St Dunstan's EDUCATION GROUP

Data Breach Policy

Related document to P14 – Data protection and GDPR

Policy Owner: Chief Operating Officer (COO)

ISSR Reference: N/A

Reviewed: Michaelmas 2024

Approved: Full governing body Michaelmas 2024

Next Review: Lent 2025

Version Control Information

Reason for Amendment	Role	Date	Main Changes
Annual review	Chief Operating Officer	Michaelmas 2024	Transfer to new template

Contents

1. Introduction and aims

This policy is applicable to staff, pupils, parents / carers and visitors.

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied. St Dunstan's Education Group ('the Group) aim to take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data. This policy sets out the Group's procedures for dealing with breaches.

The UK GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out in this policy. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data processors will be provided with a copy of this policy and will be required to notify the Group of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Group's Disciplinary Policy 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 with the Group and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

2. Legislation and definitions

2.1 Legislation

This policy is based on advice from Judicium Education, and informed by the following legislation:

- UK General Data Protection Regulation (UKGDPR), 2018
- Data Protection Act, 2018.

2.2 Definitions

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.
Special category data	Previously termed 'sensitive personal data', special category data is similar by definition and refers to data concerning an individual data subject'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.
Data subject	An individual about whom such information is stored is known as the data subject. It includes, but is not limited to, job applicants, employees, pupils, parents / carers.
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.
Information Commissioner's Office (ICO)	ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

3. Roles and responsibilities

3.1 St Dunstan's Education Group

The Group's governing board has ultimate responsibility for data protection but will delegate day-to-day responsibility to the Head of St Dunstan's Education Group. The governing body has a duty to:

- Ensure an approved Data Protection Policy is in place and reviewed annually
- Monitor the application of the Data Protection Policy, including monitoring the number and nature of data breaches, as well as seeking reassurance on effective handling and remedial action to avoid a recurrence.

3.2 The Head of St Dunstan's Education Group

The Head of St Dunstan's Education Group (the Head of the Group) is responsible for:

- Day-to-day management of all data protection matters in accordance with the Data Protection Policy, including ensuring there is a suitable and sufficient system for identifying and reporting data breaches and that remedial action is taken to avoid recurrence
- Delegating responsibilities to other competent members of staff.

3.3 Chief Operating Officer

The Chief Operating Officer (COO) is responsible for:

- Acting as the representative of the data controller on a day-to-day basis
- Acting as first point of contact for individuals whose data the Group processes
- Overseeing the implementation of the Data Protection Policy, including ensuring appropriate security measures and a suitable procedure for reporting data breaches are in place
- Designated point of contact for reporting data breaches and coordinating the response to a possible or known data breach
- Ensuring that a training needs analysis is carried out to ensure that all staff fully understand how to avoid, recognise and report a data breach
- Reporting on data protection matters, including the number and nature of data breaches, to the governing body.

3.4 Data Protection Officer

The Data Protection Officer (DPO), Judicium Education, is responsible for:

- Monitoring compliance with data protection law and developing related policies and procedures
- Conducting an annual audit of each individual school's data protection procedures to assess data security and management of data breaches
- Liaising with the ICO (Information Commissioners' Office) regarding possible data breaches.

3.5 Staff

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with the Data Protection Policy
- Completing data protection and cybersecurity training, including understanding how to avoid, recognise and report data breaches

- Seeking advice from the COO in the following circumstances:
    - If they have any concerns that the Data Protection Policy is not being followed
    - If they or suspect or know there has been a data breach.

3.6 Pupils and parents/carers

All pupils and parents/carers are responsible for:

- Seeking advice from the COO in the following circumstances:
    - If they have any concerns that the Data Protection Policy is not being followed
    - If they are unsure whether the Group has a lawful basis to use personal data in a particular way
    - If they suspect or know that there has been a data breach.

4. Data breach procedure

4.1 What is a 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.

Examples of a data breach include, but are not limited to:

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

4.2 When does a data breach need to be reported

The ICO must be notified 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 include:

- 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, e.g. 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.

