CHANCERY EDUCATION TRUST

PERSONAL DATA BREACH POLICY

NOVEMBER 2025

Next Review Date: November 2026

Staff should make themselves aware of all policies and amendments or updates to policies and adhere to the same, which will be made available on relevant websites and internal data and computer systems.

Executive Summary for the CET Personal Data Breach Policy November 2025.

1. Purpose and Principles

- The policy ensures compliance with UK GDPR and sets out how the Trust identifies, reports, manages, and prevents personal data breaches.
- All staff must understand and comply with the policy; breaches may result in disciplinary action.
- Data processors must also report breaches to the Trust without undue delay.

2. Key Definitions

- Personal Data: Any identifiable information about an individual (name, email, DOB, opinions, etc.).
- Special Category Data: Sensitive information (health, ethnicity, political/religious beliefs, biometric data, etc.).
- Personal Data Breach: Any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
- Data Subject: The individual to whom the data relates.
- DPO: Judicium Consulting Ltd.

3. Responsibilities

- Headteacher/Principal has overall breach-notification responsibility.
- If unavailable, matters escalate to the CEO.
- Staff must report concerns via office@cetrust.com, and escalate to the DPO if necessary.

4. Data Security Expectations

- Staff must follow data security, data protection, and cyber security policies.
- Personal data must be kept secure at all times.

5. Identifying a Personal Data Breach

Examples include:

- Loss or theft of devices or paper files
- Incorrectly sent emails or messages
- Human error
- Unauthorised access
- Hacking, phishing, or deception ("blagging")
- Equipment failure or loss of availability

6. When a Breach Must Be Reported

A breach must be reported to the ICO if it is likely to pose a risk to individuals' rights and freedoms, e.g.:

- Discrimination
- Financial loss
- Identity theft
- Loss of confidentiality
- Physical safety risks
- Exposure of private life

If risk is high, affected individuals must also be notified.

7. Reporting Procedure

If you suspect or know a breach has occurred:

1. Complete a Data Breach Report Form (Appendix 1).

2. Send it urgently to the Headteacher/Principal (or CEO for Trust staff).
3. Staff must not:
   - Notify individuals themselves
   - Contact regulators
   - Investigate further

The Headteacher/Principal/CEO will acknowledge receipt and work with the DPO on next steps.

8. Managing and Recording the Breach

The Headteacher/Principal/CEO and DPO will:

- Confirm whether a breach occurred
- Contain and limit further data loss
- Recover, correct, or delete affected data
- Record the breach in the data breach register
- Notify the ICO and/or individuals where required
- Take action to prevent recurrence

9. Assessing the Breach

Assessment considers:

- Sensitivity and volume of data
- Number and type of individuals affected
- Consequences to data subjects
- Existing protections (encryption, passwords)
- Likely future risks

10. Containment and Recovery

May include:

- Stopping further data loss
- Recovering data
- Contacting insurers or the police (e.g., for theft)

11. Notifying the ICO

- Must be done within 72 hours of becoming aware of the breach (not working hours).
- If unsure, the presumption is to report.
- Late reports must include reasons for delay.

12. Notifying Data Subjects

Required when there is high risk to rights and freedoms. Communication must include:

- DPO and ICO contact details
- Likely consequences
- Steps taken to address the breach
- Guidance on mitigating harm

If individual contact is impossible, a public notice may be issued (e.g. website statement).

13. Reporting Other Authorities

Depending on circumstances, other bodies may be notified:

- Insurers
- Local Authority
- Police
- Third parties also affected

14. Preventing Future Breaches

After a breach, the Trust will:

- Review systems, processes, and security measures
- Consider training needs, audits, and DPIAs
- Update breach registers
- Debrief leadership

15. Staff Awareness and Training

Training provided:

- At induction
- When laws or policies change
- When new risks emerge
- After an incident

CHANCERY EDUCATION TRUST

PERSONAL 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 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 Academy Schools 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 Academy School'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 Academy Schools 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 examples 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

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 Headteacher/Principal has overall responsibility for breach notification within the Academy Schools. 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 the absence of the Headteacher/Principal, please do contact the Chief Executive Officer (CEO).

Please contact office@cetrust.com in the first instance if you have 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. Should the matter remain unresolved, or requires further escalation, please contact our Data Protection Officer (DPO). 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: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 opt 1, then opt 1

Data Security and Data-Related Policies

Staff must keep personal data secure against lose 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: -

- Data Security Policy which sets out the Academy School's guidelines and processes on keeping personal data secure against loss and misuse.

