Data Breach Notification Policy

1. Contents

2. Version control

Date	Version	Revision	Owner
15/10/18	1.0	New Policy Document	Future Generation Trust Policy Team
27/01/21	2.0	Scheduled policy review	Future Generation Trust Policy Team

3. Policy Statement

Future Generation Trust is committed to the protection of all personal data and special category personal data for which we are the data controller.

The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

4. Legal framework

This policy has been developed using the Browne Jacobson GDPR toolkit for schools and has due regard to legislation and guidance, including, but not limited to the following:

- Data Protection Act (2018) and The UK General Data Protection Regulation (GDPR)
- DfE Data Protection toolkit for schools (2018)

This policy has due regard to the Trust's policies and procedures, including, but not limited to:

- CCTV Policy
- Child Protection & Safeguarding Policy
- Network and IT Security Policy
- Protection of Biometric Information Policy
- Records Management Policy
- Subject Access Request Procedure

5. About this policy

This policy informs all of our workforce on dealing with a suspected or identified data security breach.

In the event of a suspected or identified breach, the Trust/Academy will take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring. Efficient internal management of any breach is required, to ensure swift and appropriate action is taken and confidentiality is maintained as far as possible. This will be led by the Data Protection Lead (DPL) for each academy in consultation with the Trust's Data Protection Officer (DPO).

Future Generation Trust will also comply with its legal and contractual requirements to notify other organisations including the Information Commissioners Office ("the ICO") and where appropriate data subjects whose personal data has been affected by the breach. This includes any communications with the press.

Failing to appropriately deal with and report data breaches can have serious consequences for the Trust/Academy and for data subjects including:

- identity fraud, financial loss, distress or physical harm;
- reputational damage to the Trust/Academy; and
- fines imposed by the ICO.

6. Definition of data protection terms

This policy should be read in conjunction with the Trust's **Data Protection Policy** and a list of definitions can be found annexed to the document.

7. Identifying a Data Breach

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches are listed below:

- Leaving a mobile device on a train;
- Theft of a bag containing paper documents;
- Destruction of the only copy of a document;
- Sending an email or attachment to the wrong recipient;
- Using an unauthorised email address to access personal data;
- Leaving paper documents containing personal data in a place accessible to other people.

8. Internal Communication

Reporting a data breach upon discovery

If any member of our workforce suspects, or becomes aware, that a data breach may have occurred (either by them, another member of our workforce, a data processor, or any other individual) then they must contact the Data Protection Lead (DPL) for their academy immediately. The DPL will then immediately report this to the Trust's Data Protection Officer.

The data breach may need to be reported to the ICO, and notified to data subjects. This will depend on the risk to data subjects. The DPO must always be consulted in making a decision as to whether to report a data breach to the ICO. Initial investigations will inform as to whether the data breach should be reported.

If it is considered to be necessary to report a data breach to the ICO then Future Generation Trust will do so within 72 hours of discovery of the breach.

The Trust/Academy may also be contractually required to notify other organisations of the breach within a period following discovery.

It is therefore critically important that whenever a member of our workforce suspects that a data breach has occurred, this is reported internally to the DPL for their academy immediately.

Members of our workforce who fail to report a suspected data breach could face disciplinary or other action.

Any potential data breach must also be reported to the Chair of the Trust Board and the appropriate Chair of the Local Governing Body, who will need to be involved in the decision as to whether a data breach should be reported and how best to deal with it. They can then help decide who should be involved in the data breach process and ensure the issue is dealt with effectively and efficiently.

Investigating a suspected data breach

In relation to any suspected data breach the following steps will be taken as soon as possible. These do not have to be carried out as individual tasks, and the most appropriate way of dealing with any breach will depend on the nature of the breach and the information available at any time.

Breach minimisation

The first step must always be to identify how the data breach occurred, the extent of the data breach, and how this can be minimised. The focus will be on containing any data breach, and recovering any personal data. Relevant departments must be involved, such as IT, to take technical and practical steps where appropriate to minimise the breach. Appropriate measures may include:

- remote deactivation of mobile devices;
- shutting down IT systems;
- contacting individuals to whom the information has been disclosed and asking them to delete the information; and
- recovering lost data.

Breach investigation

When the Trust/Academy has taken appropriate steps to minimise the extent of the data breach it must commence an investigation as soon as possible to understand how and why the data breach occurred. This is critical to ensuring that a similar data breach does not occur again and to enable steps to be taken to prevent this from occurring.

Technical steps are likely to include investigating, using IT forensics where appropriate, to examine processes, networks and systems to discover:

- what data/systems were accessed;
- how the access occurred;
- how to fix vulnerabilities in the compromised processes or systems;
- how to address failings in controls or processes.

Other steps are likely to include discussing the matter with individuals involved to appreciate exactly what occurred and why, and reviewing policies and procedures.