4.3 Reporting a data breach

If a personal data breach is known or suspected, even if deemed low risk, an online data breach form must be submitted. Breach reporting is encouraged, 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 the Head of Administrative Services & Events at St Dunstan's College, the Head of Operations at Rosemead Preparatory School & Nursery, or the Group's COO and DPO.

Once reported, individuals should not take any further action in relation to the breach. In particular they must not notify any affected individuals or regulators or investigate further. The COO, or their nominated deputy, will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in consultation with the DPO.

4.4. Managing and recording the breach

On being notified of a suspected personal data breach, the COO, or their nominated deputy, 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 relevant school's data breach register
- Notify the ICO
- Notify data subjects affected by the breach
- Notify other appropriate parties to the breach
- Take steps to prevent future breaches.

4.5 Containment and recovery

The COO, with the support of the DPO, will take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data, and identify ways to recover, correct or delete data. This may include contacting the police, e.g. where the breach involves stolen hardware or data.

Depending on the nature of the breach, the COO, with the support of the DPO, will notify the schools insurers, as they can provide access to data breach management experts.

4.5 Notifying the ICO

The DPO 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 holidays, i.e. it is not 72 **working** hours. If the COO or DPO is unsure 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.

The Group and the DPO will consider the factors set out below:

The potential harm to the rights and freedoms of data subjects	This is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. It can include: • Exposure to identify theft through the release of non-public identifiers, e.g. passport number • Information about the private aspects of a person's life becoming known to others, e.g. financial circumstances.
The volume of personal data	There should be a presumption to report to the ICO where: • A large volume of personal data is concerned • There is a real risk to individuals suffering some harm. It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances of the loss or the extent of information about each individual.
The sensitivity of the data	There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress. This is most likely to be the case where the breach involves special category personal data. If the information is particularly sensitive, even a single record could trigger a report. The ICO provides two examples:

	• Theft of a manual paper-based filing system, or unencrypted digital media, holding the personal data and financial records of 50 named individuals would be reportable • Breach of a similar system holding the trade union subscription records of the same number of individuals, where there are no special circumstances surrounding the loss, would not be reportable.

4.6 Notifying data subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the COO or their nominated deputy, 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 relevant school and the Group have, or intend, to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the COO will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities, including 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 Group will consider alternative means to make those affected aware, for example, by making a statement on the website.

4.7 Notifying other authorities

The Group will need to consider whether other parties need to be notified of the breach. This may include, but is not limited to:

- Insurers
- Parents / carers
- Third parties, e.g. when they are also affected by the breach
- Local authority
- The police, e.g. if the breach involved theft of equipment or data.

4.8 Assessing the breach

Having dealt with containing the breach, the Group will also 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. Factors that will inform this decision, will 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 Group and individual schools
- Any other wider consequences which may be applicable.

4.9 Preventing future breaches

Once the data breach has been dealt with, the Group will consider its security processes with the aim of preventing further breaches. Consideration will include:

- Establishing what security measures were in place when the breach occurred
- Assessing whether technical or organisational measures can be implemented to prevent the breach happening again
- Considering whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice
- Considering whether it is necessary to conduct a privacy or data protection impact assessment
- Considering whether further audits or data protection steps need to be taken
- Updating the relevant school's data breach register
- To debrief governors and the executive team following the investigation.

4.10 Reporting data breach 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 don't meet the criteria of a data breach, that you may have to the COO or the DPO. This can help capture risks as they emerge, protect the Group from data breaches and keep our processes up to date and effective.

4.11 Training

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

5. Monitoring

This policy will be reviewed by the COO annually. At every review, the policy will be approved by the Finance and Resource Committee.

6. Links with other policies and documents

This Data Breach Policy links to the following policies:

- Data Protection Policy
- CCTV Policy
- Data Retention Policy
- Information Security Policy
- Privacy notices