- Data Protection Policy which sets out the Academy School's obligations under UK GDPR about how they process personal data.

- Cyber Security Policy which sets out the Academy School's obligations for cyber security issues.

These policies are also designed to protect personal data and can be found on the Academy School's shared drive and websites.

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;
- Alteration of personal data without permission; and
- Loss of availability of personal data.

When Does It Need To Be Reported?

The Academy School 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: -

- Complete a data breach report form (which can be obtained from the Headteacher/Principal for Academy School Staff, Chief Executive Officer (CEO) for Trust Staff. Also available in Appendix 1;
- Email the completed form to the Headteacher/Principal for Academy School Staff, Chief Executive Officer (CEO) for Trust Staff

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 simply not available. In these circumstances, you should submit the report directly to Headteacher/Principal/CEO without consulting your line manager. Breach reporting is encouraged throughout the Academy School 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, Headteacher/Principal, CEO or 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 Headteacher/Principal/CEO 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 Headteacher/Principal/CEO 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 Academy School'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.

Assessing The Breach

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

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

Containment and Recovery

Headteacher/Principal/CEO with the support of our DPO will identify how the breach occurred and take immediate steps to stop of minimise further loss, destruction or unauthorised disclosure of personal data.

Headteacher/Principal/CEO 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, Headteacher/Principal/CEO with the support of our DPO, will notify the trust business insurer, as the insurer can provide access to data breach management experts.

Notifying the ICO

The CEO 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 Academy 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.

If the Academy School are unsure whether to report, the presumption should be to report. The Academy School will take into account of 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 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.

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 if the loss or the extent of information about each individual.

The sensitivity of 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.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the CEO 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 Academy School 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 CEO 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 Academy School will consider alternative means to make those affected aware (for example by making a statement on the Academy School website).

Notifying the Police

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

Notifying Other Authorities

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

- Insurers;
- The Information Commissioners Office (ICO);
- Parents or affected data subjects;
- 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.

Preventing Future Breaches

Once the data breach has been dealt with, the Chief Executive Officer (CEO), DPO and the Headteacher/Principal 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 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 Headteacher/Principal for Academy School Staff, the CEO for Trust Staff or the DPO. This can help capture risks as they emerge, protect the Academy School 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 our policy;
- When significant new threats are identified; and
- In the event of an incident affecting our Academy School.

The Academy School 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

The policy is reviewed annually, although the Trust may vary or amend it periodically to ensure that we fulfil our obligation around the Personal Data Breach Policy. All proposed changes to this policy would be made following the approval from the Committee.

Staff are required to complete a Google Form to acknowledge they have read and understood the contents of this policy.

	Name	Date
Policy written by	Judicium/CET Board	November 2025
Reviewed by Committee	CET Board	December 2025
Approved by Committee	CET Board	March 2026
Adopted by Governing Body	Local Governing Board	June 2026
To be reviewed annually	November 2026	

Useful policies and information

- Data Protection and Subject Access Request Policy
- Freedom of Information Policy
- ICO – www.ico.org.uk

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 Headteacher/Principal/CEO 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 know or suspect there has been a data breach. Do not delay to satisfy yourself whether a data breach has definitely happened and do not contact any individuals who may be affected by the data breach. Headteacher/Principal/CEO along with DPO, will investigate the potential breach and take necessary actions.

Name and contact details of person notifying the actual or suspected breach	[*Insert name and contact details*] If you wish to submit an anonymous report, leave this section blank
Department/Manager	[*Insert department from which the report emanated and the relevant manager*]
Date of actual or suspected breach	[*Insert date*]
Date of discovery of actual or suspected breach	[*Insert date*]
Date of this report	[*Insert date*]
Summary of the facts	[*Provide as much information as possible – including the amount, sensitivity and type of data involved*]
Cause of the actual or suspected breach	[*Provide a detailed account of what happened*]
Is the actual or suspected breach ongoing?	Yes ☐ No ☐ Not known ☐
Who is or could be affected by the actual or suspected breach?	[*Include details of categories and approximate number of data subjects concerned*]
Are you aware of any related or other data breaches?	Yes ☐ No ☐ [If yes, provide more details]