Cygnet Evaluation

Cygnet Evaluation – Data Incident Reporting Procedure

Purpose and scope

Anyone working for Cygnet Evaluation who suspects a data incident must report it to the Data Protection Lead straight away, and no later than the same working day. This procedure sets out what happens next, so that incidents are contained quickly and client organisations, the Information Commissioner's Office (ICO) and affected people are told when the law or a contract requires it.

It applies to:

- everyone who works for or with Cygnet Evaluation, including associates, freelancers and subcontractors;
- all personal data Cygnet Evaluation handles, in any format: electronic files, cloud storage, email, recordings, transcripts, notes and paper;
- data Cygnet Evaluation holds **as a processor** on behalf of client organisations, such as evaluation data shared by Citizens Advice Powys, and data it holds **as a controller** for its own business, such as enquiries, client contacts, meeting and workshop notes, website analytics data and financial records.

As Cygnet Evaluation's privacy policy states, it acts as a processor for client data unless agreed otherwise, and processes that data only on the client's instructions. The procedure also covers incidents at the third-party providers Cygnet Evaluation uses: website hosting, email, website analytics, online meeting platforms and cloud storage.

It sits alongside Cygnet Evaluation's privacy notice (cygnetevaluation.org/privacy) and the data sharing agreements and contracts agreed with each client.

What counts as a data incident

A data incident is any event that puts the confidentiality, integrity or availability of personal data at risk. It counts whether it was accidental or deliberate, and whether or not harm actually follows. Report near misses too: if in doubt, report it.

Type	Examples in evaluation work
Confidentiality (data seen by someone who shouldn't see it)	Email with participant details sent to the wrong person; file link shared with the wrong people or left public; a report or quote that identifies or potentially identifies a participant; laptop or phone lost or stolen; an account hacked or phished
Integrity (data changed or corrupted)	Interview notes or a data file altered or overwritten in error; data from two clients mixed up
Availability (data lost or inaccessible)	Recordings or transcripts deleted before analysis; ransomware or a device failure with no backup; paper notes lost
Supplier incident	A website host, email, analytics, online meeting or cloud storage provider reports a breach affecting Cygnet Evaluation's data, or an online meeting is recorded or accessed without permission
Breach of agreement	Data kept beyond the agreed date; data used for a purpose not in the data sharing agreement; data passed to someone not named in it

A **personal data breach** under UK GDPR is an incident that has actually led to personal data being lost, destroyed, changed, disclosed or accessed without authorisation. All breaches are incidents, but not all incidents are breaches. The assessment in step 3 decides which it is.

Roles and contacts

Role	Who	Contact
Data Protection Lead (receives reports, leads the response)	Jenny Phillips	hello@cygnetevaluation.org 07584 839066
Information Commissioner's Office	Breach reporting, only where Cygnet Evaluation is the controller	ico.org.uk/for-organisations/report-a-breach 0303 123 1113

Everyone who works on a project must know who the Data Protection Lead is and how to reach them. The Lead checks the client contacts for each project when its data sharing agreement is signed.

The process, step by step

The clock starts when anyone at Cygnet Evaluation becomes aware of the incident, not when the investigation ends.

1. **Report: immediately, and the same working day at the latest.** Tell the Data Protection Lead by phone, then confirm by email. Say what happened, when, what data and whose, how many people, and what has been done so far. Don't investigate on your own, delete evidence, or contact affected people yet.

2. **Contain: straight away.** Limit the damage. For example:
    - ask a wrong recipient to delete the email and confirm in writing;
    - remove or change the sharing on a file link;
    - change passwords and sign out other sessions;
    - remotely lock or wipe a lost device;
    - restore data from a backup.

3. **Assess: within 24 hours.** The Lead records:
    - what data is involved, including any special category data such as health, disability or ethnicity, and financial details;
    - how many people are affected and whether any are vulnerable;
    - whether the data was encrypted;
    - how likely and how serious harm to people is: distress, discrimination, financial loss, damage to reputation or relationships, or physical safety.

4. **Notify: within 24 hours for client data.** Where the data belongs to a client, tell the client controller (next section). The client decides on notifying the ICO and individuals. Where Cygnet Evaluation is the controller, the Lead decides within the 72-hour ICO deadline.

5. **Record: every incident, including near misses and those not reported to anyone.** Add it to the incident log with the reasons for each decision.

6. **Review: within 2 weeks of closing.** Identify the cause and the changes needed, such as training, settings or ways of working. Share what was learned with the client where its data was involved.

Notifying clients, the ICO and individuals

Who Cygnet Evaluation tells depends on whose data it is.

Whose data	Cygnet Evaluation's role	Who to tell	Deadline
Client evaluation data, where an external client is named as the Data Controller	Processor	The client's named contacts, by phone then email. The client decides on ICO and individual notifications. Cygnet Evaluation does not report to the ICO or contact individuals unless the client asks it to.	Without undue delay, within 24 hours of becoming aware
Cygnet Evaluation's own data (enquiries, contacts, associates)	Controller	The ICO, if the breach is likely to result in a risk to people's rights and freedoms	Within 72 hours of becoming aware
Cygnet Evaluation's own data, high risk	Controller	The affected individuals as well, in plain language	Without undue delay

The notice to a client includes:

- what happened, and when it happened and was discovered;
- the categories of data and an approximate number of people and records affected;
- the likely consequences;
- what has been done to contain it, and what is planned next;
- the name and contact details of the Data Protection Lead.

If some details aren't yet known, send what is known within the deadline and follow up as more is found. Keep helping the client with its own investigation and notifications.

Use the ICO's self-assessment tool to decide whether a breach of Cygnet Evaluation's own data needs reporting. Record the decision either way.

Incident log and review

The Data Protection Lead keeps a log of every incident, newest first, and keeps each entry for at least 3 years. Clients can see the entries about their data on request.

Date found	What happened	Data and people affected	Client affected	Risk (low / medium / high)	Action taken	Client notified (date)	ICO notified (date or reason not)	Closed

This procedure is reviewed every year, after any serious incident, and when a new data sharing agreement asks for something different.

DATE OF REVIEW 19/06/26