



Data Breach Policy

Version: 5.0

Date: 23/09/2024

thesovereigntrust.uk

The Sovereign Trust is a Multi Academy Trust registered in England No. 09666511. Registered Office: Manor Academy Sale, Manor Avenue, Sale M33 5JX




Document Control

| | |
|---------------------------------|--------------------|
| Title | Data Breach Policy |
| Supersedes | 4.0 |
| Owner | CEO |
| Circulation/Distribution | All |
| Review Period | Annually |

The Sovereign Trust is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with Trust's policy review schedule.

A current version of this document is available to all interested parties [The Sovereign Trust Website](#)

Signature: 

Date: 23/09/2024

Version History

| | | | | |
|-------------------------|-------------|---|---------------|---------------|
| Next Review Date | | 23/09/2025 | | |
| Version | Date | Amendments | Author | Status |
| 1.0 | 06/05/2018 | Initial Issue | CEO | Approved |
| 2.0 | 19/08/2021 | Updated references to UK GDPR. | CEO | Approved |
| 3.0 | 19/08/2021 | Added cyber security policy reference, training section and acknowledgement of reading the policy wording. | CEO | Approved |
| 4.0 | 03/08/2022 | Formatting Amendments | CEO | Approved |
| 5.0 | 23/09/2024 | Definitions moved into table, included a data breach form, included information about containment and recovery and more information on harm to data subjects. | CEO | Approved |
| | | | | |
| | | | | |
| | | | | |

Data Breach Policy

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 requires staff to report actual or suspected data breaches, and our procedure for dealing with breaches is set out below. All staff are required to familiarise themselves with the policy and comply with its provisions. Training will be provided 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 Trust of any data breach without undue delay after becoming aware of it. Failure to do so may result in a breach of the terms of the processing agreement.

A breach of this policy will be treated as a disciplinary offence, which, depending on the seriousness of the breach, may result in disciplinary action under the Trust's disciplinary policy and procedure up to and including summary dismissal.

This policy does not form part of any individual's terms and conditions of employment with the Trust and is not intended to have a 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.

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, or 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. |
| ICO | The ICO is the Information Commissioner’s Office, the UK’s independent regulator for data protection and information. |
| Data Protection Officer (DPO) | The person we appoint from time to time to lead the development and implementation of our data protection and compliance with the UK GDPR and other applicable. |

Responsibility

The Executive Headteacher/Head of Schools has overall responsibility for breach notification within the Trust. They ensure that 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 Executive Headteacher/Head of Schools, please contact the Chief Information Officer.

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 followed.

The DPO's contact details are set out below: -

| | |
|--------------------------|--|
| Data Protection Officer: | Judicium Consulting Limited |
| Address: | 72 Cannon Street, London, EC4N 6AE |
| Email: | dataservices@judicium.com |
| Web: | www.judiciumeducation.co.uk |
| Telephone: | 0345 548 7000 opt 1 opt 1 |

Security and Data-Related Policies

We must keep personal data secure against loss or misuse. All staff are required to comply with our information security guidelines and policies. In particular, staff should refer to the following policies that are related to this Data Breach Policy: -

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

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

Data Breach Procedure

What is a personal data breach?

A personal data breach is a security breach that leads 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 are where information is obtained by deceiving whoever holds it.
- Alteration of personal data without permission;
- Loss of availability of personal data.

When does it need to be reported?

The Trust must notify the ICO of a data breach that is likely to risk individuals' rights and freedoms. This means that the breach needs to involve more than just losing personal data, and if unaddressed, it 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 (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.

If the breach is likely to result in a high risk to individuals' rights and freedoms of individuals, they 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:

- Complete a data breach report form (Appendix 1);
- Email the completed form to Chief Information Officer

Where appropriate, you should liaise with your line manager about completion of the data report form. However, this may not be appropriate or possible, e.g., if your line manager is aware of the breach and instructed you not to report it or if they are not available. In these circumstances, you should submit the report directly to the Chief Information Officer without consulting your line manager. 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 their line manager, the Chief Information Officer or the DPO.

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

Managing and Recording the Breach

On being notified of a suspected personal data breach, the Chief Information Officer 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 and (so far as reasonably practicable) 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; and
- Take steps to prevent future breaches.

Containment and Recovery

The Chief Information Officer, with the support of our DPO, will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data.

