Data Breach Policy with Matrix

Approved by: THE FINANCE AUDIT & RISK COMMITTEE	**Date:** 13th May 2024
Last reviewed on: 13th May 2024	
Next review due by: May 2026	

Introduction

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The UK GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. 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 (i.e. any individual who is using or has access to personal data within Greensand Multi Academy Trust) will be provided with a copy of this policy and will be required to notify the Trust 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 Trust'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 with the Trust 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.

Employee Wellbeing

Greensand Multi Academy Trust ("the Trust") is committed to promoting the positive mental, physical and emotional wellbeing of its staff and recognises that enhancing individual wellbeing offers benefits not just to our staff but also to the wider communities within our organisation.

As such, when implementing this policy, consideration will be given to the impact on workload and wellbeing and take appropriate action to monitor, mitigate and support all those involved in its application.

Public Sector Equality Duties

The Trust is committed to equality, both as an employer and a service provider. We welcome our general duty under the Equality Act 2010 to eliminate discrimination, to advance equality of opportunity and to foster good relations. We will ensure diligence in regard of our specific duties. This policy will be consistently and fairly applied to all stakeholders, with due regard for ensuring no-one experiences less favourable treatment in its application.

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'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.

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.

Data Subject

Person to whom the personal data relates.

Information Commissioner's Office - ICO

The ICO is the UK's independent regulator for data protection and information.

Responsibility

The School Business Managers in Greensand schools are responsible for notifying breaches to the Data Protection Officer (DPO). 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 their school.

Upon receipt of data breach information, the DPO will complete a data breach form, attaching all relevant documentation and this is countersigned by the CEO. The DPO uses the ICO Assessment tool to see whether an issue needs to be reported. The DPO may also advise school about further training for staff where appropriate.

The DPO logs the breach and a summary of incidents is presented within the termly DPO report to Trustees.

The 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: Wendy Hill

Address: Reigate School, Pendleton Road, Reigate, Surrey RH2 7NT

Email: w.hill@reigate-school.surrey.sch.uk

Telephone: 01737 948187.

Security and Data-related Policies

Staff should refer to the Trust's Data Protection Policy which sets out the school's obligations under UK GDPR about how they process personal data.

Data Breach Procedure

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 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.

When does it need to be reported?

The Trust 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.

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:-

- Contact the DPO;
- complete a data breach report form;
- email the completed form to: w.hill@reigate-school.surrey.sch.uk with relevant attachments;

The DPO will then sign the form, attach evidence and the CEO countersigns. The breach is logged and incidents reported within termly DPO report to Trustees.

Where appropriate, you should liaise with your Line Manager about completion of the data breach report form. Breach reporting is encouraged throughout the Trust 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 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. The DPO will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the appropriate Data Protection Champion (DPC).

Managing and Recording the Breach

On being notified of a suspected personal data breach, the SBM 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 Trust'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.

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 school holidays (i.e. it is not 72 working hours). If the school are 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.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the SBM 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, the SBM will co-operate with and seek guidance from the DPO.

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).

Notifying Other Authorities

The Trust 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.

Assessing the Breach

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

The Trust 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 Trust 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?;
- any other wider consequences which may be applicable.

Preventing Future Breaches

Once the data breach has been dealt with, the Trust 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;
- update the data breach register;
- debrief governors/management following the investigation.

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 the SBM or DPO. This can help capture risks as they emerge, protect the Trust from data breaches and keep our processes up to date and effective.

Monitoring

We will monitor the effectiveness of this and all 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 Trust.

Data Breach Matrix

This will help assess the impact of a data breach by “risk scoring”. This risk scoring is achieved when you multiply the probability against the impact.

		Impact				
		Trivial	Minor	Moderate	Major	Extreme
Probability	Rare	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very likely	Medium	Medium	High	High	High

When assessing impact, look at what the actual impact and damage to the individual concerned. When assessing probability, assess what is the likelihood of this breach happening again.

All red or amber incidents will need to be reviewed by the DPO to assess whether reporting is required to the ICO, external authorities or the data subjects.

Impact Criteria – Explained

Impact Criteria				
Trivial	Isolated local negative perception	Affects small number of (<10)	Negligible regulatory and/or contractual. Breach not reportable	1
Minor	Sustained local negative perception	May involve 50 data subject – no sensitive data	Minor regulatory and/or contractual breach, reportable	2
Moderate	Sustained local and/or regional perception	May involve 100+ data subject or relates to sensitive data	Regulatory censure and/or contractual breach, reportable	3
Major	Sustained regional and/or national negative perception	May affect 500+ data subjects. Remediation is likely to be time consuming and complex	Regulatory fines and/or significant corporate breach	4
Extreme	Sustained negative national perception	Affects significant numbers of data subjects (>1000+). Remediation is likely to be time consuming and complex, tracked at a senior level and related to sensitive information	Corporate litigation	5

Probability Criteria

	Probability Criteria	
Rare	One off incident will not be repeated	1
Unlikely	May happen again, but remedial actions make this unlikely	2
Moderate	Could happen again but remedial action has reduced this likelihood	3
Likely	Is likely to happen again within 1-7 days unless action is taken	4
Very Likely	Is likely to happen again almost immediately unless action is taken ASAP	5