Data Breach Policy

Author / Responsible Person	**Chief Information Officer**
Ratified by	**CEO**
Date Ratified	**February 2024**
Next Review Date	**February 2026**
Review Cycle	**2 Years**

Background and scope of 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 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 will be provided with a copy of this policy and will be required to notify the Company 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 Company'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 Company 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.

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.

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

Responsibility

The Data Protection Officer has overall responsibility for breach notification within the Company. 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.

We have appointed data protection specialists, Judicium Consulting Ltd to advise and assist our organisation with data protection compliance. If you have any questions about how we handle your personal information which cannot be resolved by Trust staff, then you can contact Judicium on the details below: -

Email: dataservices@judicium.com
Phone: 0345 548 7000 (option 1 then 1)
Web: www.judiciumeducation.co.uk

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 Company 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); 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 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: -

- Log a call with the IT Service Desk
- Email the CIO (andy.meighen@futureacademies.org)

Where appropriate, you should liaise with your line manager about reporting the incident. If in doubt, report it and the data team will advise. 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, Andy Meighen or Judicium.

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 IT Service Desk will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with Judicium.

Managing and Recording the Breach

On being notified of a suspected personal data breach, the CIO will notify Judicium. 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 Company'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.

Notifying the ICO

The DPO (Judicium) 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 Company 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 CIO will notify the affected individuals without undue delay including the name and contact details of the ICO, the likely consequences of the data breach and the measures the Company have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, CIO will co-operate with and seek guidance from Judicium, 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 Company will consider alternative means to make those affected aware (for example, by making a statement on the Company website).

Notifying Other Authorities

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

- Insurers;
- 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 Company will carry out all necessary investigations into the breach.

The Company 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 Company 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 Company; and
- Any other wider consequences which may be applicable.

Preventing Future Breaches

Once the data breach has been dealt with, the Company 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 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 ICO or Judicium. This can help capture risks as they emerge, protect the Company from data breaches and keep our processes up to date and effective.

Training

The Company will ensure that staff are trained and aware on the need to report data breaches to ensure that they know to detect a data breach and the procedures of reporting them. 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 Company.

---END---