Data Breach Notification Policy

Reviewed: June 2026

Reviewed:	02/06/2026
Expiry Date:	05/05/2027
Next Review:	June 2027
Appraised:	N/A
Next Appraisal:	August 2026

Footprints Centre, 553 Farnborough Road, Clifton, Nottingham, NG11 9DG
Tel: 0115 958 6641 Web: www.footprintscec.org

Contents

Remote working Policy

1.0 Statement of Intent

Footprints Conductive Education Centre (Footprints CEC) is committed to ensuring data security. This policy provides guidance on dealing with a suspected or identified data security breach. In the event of a suspected or identified breach, Footprints Conductive Education Centre must take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring. We must manage communications internally, to ensure swift and appropriate action is taken and confidentiality is maintained. We must also manage our external communications as we may be required by law or contract to notify the data controller, the Information Commissioners Office ('ICO') or the individuals ('data subjects') whose data has been affected by the breach. We must also ensure that any press communication is handled centrally.

Failing to deal with and report data breaches appropriately can have serious consequences for Footprints Conductive Education Centre and data subjects including:

- Risk to the data subjects including identity fraud, financial loss, distress, or physical harm.
- Reputational damage to Footprints Conductive Education Centre
- Fines imposed by the ICO of up to the higher of £20million or 4% of annual global turnover.

2.0 Definitions

Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
Data protection laws	The UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (where applicable), and any legislation, statutory instruments, regulatory requirements, or guidance in force from time to time relating to the processing of personal data and privacy, each as amended, replaced, or superseded;
Data subject	The identifiable individual to whom the personal data relates;
GDPR	The UK General Data Protection Regulation as it forms part of the law of England and Wales, Scotland, and Northern Ireland, as amended from time to time;
Personal data	Any information relating to a living individual who can be identified directly or indirectly by reference to an identifier such as a name, ID number, location data, an online identifier or by one or more factors specific to the physical, psychological, genetic, mental, economic, cultural, or social identity of the individual;
Special category data	Personal Data revealing the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation or genetic or biometric data.

3.0 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.

4.0 Internal Communication

Reporting a data breach

If you suspect a data breach may have occurred, then you must contact the Data Protection Officer ('DPO') immediately at:

Stephen Frew

Footprints Centre, 553 Farnborough Road, Clifton, Nottingham, NG11 9DG. Tel: 01159586641.
Stephen.Frew@footprintscec.org

If an ICO notification is required by law about the data breach, then notification must be made within 72 hours of discovery of the breach where we are a controller. We may also be contractually required to notify a data controller of the breach immediately upon discovery. It is therefore important that all potential data breaches are reported internally to the DPO immediately.

Employees who fail to report a potential data breach could face disciplinary action.

A written internal record of every personal data breach must be maintained, whether or not the breach is reportable to the ICO. The record should capture the facts relating to the breach, its effects, the risk assessment, the decision on whether notification was required, and the remedial action taken.

Investigating a data breach

The DPO alongside the Trustees will assess each report of a potential data breach and take the following steps:

- **Breach minimisation**: Liaise with IT to take steps where appropriate to minimise the breach. Appropriate measures may include:
    - Remote deactivation of mobile devices.
    - Shutting down IT systems.
    - Recovering lost data.

- **Breach investigation**: 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.

- **Breach analysis**: Analyse the data breach to determine:
    - How many data subjects were affected.
    - What data was accessed, and whether it was special category data.
    - Whether any data relates to third-party data controllers.
    - What notifications are required (see 'External Communication' below).

5.0 External communication

All external communication is to be managed and overseen by the DPO and the Trustees.

6.0 Law Enforcement

The management and Trustees will assess whether the data breach incident requires reporting to the Police, e.g. if it involved theft. Management shall coordinate communications with the Police and the collection of internal reports and evidence where appropriate.

Other data controllers

If the data breach involves personal data which we process on behalf of a third-party data controller, we must notify that controller without undue delay and in accordance with any contractual reporting requirements. The controller is responsible for assessing whether notification to the ICO or affected individuals is required, although we must provide all information and assistance reasonably required to support that assessment and any resulting notifications.

