



Data Breach Policy

Last reviewed: August 2025

Date of Next Review: August 2026

Reviewed by: Governing Body

Version 1.2

1 TABLE OF CONTENTS

1	Table of Contents	2
1	Availability of the Policy (Reg 33(b))	3
2	Introduction	3
3	Definitions	4
3.1.1	Personal Data	4
3.1.2	Special Category Data	4
3.1.3	Personal Data Breach	4
3.1.4	Data Subject	4
3.1.5	ICO	4
4	Responsibility	4
5	Security and Data-Related Policies	5
6	What is a Personal Data Breach?	5
7	Data Breach Procedure	5
7.1	When Does it Need to be Reported?	6
7.2	Reporting a Data Breach.....	6
8	Managing and Recording the Breach.....	7
9	Notifying the ICO.....	7
10	Notifying Data Subjects.....	7
11	Notifying Other Authorities	8
12	Assessing the Breach.....	8
13	Preventing Future Breaches.....	8
14	Reporting Data Protection Concerns	9
15	Training	9
16	Monitoring	9

At Daffodil Preparatory School, we believe that every child should be given the opportunity to develop to the highest standard academically, with good morals, social skills and cultural awareness to become a well-rounded individual. Through our Vision, Ethos and Aims, at Daffodil Preparatory School we provide this opportunity for our children and are pleased to do so within our school environment.

We anticipate all applicants to give their commitment, respect and wholehearted support to uphold and maintain our school ethos and values. In line with our values, we do not tolerate extreme religious or political views in any capacity. This includes any views which are prohibited under the law as well as those views that contravene our ethos and stance on equality, tolerance and respect for all, regardless of race, gender, faith (or none) or sexual orientation or gender preference.

1 AVAILABILITY OF THE POLICY (REG 33(B))

This policy is available to all parents and carers:

- On the school website: www.daffodilprepschool.org.uk
- In printed form upon request from the school office

2 INTRODUCTION

At Daffodil Preparatory School, we recognise our responsibility to protect the rights of individuals whose personal data we obtain, store, process, or share. The **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018** require organisations to take appropriate security measures against unauthorised access, alteration, disclosure, or destruction of personal data.

The UK GDPR places clear obligations on staff to report any actual or suspected data breaches without delay. This policy sets out the school's procedures for identifying, reporting, and managing data breaches to ensure that incidents are handled lawfully, transparently, and effectively. All members of staff are required to familiarise themselves with its contents and comply with its provisions. Training will be provided to ensure that staff understand their responsibilities under this policy.

Data Processors working on behalf of the school will also be provided with a copy of this policy and are required to notify the school of any data breach without undue delay after becoming aware of it. Failure to do so may constitute a breach of the terms of their processing agreement.

Any breach of this policy will be treated as a disciplinary offence and may result in action under the school's Disciplinary Policy and Procedure, up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment and is not intended to have contractual effect. Changes to data protection legislation will be monitored, and the school will update this policy where necessary to ensure continued compliance with statutory obligations, the **Independent School Standards Regulations (ISSRs)**, and the expectations of **Ofsted**.

3 DEFINITIONS

3.1.1 Personal Data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for example a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

3.1.2 Special Category Data

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

3.1.3 Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

3.1.4 Data Subject

Person to whom the personal data relates.

3.1.5 ICO

ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

4 RESPONSIBILITY

The Headteacher has overall responsibility for breach notification within the School. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

In the absence of the Headteacher, please do contact Mr A Zaman (The Director).

The Data Protection Officer (DPO) 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:

Address:

Email:

Web: www.judiciumeducation.co.uk

Telephone:

Lead Contact:

5 SECURITY AND DATA-RELATED POLICIES

Staff should refer to the following policies that are related to this data breach policy: -

- Security Policy which sets out the School's guidelines and processes on keeping personal data secure against loss and misuse.
- Data Protection Policy which sets out the School's obligations under UK GDPR about how they process personal data.
- Cyber Security Policy which sets out the School's obligations and guidelines for Cyber Security issues.

These policies are also designed to protect personal data and can be found on the school website.

6 WHAT IS A PERSONAL DATA BREACH?

7 DATA BREACH PROCEDURE

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other “blagging” attacks where information is obtained by deceiving whoever holds it.

7.1 WHEN DOES IT NEED TO BE REPORTED?

The School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

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);
- the exposure of the private aspect of a person’s life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

7.2 REPORTING A DATA BREACH

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should:

Complete a data breach report form (which can be obtained from the office;

- Email the completed form to Miss S Ali.

Where appropriate, you should liaise with your line manager about completion of the data report form. Breach reporting is encouraged throughout the School and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, Miss S Ali or the DPO.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. Miss S Ali will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the DPO.

8 MANAGING AND RECORDING THE BREACH

On being notified of a suspected personal data breach, Miss S Ali will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to: -

- Where possible, contain the data breach;
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the School's data breach register;
- Notify the ICO where required;
- Notify data subjects affected by the breach if required;
- Notify other appropriate parties to the breach;
- Take steps to prevent future breaches.

9 NOTIFYING THE ICO

Miss S Ali will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (i.e. it is not 72 working hours). If the School is unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

10 NOTIFYING DATA SUBJECTS

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, Miss S Ali will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures the School have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, Miss S Ali will co-operate with and seek guidance from the DPO, the ICO and any other relevant 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).

11 NOTIFYING OTHER AUTHORITIES

The School will need to consider whether other parties need to be notified of the breach. For example:

- Insurers;
- Parents;
- Third parties (for example, when they are also affected by the breach);
- Local authority;
- The police (for example, if the breach involved theft of equipment or data).

This list is non-exhaustive.

12 ASSESSING THE BREACH

Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

The School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover, correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include:

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

13 PREVENTING FUTURE BREACHES

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will:

- Establish what security measures were in place when the breach occurred;

- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it is necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

14 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 you to report any concerns (even if they do not meet the criteria of a data breach) that you may have to Miss S Ali 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.

15 TRAINING

The School will ensure that staff are trained and aware of the need to report data breaches to ensure that they know how to detect a data breach and the procedures of reporting them. This policy will be shared with staff.

16 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.