Personal Data Breach Procedure

Steffi Hesketh Tutoring – online one-to-one and group tutoring

Document control	**Details**
Document	Personal Data Breach Procedure
Organisation	Steffi Hesketh Tutoring (sole trader), online-only tutoring, based in Southampton, Hampshire
Business address	32 Inver Way, Southampton, SO19 1SF
Policy owner	Steffi Hesketh-Spells, Owner and Designated Safeguarding Lead (DSL)
Deputy DSL	Shim Amin, contactable via the business email (steffihesketthtutoring@gmail.com). If neither the DSL nor the Deputy DSL can be reached, follow the alternative route in the Safeguarding and Child Protection Policy (contact children's social care, the police or the LADO directly).
Contact	steffihesketthtutoring@gmail.com, 07802 828910
Version	1.0
Effective date	November 2026
Review date	November 2027, or sooner after a serious incident, a change in law or guidance, or a change to the Hampshire contract
Applies to	Steffi Hesketh-Spells, all self-employed tutors, cover tutors and anyone else working for or on behalf of the business
Contract	Hampshire County Council SEND Alternative Provision Register Agreement CS25116 and Tutoring Call-Off Contract CS25116A

Document control	Details
Approved by	Steffi Hesketh-Spells. Signature: Steffi Hesketh-Spells, Owner and Designated Safeguarding Lead. Date approved: 9 November 2026

Data protection details	
Data controller	Steffi Hesketh Tutoring (Steffi Hesketh-Spells, sole trader)
ICO registration number	ZC116584
Person responsible for data protection	Steffi Hesketh-Spells
Breach reporting contact	steffiheskethtutoring@gmail.com and 07802 828910 (telephone or WhatsApp for anything urgent)

1. Purpose

This procedure explains what we do if personal data is lost, stolen, sent to the wrong person, accessed without permission, or otherwise compromised. It helps us:

- protect the people affected, especially children;
- meet our duties under the UK GDPR and the Data Protection Act 2018;
- meet clause 28.15 of the Hampshire Call-Off Contract, which requires us to tell the Council without undue delay about any Data Loss Event involving personal data processed under the contract.

It completes the brief statement in section 11 of our Privacy Notice and works alongside section 11 and Schedule 4 of the Tutor Data Protection, Privacy, Confidentiality and Online Working Agreement.

2. What is a personal data breach?

A personal data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. It can be digital or on paper, and it does not need to involve hacking.

Examples in online tutoring:

- emailing or messaging a report, EHCP or pupil plan to the wrong parent or professional;
- sharing the wrong screen, file or browser tab in a lesson;
- a pupil seeing another pupil's details or work in a group;
- a lost or stolen laptop, phone or notebook;
- a compromised Google, email, WhatsApp or platform account;
- a meeting link posted publicly, or an unknown person entering a lesson;
- an unauthorised lesson recording;
- uploading pupil information to a public AI tool;
- information kept after it should have been deleted;
- a Drive folder shared with "anyone with the link" by mistake.

Safeguarding records, health and SEND information, and EHCPs are especially sensitive. A breach involving them is treated as higher risk.

3. Roles

- **Everyone (Steffi and all tutors):** report any suspected breach straight away. Do not wait until you are sure, and do not try to investigate on your own.
- **Tutors:** contain the breach where it is safe to do so, and report to Steffi immediately. In every case, report within four hours of becoming aware (Tutor Data Protection Agreement, section 11). Use Schedule 4 of that agreement.
- **Steffi Hesketh-Spells:** leads the response. She assesses risk, decides on notifications, keeps the breach log, and acts as DSL where there is any safeguarding risk.
- **Deputy:** Shim Amin (Deputy DSL), contactable via the business email (steffiheskethtutoring@gmail.com). If Steffi cannot be reached promptly during a suspected breach, the tutor should contain it and keep trying Steffi by phone. If the Council's data is involved, also tell the Council directly using the contact below.

4. Step-by-step procedure

Step 1 – Contain (straight away)

- Recall or unsend the message if possible. Ask the wrong recipient to delete it and confirm in writing that they have not kept or shared it.
- Revoke links and sharing permissions. Remove unknown participants from lessons. Change passwords and sign out of all sessions.
- Report lost or stolen devices. Use remote lock or wipe where available.
- Disconnect a compromised device from the internet.
- Preserve evidence (times, recipients, screenshots of settings or logs) without making extra copies of the personal data.

Step 2 – Report internally (immediately, and within four hours at most)

Tell Steffi by telephone or WhatsApp, then send the Schedule 4 report form by email. Record the date and time you became aware of the breach. This matters because the 72-hour ICO deadline runs from when the business becomes aware.