Information Commissioners Office

If Footprints Conductive Education Centre is the data controller in relation to the personal data involved in the data breach, we must assess without undue delay whether the breach is likely to result in a risk to the rights and freedoms of individuals. If so, the breach must be notified to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. If notification is made later than 72 hours, reasons for the delay must be recorded and provided to the ICO. If the breach is unlikely to result in a risk to the rights and freedoms of individuals, notification to the ICO is not required, but the breach must still be documented internally.

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

If notification to the ICO is required then see 'Producing an ICO breach report' below.

Where the initial notification to the ICO cannot include all required information, an initial report should still be made within the applicable timeframe with the available facts, and further information should be provided to the ICO without undue delay as it becomes known.

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 must be notified without undue delay. 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 Footprints Conductive Education Centre to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.

Such communication shall not be required 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 ensures 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, 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 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 management.

If communication to the press is required, the following process shall be followed:

- The need for press communication is identified and wording drafted by the DPO or the Communications Manager - Claire Clarkson.
- Appropriate channels of communication are identified (including accompanying social media statements where appropriate).
- The draft press release is supplied to a relevant senior manager or board member.
- The board member approves the press communication and channels of communication.
- All public facing staff are briefed on how to handle queries resulting from the press release.
- The communication is issued by the DPO OR Claire Clarkson.

7.0 Producing an ICO Breach Notification Report

Please provide as much information as possible and ensure that all mandatory (*) fields are completed. If you don’t know the answer, or you are waiting on completion of an internal investigation, please include that in the

report. In addition to completing the form below, consider including other relevant supporting information, e.g. incident reports.

In the wake of a data protection breach, swift containment and recovery of the situation are 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 form.

7.1 Organisation details

(a) Footprints Conductive Education Centre - is it the data controller in respect of this breach?

(b) For further information, please contact Stephen Frew or Claire Clarkson, Stephen.Frew@footprintscec.org or claire.clarkson@footprintscec.org Footprints Centre, 553 Farnborough Road, Clifton, Nottingham, NG11 9DG. Tel: 0115 958 6641

7.2 Details of the data protection breach

(a) * Please describe the incident in as much detail as possible.

(b) * When did the incident happen?

(c) * How did the incident happen?

(d) If there has been a delay in reporting the incident to the ICO, please explain your reasons for this.

(e) What measures did the organisation have in place to prevent an incident of this nature occurring?

(f) Please provide extracts of any policies and procedures considered relevant to this incident and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

7.3 Personal data placed at risk

(a) * What personal data has been placed at risk? Please specify if any financial or special category (sensitive) personal data has been affected and provide details of the extent.

(b) * How many individuals have been affected?

(c) * Are the affected individuals aware that the incident has occurred?

(d) * What are the potential consequences and adverse effects on those individuals?

(e) Have any affected individuals complained to the organisation about the incident?

7.4 Containment and recovery

(a) * Has the organisation taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.

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

(c) What steps has your organisation taken to prevent a recurrence of this incident?

7.5 Training and guidance

(a) As the data controller, does the organisation provide its staff with training on the requirements of the Data Protection Act? If so, please provide any extracts relevant to this incident here.

(b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so, when?

(c) As the data controller, does the organisation provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

7.5 Previous contact with the ICO

(a) * Have you reported any previous incidents to the ICO in the last two years?

(b) If the answer to the above question is yes, please provide brief details, the date on which the matter was reported and, where known, the ICO reference number.

7.6 Miscellaneous

(a) Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.

(b) Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.

(c) Have you informed any other regulatory bodies about this incident? If so, please provide details.

(d) Has there been any media coverage of the incident? If so, please provide details of this.

8.0 Sending this Form

Submit reportable personal data breaches to the ICO using the current reporting method published by the ICO. Before submitting, ensure the organisation has gathered the available facts about what happened, when and how the breach was discovered, the categories and approximate number of affected individuals and

records, the likely consequences, and the mitigation steps already taken or proposed. If all details are not yet available, make the report within the required timeframe and provide further information to the ICO without undue delay.

What happens next?

When the ICO receive this form, they will contact you within seven calendar days to provide:

- a case reference number; and
- information about the next steps the ICO will take (if any).

If you need any help in completing this form, you can contact the ICO helpline on **0303 123 1113** or **01625 545745** (operates 9 am to 5 pm Monday to Friday).