Security Incident and Data Breach Policy

Reviewed and adopted by Resource & Governance Committee: September 12th 2024
Next Review Date: Q3 2025

Security Incident and Data Breach Policy

Construction Youth Trust ('the Trust') is responsible for the protection of individuals about the processing of personal data and is legally required under the Directive 95/46/EC General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018 to comply with these requirements.

Every care must be taken to protect information and to avoid a security incident, especially where the result is a data breach when personal information is lost or disclosed inappropriately to an unauthorised person. In the unlikely event of such a security incident it is vital that appropriate action is taken to minimise any associated risk. The Trust will investigate all security incidents classified as 'serious' using a set plan and follow a Breach Management Plan in the event of a data breach.

Obligations and responsibilities under the General Data Protection Regulation are not optional; they are mandatory. There can be harsh penalties, up to £20 million or 4% of global turnover for the preceding year (whichever is the greater) in relation to breaches of rights and obligations and up to £10 million or 2% of global turnover for the preceding year (whichever is the greater) imposed for non-compliance regarding Control and Mitigation.

All individuals permitted to access personal data in line with their work must agree to comply with this policy and agree to undertake any relevant training that may be appropriate.

This policy applies to all information held by the Trust falling within the scope of the General Data Protection Regulation and Data Protection Act 2018, in all formats including paper, electronic, audio, and visual. It applies to all staff and those working on behalf of the Trust who have access to the Trust's information.

This policy takes effect immediately and all staff should be made aware of security incident requirements. Any queries should be directed to the Data Protection Officer (contact details below).

This policy will be reviewed annually.

1. Purpose

1.1 The purpose of this policy is to ensure a standardised management approach in the event of a serious security incident, including the handling of a data breach. Security incident management is the process of handling security incidents in a structured and controlled way ensuring they are dealt with:

- speedily and efficiently
- consistently
- ensuring damage is kept to a minimum (i.e. loss of equipment (laptop/memory stick) and/or loss of personal data)
- ensuring that the likelihood of recurrence is reduced by the implementation of appropriate measures.

2. Types of security incidents

2.1 This policy addresses the reporting and handling of security incidents and data breaches. A data security breach can happen for many reasons:

- Loss or theft of data or equipment on which data is stored i.e. IT equipment or information (laptops, mobiles, devices containing personal data e.g. memory sticks)

- Unauthorised disclosure containing personal information
- Inappropriate access controls allowing unauthorised use
- Breach of physical building access/security
- Human error e.g. personal information being left in an insecure location, using incorrect email or postal address, uploading personal information to a website
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deception

3. Reporting a security incident

3.1 This section explains how to report a security incident including a data breach.

3.2 The person who discovered the security incident must report the security incident to the Data Protection Officer (dpo@constructionyouth.org.uk) immediately by email and no later than 24 hours using the security incident form (appendix 1). If this is not possible then a senior staff member should be informed. If the incident occurs or is discovered outside normal working hours, this should be done as soon as practicable. In the event that a staff member's laptop and work phone have been stolen/lost, they should contact the office via their personal mobile/home phone as soon as possible.

3.3 The Data Protection Officer will determine and lead on an investigation although others may be invited to assist depending on the severity of the security incident. Staff must not attempt to conduct their own investigations (other than reporting the incident).

3.4 The Head of Central Resources is ultimately responsible for making any decisions on serious security and incident breaches, where required by our Cyber insurance we will notify our insurers of the breach and they may request to lead on the response/recovery of the incident. Any decision to take disciplinary action will be in line with the Trust's disciplinary policy.

3.5 The security incident report will be concluded when all investigations are complete.

4. Responsibility of Data Protection Officer

4.1 Breach Management Plan

The Data Protection Officer will lead all data breach investigations and will follow the Information Commissioner's Office (ICO) suggested Breach Management Plan:

1. Containment and Recovery
2. Assessment of ongoing risk
3. Notification of Breach
4. Evaluation and Response

4.2 Containment and Recovery

Containment and recovery involves limiting the scope and impact of the data breach including, where necessary, damage limitation.

The Data Protection Officer will:

- Lead the investigation

- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a process, finding a lost piece of equipment, or simply changing access codes etc.
- Establish if there is anything that can be done to recover any losses and limit the damage the breach can cause.
- Where appropriate inform the ICO within 24 - 72 hours and;
- Where appropriate inform the police

5. Assessing the risks

5.1 The next stage of the management plan is for the Data Protection Officer to assess the risks which may be associated with the breach considering the potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

In making this assessment the Data Protection Officer will assess:

- What type of data is involved
- How sensitive it is
- If data has been lost or stolen are there any protections in place such as encryption
- What has happened to the data
- What are the consequences if a third party has the data
- How many and who are the individuals' affected
- What harm can come to those individuals
- If there are wider consequences to consider such as a risk to public health or loss of public confidence

6. Notification

6.1 The Data Protection Officer will decide whether the Information Commissioner's Office (ICO) or the data subjects should be notified of the breach and will inform the Head of Central Resources. The ICO must be notified within 24 – 72 hours. This is the sole responsibility of the Data Protection Officer and staff **must not** make any notifications directly.

6.2 The ICO will need to be notified of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals, for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. This will be assessed on a case-by-case basis by the Data Protection Officer.

7. Evaluation and Response

7.1 The Data Protection Officer will:

- fully review both the causes of the breach and the effectiveness of the response to it
- keep a breach log
- report to the Head of Central Resources
- implement an action plan to correct identified issues if required
- monitor staff awareness of security issues and look to fill any gaps through

training

8. Links with other policies

This Security Incident and Data Breach policy is linked to the Trust's:

- Data Protection Policy
- Information Sharing Policy
- Data Protection Impact Assessment Policy
- Information Security Policy
- Safeguarding policy
- Privacy Notices

Appendix 1

Security Incident and Data Breach Notification Form

Contact details of person submitting form

Name	
Job Title	
Contact number	
Email	

Incident information

Date of incident	
How did the incident happen?	
Who reported the incident?	
Description of breach:	

Type of breach (please tick)

Loss of IT equipment		Human error	
Theft of IT equipment		Hacking	
Unlawful disclosure		Blagging/phishing	
Unlawful access		Fire/Flood	
Other (please describe)			

Personal data placed at risk

Number of individuals affected	

Have the affected individuals been made aware?	Yes		No	
What are the potential consequences and adverse effects on those individuals?				

Have any affected individuals complained about the incident?	Yes		No	

Provide details of any action taken to minimise/mitigate the effect on the data subjects.

Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

Please provide brief details of any supporting information.

Once complete please email form to:
Data Protection Officer at dpo@constructionyouth.org.uk