Step 3 – Assess the risk (Steffi, as soon as possible and within 24 hours)

Steffi records the following in the breach log (Appendix A):

- what happened, when, and how it was found;
- what data was involved and how many people;
- whether special category data or safeguarding data is involved, or children are affected;
- who has or may have the data, and whether it has been recovered;
- the likely consequences, for example distress, discrimination, identity fraud, safeguarding risk, or loss of confidentiality;
- whether there is a **risk** to people's rights and freedoms (if so, report to the ICO) and whether that risk is **high** (if so, also tell the people affected).

Steffi will use the ICO's online self-assessment tool if she is unsure.

Step 4 – Safeguarding check (immediately)

If the breach could put a child at risk (for example a pupil's address revealed to someone they need protection from, or safeguarding records disclosed), Steffi acts as DSL under the Safeguarding and Child Protection Policy straight away. This includes contacting Hampshire Children's Services or the police where needed. Safeguarding action always comes before the paperwork.

Step 5 – Notify

Who	**When**	**How**
Hampshire County Council – any breach or Data Loss Event involving personal data processed under the contract (for example Council-referred pupils' details, EHCPs or referral papers), whether or not the ICO needs to be told	Without undue delay (Call-Off clause 28.15). Our standard is within 24 hours of becoming aware.	The Council's contract manager, via the agreed secure route with the Council. Give the facts known so far and update the Council as more is learned. Work with the Council on the investigation and any notifications.

Who	When	How
Information Commissioner's Office (ICO) – where the breach is likely to result in a risk to people's rights and freedoms	Without undue delay and, where feasible, **within 72 hours** of becoming aware (UK GDPR Article 33). If not all details are known, report what is known within 72 hours and send the rest later. If reporting after 72 hours, give the reasons for the delay.	ICO online breach reporting form at ico.org.uk, or the ICO helpline on 0303 123 1113
The people affected (pupils, usually through their parents or carers, and others) – where the breach is likely to result in a **high** risk	Without undue delay (UK GDPR Article 34)	In clear, plain language and in an accessible format (see the Accessible Communication Policy). Explain what happened, the likely effects, what we have done, what they can do to protect themselves, and who to contact. For a Council-referred pupil, agree the approach with the Council first unless delay would increase the risk.
Police or Action Fraud – suspected crime, for example theft or hacking	As soon as possible	999 in an emergency, 101, or Action Fraud
Insurer – if cover applies	As the policy requires	Hiscox, policy PL-PSC10004022110/00, valid 17/08/2026 to 16/08/2027. Hiscox claims line 0800 280 0351. No cyber cover is listed on this policy.

Do not contact the ICO, families, the press or the insurer on behalf of the business unless Steffi has authorised it or the law requires it (Tutor Data Protection Agreement, section 11).

Step 6 – Recover and review (within 10 working days)

- Make sure the data is recovered or deleted and that access is secured.
- Find the cause and take action to stop it happening again. Examples: training, two-step verification, changing sharing defaults, checking recipients before sending, or using pupil references instead of names.
- Update the breach log with the actions, decisions and reasons. This includes the reason for any decision *not* to notify the ICO or the people affected.
- Tell the Council what was learned where its data was involved.

5. Recording all breaches

Every breach and suspected breach is recorded in the breach log, even if it is not reportable (UK GDPR Article 33(5)). The log is kept securely, separately from pupil records, and is available to the ICO and the Council on request.

6. Preventing breaches

We reduce risk by:

- using approved, UK-adequate platforms only (Call-Off clause 28.16);
- using strong unique passwords and two-step verification on all business accounts;
- encrypting and screen-locking devices;
- using pupil references instead of names in trackers and invoices;
- sharing on a "need to know" basis only;
- checking recipients before sending;
- never putting pupil information into public AI tools;
- keeping safeguarding records restricted;
- removing tutor access promptly when work ends;
- giving data protection training at induction and every year.

7. Review

Steffi reviews this procedure every year and after any significant breach. She will also review it if ICO guidance or data protection law changes, including changes made by the Data (Use and Access) Act 2025.

8. Related policies

- Privacy Notice
- Tutor Data Protection, Privacy, Confidentiality and Online Working Agreement (including the Schedule 4 breach report form)

- Safeguarding and Child Protection Policy (records and information sharing; KCSIE principles)
- Online Tuition, Acceptable Use and Recording Policy
- Business Continuity and Disaster Recovery Plan
- Accessible Communication Policy

Appendix A – Personal data breach log

Ref	Date and time aware	Reported by	What happened	Data and people affected	Council data involved?	Contained (how, when)	Risk level and reasons	Safeguarding action	Council told (date and time)	ICO told (date and time and ref) or reason not	People told (date) or reason not	Actions to prevent recurrence	Closed (date)