The Chief Information Officer, with the support of our DPO, will 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 Chief Information Officer, with the support of our DPO, will notify The Professional Indemnity Insurer and/or cyber insurer, as the insurer can provide access to data breach management experts.

Notifying the ICO

The Chief Information Officer will notify the ICO when a personal data breach has occurred that is likely to risk individuals' rights and freedoms.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72-hour deadline is applicable regardless of the Trust's holidays (i.e., it is not 72 working hours). If the Trust 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 for why the matter was not referred to the ICO sooner.

If the Trust are unsure whether to report, the presumption should be to report. The Trust will take into account the factors set out below:

The potential harm to the rights and freedoms of data subjects

This is the overriding consideration when 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 identity 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 personal data breach must be reported unless it is unlikely to result in a risk to data subjects' rights and freedoms.

The volume of personal data

There should be a presumption to report to the ICO where:

- A large volume of personal data is concerned, and
- There is a real risk to individuals suffering some harm.

However, it will 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 data

There should be a presumption of reporting to the ICO when 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.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Chief Information Officer will notify the affected individuals without undue delay, including the name and contact details of the DPO and the ICO, the likely consequences of the data breach and the measures the Trust have (or intended) to take to address the breach, including where appropriate, recommendations for mitigating potential adverse effects.

When determining whether it is necessary to notify individuals directly of the breach, the Chief Information Officer 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 Trust will consider alternative means to make those affected aware (for example, by making a statement on the Trust website).

Notifying the Police

The Trust will already have considered whether to contact the police for containment and recovery. Regardless of this, if it subsequently transpires that the breach arose from a criminal act, the Trust will notify the police and/or relevant law enforcement authorities.

Notifying Other Authorities

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

- The Information Commissioners Office (ICO);
- Affected data subjects;
- 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, two-factor authentication);
- What has happened to the data, e.g., if data has been stolen, could it be used for harmful purposes;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the Trust and
- 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 from 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.

Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an afterthought. Data security concerns may arise at any time, and we encourage you to report any concerns (even if they do not meet the criteria of a data breach) that you may have to the Chief Information Officer or the DPO. This can help capture risks as they emerge, protect the Trust from data breaches and keep our processes up-to-date and effective.

Staff Awareness and Training

Key to the success of our systems is staff awareness and understanding. We provide regular training to staff:

- At induction;
- When there is any change to the law, regulation or policy;
- When significant new threats are identified; and
- In the event of an incident affecting our Trust.

The Trust will ensure that staff are trained and aware of the need to report data breaches, as well as know how to detect a data breach and the procedures for reporting it. This policy will be shared with 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 Trust.

Appendix 1 – Data Breach Report Form

If you know or suspect a personal data breach has occurred, please:

- Complete this form; and
- Email or deliver it to the Chief Information Officer and the DPO, ensuring that you mark your email as urgent with the subject 'Data Breach'.

Time is of the essence with data breaches. You must submit this report as soon as you know or suspect there has been a data breach. Do not delay in satisfying yourself whether a data breach has definitely happened, and do not contact any individuals who may be affected by the data breach. [NAME] and DPO will investigate the potential breach and take necessary actions.

| | |
|---|--|
| Name and contact details of the person notifying the actual or suspected breach | <i>[Insert name and contact details]</i> <i>If you wish to submit an anonymous report, leave this section blank</i> |
| Department/manager | <i>[Insert department from which the report emanated and the relevant manager]</i> |
| Date of actual or suspected breach | <i>[Insert date]</i> |
| Date of discovery of actual or suspected breach | <i>[Insert date]</i> |
| Date of this report | <i>[Insert date]</i> |
| Summary of the facts | <i>[Provide as much information as possible – including the amount, sensitivity and type of data involved]</i> |
| Cause of the actual or suspected breach | <i>[Provide a detailed account of what happened]</i> |
| Is the actual or suspected breach ongoing? | Yes <input type="checkbox"/> No <input type="checkbox"/> Not known <input type="checkbox"/> |

| | |
|--|---|
| Who is or could be affected by the actual or suspected breach? | <i>[Include details of categories and approximate number of data subjects concerned]</i> |
| Are you aware of any related or other data breaches? | <p>Yes <input type="checkbox"/></p> <p>No <input type="checkbox"/></p> <p><i>[If yes, provide more details]</i></p> |