to assess risks, contain the impact of the breach and notify third parties where applicable.

Reporting a Data Breach to the Compliance Department

All data breaches must be reported to the Compliance Department immediately on discovery. If there is not a member of staff from the Compliance Department available, another member of the Breach Notification Team must be notified. If it is very urgent and/or serious in nature, we would recommend attempting to contact the department by phone. When a breach is reported, a member of the Compliance Office will ask the reporting individual to complete and immediately return the Suspected Data Breach Form at Appendix 2. A member of the Compliance Department will then record the incident in the Breach Log, a copy of which is attached at Appendix 3 and notify the Breach Notification Team if necessary.

Once staff have reported the incident to the Compliance Department, no further action should be taken in relation to the breach by the staff reporting it. In particular, the reporting staff must not notify any affected individuals or regulators or investigate further. The Compliance Department will acknowledge each breach report form and take appropriate steps to deal with the matter in collaboration with the School's DPO.

Reporting a Data Breach to the Data Subject/s Concerned

The Compliance Department will ensure that the nominated Governor for data protection is informed of a reportable breach, as appropriate, and as soon as practicable.

Reporting a Data Breach to the ICO (the Information Commissioner's Office)

The School does not need to report every data breach to the data protection regulator (ICO). However, for data security breaches that result in a risk to people's rights and freedoms, the School is under a legal obligation to notify the ICO, without undue delay and within a strict timeframe (maximum 72 hours) or risk a significant financial or other penalty. This deadline is applicable regardless of School holidays. If there is a delay in meeting the deadline, written reasons will be recorded as to the reason for the delay.

Examples of where the breach may have a significant effect includes:

- Potential or actual discrimination;
- Potential or actual financial loss;
- Potential or actual loss of confidentiality;
- Risk to physical safety or reputation;
- Exposure to identity theft (for example, through the release of non-public identifiers such as passport details); and
- The exposure of the private aspect of a person's life becoming known by others.

The Compliance Department will determine this using, amongst other things, the self-assessment form on the ICO website. The external DPO, Judicium, will also be immediately notified and the School, in conjunction with the DPO, will reach a decision about whether the breach is reportable to the ICO.

Where required, the School can notify the ICO by completing the 'Personal data breach reporting form' on the 'Data breach reporting' section of the ICO's website, or by informing them over the phone by calling 0303 123 1113.

Reporting a Data Breach to the Data Subject/s Concerned

For data breaches that result in a high risk to the rights and freedoms of individuals, the School is under a legal obligation to inform those concerned directly and without undue delay. A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO.

The School will determine whether it is necessary to report the breach to the data subjects, in conjunction with the DPO, the ICO and where relevant, other authorities such as the police.

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School will consider alternative means to make those affected aware (for example, by making a statement on the School website).

Information that must be provided to individuals when telling them about a breach includes:

- The nature of the personal data breach;
- The name and contact details of the person responsible for data protection 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 personal data breach and including, where appropriate, the measures taken to mitigate any possible adverse effects.

The Compliance Department, in consultation with the Breach Notification Team, will decide whether notification to the individuals affected is necessary. Updates will be provided to affected individuals, where applicable.

Breach Assessment

Once informed of a breach, the Compliance Department and, where necessary the Breach Notification Team, will assess the actions necessary to mitigate any resulting harm. Each breach will be assessed individually, and any actions taken shall be appropriate to the particular circumstances. The Incident Grading Document at Appendix 4 will be used to assess the severity of the breach.

The objectives following a breach are:

1. **Prevent further spread or loss of data;**
    - Identify how the breach occurred;
    - Immediately take steps to limit the consequences and prevent a recurrence.

2. **Identify ways to recover losses (if appropriate);**

3. **Identify risks;**
    - Obtain specialist legal advice, as appropriate;
    - Identify the amount, sensitivity and type of data in question;
    - Confirm what security measures were in place and the measures to be put in place after the data security breach;
    - Confirm who has been put at risk and assess the potential harm to individuals, including what the data could tell a third party about the data subject(s);
    - Consider the additional and wider consequences of the breach including loss of reputation, loss of business, liability for fines or breach of contract.

4. **Notify the appropriate parties of the breach**
    - Consider who to inform about the breach, including any legal or contractual obligations (including, but not limited to, the police, local and regulatory authorities, the School's insurers and data subjects);
    - Assess whether the breach meets notification thresholds, and whether there would be any adverse consequences of informing third parties;
    - If there is likely to be a risk to individuals' rights and freedoms, the School will notify the ICO. Whether or not the ICO are notified, the School will record its decision (see Appendix 2);
    - If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the School will inform the data subjects without undue delay (bearing in mind the exceptions listed in Article 34 of the UK GDPR – see the flow diagram in Appendix 5);
    - When informing other parties, consider what details to tell individuals and how to do so without causing undue harm.

5. **Prevent future breaches**
    - Assess data security risks and whether steps can be taken to mitigate these, including the review of, or introduction of, relevant Data Protection Impact Assessments;
    - Review of key policies to ensure procedures are adequate;
    - Derive "lessons learned" to educate staff in data security measures;
    - Debrief Breach Notification Team members, and the Governors where applicable, following the investigation; and
    - Consider whether further audits or data protection steps need to be taken

A breach reporting procedure flowchart can be found at Appendix 5 and used as guidance for staff.

Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate. Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

Appendix 1 - Data Breach Classification

CLASSIFICATION	DESCRIPTION OF DISCLOSURE TYPES
GREEN	No impact - information formally made public or information which would have no impact on privacy, business, or corporate reputation if it was to be put into the public domain by any other means.
AMBER	Information kept strictly internal or shared with agreed partners/suppliers.
	Information posing little or no risk to individuals' rights and freedoms.
RED (Special category or confidential, likely to result in a high risk to the rights and freedoms of individuals)	Unauthorised disclosure of special category information on individuals relating to: ○ Medical conditions & Learning Support ○ Ethnicity ○ Sexuality or sex life ○ Political opinions ○ Religious or philosophical beliefs ○ Trade Union membership ○ Biometric or genetic data ○ Details of criminal offences or alleged offences
	Unauthorised disclosure of financial data - personal data which reveals anything about the financial circumstances of any individuals or families.
	Unauthorised disclosures that would be likely to have an impact on the health, safety and wellbeing of individuals or cause embarrassment.
	Disclosures meaning data was seen by non-intended recipient/s because of identity theft, fraud, cyber-attacks.
	Information which would have a significant impact on the reputation or business of the School.

Appendix 2 - Suspected Data Breach Form

In the event of an actual or suspected data security breach, please complete the following and email urgently to compliance@theleys.net.

Please provide your name, position and department:

What is/was the date/time of the suspected or actual data security breach? (or an estimate)

Can you provide a description of the data involved?

Can you provide a summary of the incident?

Is the breach on-going? (If known)

What steps have you taken to reduce the effects of the breach? (If known)

How many parties are affected by the breach? Has anyone been notified? (If applicable & known)

Can you provide details about the investigation?

Date:

Appendix 3 - The Leys School Data Protection Breach Log

Date Breach Occurred	Date/time Compliance Officer Notified	Details of the Breach (including the likely consequences)	Incident Grading	Data Subject/s (approximate numbers)	Breach Likely to result in a high risk to individuals' rights and freedoms? (Y/N)	Supervisory Authority (ICO) notified within 72 hours of the breach and individuals affected informed? (Y/N)	If No, what is the reason?	Steps Taken Following Breach

Appendix 4 - Incident Grading Document

This document is a guide to assess the severity of the data breach. It should be remembered that all data breaches should be logged, irrespective of the severity.

Incident grading 1 = Negligible
Any type of incident formally recorded, or something worthy of investigation but turns out to be a "false positive", "near miss" or loss of equipment where there is a remote chance of the data being readable, which has a negligible impact on privacy or the School. * *Reporting of such incidents is still valuable and should be used as part of ongoing information security risk assessment.*

Incident grading 2 = Minor	
Confidentiality	Confirmed or likely loss of personal data or other privacy breach relating to up to 10 individuals that poses low risk to privacy and no health or safety impacts (e.g. just name, address, pupil number).
Integrity	Confirmed or likely issues relating to integrity of information on up to 10 individuals such as confused identities, out of date information or records misplaced which causes localised inconvenience or delays.
Availability	Some localised and short-lived loss of availability, such as through a temporary systems failure, which leads to the disruption of non-critical teams/areas.

Incident grading 3 = Moderate	
Confidentiality	Confirmed or likely loss of personal data or privacy breach relating to more than 10 individuals OR any breach of special category or particularly confidential (e.g. financial) information at red level on the Breach Classification chart which is unlikely to have a major impact on the health or safety of individuals. Likely local media interest and adverse publicity.
Integrity	Issues relating to integrity of information to the extent that the data can no longer be understood or is out of date and could have health, social care and safety or other implications.
Availability	Some disruption to critical services that means information is unavailable causing unacceptable impact and invocation of local team business continuity plans. This may be either a short disruption to a very critical team/area or a longer disruption to a group of less critical teams/areas.

Incident grading 4 = Major

Confidentiality	Confirmed or likely loss of personal data or privacy breach relating to more than 100 individuals OR breach of any special category data at red level which is highly likely to affect the health or safety of one or more individuals OR any privacy breach which, because of the high-profile nature of the person(s) affected or other circumstances, is likely to lead to national media attention and cause significant reputational damage.
Integrity	An integrity issue which means data relating to more than 100 individuals is in effect no longer usable or understandable (and cannot be rectified) and is likely to impact on their health and safety.
Availability	Sustained loss of availability of information which has serious impact on the delivery of a number of critical areas, resulting in business continuity plans being invoked for at least one business area.

Incident grading 5 = Extreme	
Confidentiality	Loss of data or privacy breach relating at large scale (i.e. 100,000+ persons or complete datasets); likely national/international media adverse publicity, prolonged damage (for example parent trust) and could lead to consequences to large numbers of individuals such as identity theft, financial loss etc.
Integrity	Integrity problem which leads to significant amounts of data on 100,000+ persons being unreadable or unusable and does directly lead to health and safety issues or significant services issues (e.g. entire data set for pupil group corrupted beyond use that must be re-created).
Availability	Outage or other issue which leads to general failure of IT so that teams/areas which are critical to the school are not running for a prolonged period. Business Continuity Plans across school/trust are invoked.

Appendix 5 - Suspected Personal Data Breach - Internal Response Plan

'A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" – Art 4(12) GDPR