Breach analysis

In order to determine the seriousness of a data breach and its potential impact on data subjects, and so as to inform Future Generation Trust as to whether the data breach should be reported to the ICO and notified to data subjects, it is necessary to analyse the nature of the data breach.

Such an analysis must include:

- the type and volume of personal data which was involved in the data breach;
- whether any special category personal data was involved;
- the likelihood of the personal data being accessed by unauthorised third parties;
- the security in place in relation to the personal data, including whether it was encrypted;
- the risks of damage or distress to the data subject.

The Trust's **Data Breach Notification Report** must be completed in every case of a suspected breach, and retained securely, whether or not a decision is ultimately made to report the data breach. This will act as evidence as to the considerations of the Trust in deciding whether or not to report the breach.

All members of our workforce are responsible for sharing all information relating to a data breach with the DPL and/or DPO, which will enable the **Data Breach Notification Report** to be completed.

The DPL and/or DPO may require individuals involved in relation to a data breach to each complete relevant parts of the report as part of the investigation into the data breach. If any member of our workforce is unable to provide information when requested then this should be clearly reflected in the report together with an indication as to if and when such information may be available.

In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this report.

9. External Communication

All external communication is to be managed and overseen by the DPO and Chair of the Trust Board. If appropriate, the Chair of the Local Governing Body and Headteacher will also be involved.

Law Enforcement

The DPO and/or Chair of the Trust Board will assess whether the data breach incident requires reporting to any law enforcement agency, including the police. This will be informed by the investigation and analysis of the data breach, as set out above.

The DPO and/or Chair of the Trust Board shall coordinate communications with any law enforcement agency.

Other organisations

If the data breach involves personal data which we process on behalf of other organisations then we may be contractually required to notify them of the data breach. Future Generation Trust will identify as part of its investigation of the data breach whether or not this is the case and any steps that must be taken as a result.

Information Commissioner's Office

If Future Generation Trust is the data controller in relation to the personal data involved in the data breach, which will be the position in most cases, then the Trust has 72 hours to notify the ICO if the data breach is determined to be notifiable.

A data breach is notifiable unless it is unlikely to result in a risk to the rights and freedoms of any individual. The DPO and Chair of the Trust Board will make an assessment of the data breach against the following criteria taking into account the facts and circumstances in each instance:

- the type and volume of personal data which was involved in the data breach;
- whether any special category personal data was involved;
- the likelihood of the personal data being accessed by unauthorised third parties;
- the security in place in relation to the personal data, including whether it was encrypted;
- the risks of damage or distress to the data subject.

If a notification to the ICO is required then see section 10 of this policy below.

Other supervisory authorities

If the data breach occurred in another country or involves data relating to data subjects from different countries then the DPO and Chair of the Trust Board will assess whether notification is required to be made to supervisory authorities in those countries.

Data subjects

When the data breach is likely to result in a high risk to the rights and freedoms of the data subjects then the data subject will be notified without undue delay. This will be informed by the investigation of the breach by the Trust/Academy.

The communication will be coordinated by the DPO and will include at least the following information:

- a description in clear and plain language of the nature of the data breach;
- the name and contact details of the DPO;
- the likely consequences of the data breach;
- the measures taken or proposed to be taken by Trust/Academy to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.

There is no legal requirement to notify any individual if any of the following conditions are met:

- appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the data breach, in particular, measures which render the data unintelligible to unauthorised persons (e.g. encryption);
- measures have been taken following the breach which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;
- it would involve disproportionate effort to contact individuals. In which case a public communication or similar equally effective measure of communication to the data subjects shall be issued.

For any data breach, the ICO may mandate that communication is issued to data subjects, in which case such communication must be issued.

Press

Staff shall not communicate directly with the press and shall treat all potential data breaches as confidential unless otherwise instructed in writing by the DPO.

All press enquiries shall be directed to **Stuart Ayres**, Chief Executive Officer.

10. Reporting a Data Breach to the ICO

Should Future Generation Trust experience a data breach and need advice about what to do next, how to contain it and/or how to prevent the same issue occurring again, then our DPO will call the ICO helpline on **0303 123 1113.**

Should Future Generation Trust need to report a data breach to the ICO then our DPO will follow the current guidance on the ICO website.

www.ico.org.uk/for-organisations/report-a-breach/

11. Evaluation and response

Reporting is not the final step in relation to a data breach. Future Generation Trust will seek to learn from any data breach. Therefore, following any breach an analysis will be conducted as to any steps that are required to prevent a breach occurring again. This might involve a step as simple as emailing all relevant members of our workforce to reinforce good practice, or providing additional training, or may in more serious cases require new technical systems and processes and procedures to be put in place.

12. Monitoring and Review

The Future Generation Trust Board has overall responsibility for this policy and for reviewing its implementation and effectiveness. The Headteacher has operational responsibility for implementation at their academy.

This policy will be reviewed every two years.

Policy adopted on: **25 March 2021**

Review Date: **March 2023**

Signed: Fliss Dale **Designation:** Chair of Trust Board