Privacy & Data Request Kit — Free Sample

Free sample — 2 complete SOPs from the full kit. Try it before you buy.

These procedures are general guidance for a small business, not legal advice. Privacy rules differ by place, so check your own local privacy law before you rely on them, and get proper legal advice if a request is complicated or disputed.

What's inside

- SOP 01 — Taking in a data request
- SOP 02 — Checking who is asking (identity check)

SOP 01 — Taking in a data request

Purpose: To make sure every data request is spotted, written down and answered on time, no matter how it arrives — by email, through the website contact form, by phone, in person, or on social media.

Scope: This covers every request from a client, former client, email subscriber or website visitor asking about their personal data: what we hold, a copy of it, a correction, or deletion. It applies to Fern & Field Coaching, a 2-person coaching business with a client list, an email list and an online booking system.

Who does it: Whoever first sees the request takes it in. One person is named as the privacy contact and owns the request from start to finish.

Steps

1. Spot the request. Check the inbox, the website contact form, voicemail and social media messages every working day. A request counts even if the person does not use formal words — "what do you have on me?" is a data request.
2. Do not answer the substance straight away. Reply within 2 working days to confirm you received it and say who is handling it.
3. Write it in the request log the same day. Record the date received, the person's name, how they contacted you, and what they asked for in their own words.
4. Start the clock. Mark the deadline on the calendar: most requests must be answered within 30 days of receipt, or sooner if your local law says so. Count from the day the request arrived, not the day you noticed it.
5. Ask the person to confirm what they want if the request is unclear. For example: "Do you want a copy of everything we hold, or only your booking history?"
6. Pass the request to the privacy contact with the log entry number. If the privacy contact is away, the other team member takes over.
7. Tell the person if you need proof of identity from them (see SOP 02).

8. File the original message. Save the email or a screenshot of the message in the request folder, named with the log entry number and the date.

Quality check: Before the end of the day, the privacy contact checks the log entry is complete, the deadline is on the calendar, and the person has had an acknowledgement.

If it goes wrong: If a request is found late — for example, buried in a spam folder — log it at once with the true date it arrived, tell the person, apologise, and prioritise it. Do not backdate the log or pretend it arrived later than it did.

Records: Keep the original message, the log entry, the acknowledgement sent, and any clarification exchanged, in the request folder for at least 2 years after the request is closed.

SOP 02 — Checking who is asking (identity check)

Purpose: To make sure personal data is only given to the person it belongs to, or to someone properly acting for them, and never handed to a stranger by mistake.

Scope: This covers every access, deletion or correction request at Fern & Field Coaching where data will be shared, changed or deleted. It applies to clients, former clients and email subscribers.

Who does it: The privacy contact runs the identity check, and the other team member never releases data until the privacy contact confirms the check is passed.

Steps

1. Decide how strong the check needs to be. A request for a copy of all data needs a stronger check than fixing a spelling mistake. When in doubt, use the stronger check.
2. Ask for two matching pieces of information that only the real person would know. Good options are the email address on the account, the phone number on the booking, the date of their last session, or the name of their coach.
3. An email from the same address on file counts as one piece; ask for one more from the list above.
4. If the request came from a different email address, by phone, or in person, ask for two pieces and check them against the client list and booking system first.
5. If someone says they are acting for the person — a parent, a partner, a lawyer — ask for written permission from the person, or proof of legal authority, before sharing anything. A verbal "they said it's fine" is not enough.
6. Record in the log which pieces matched, and the date. Do not store copies of identity documents; if your local law requires a copy, keep it in the request folder only and delete it as soon as the request is closed.
7. If the check fails or the person cannot provide the information, tell them what else they can provide, and do not release, change or delete any data until the check passes.
8. If you suspect a fake request or a trick to get someone else's data, stop, tell the other team member, and log it as a suspected impersonation attempt. Do not tell the requester what information you hold.

Quality check: The privacy contact re-checks the log before any data leaves the business: the identity check is marked passed and the person receiving the data is the person it belongs to.

If it goes wrong: If data is sent to the wrong person, treat it as a data breach at once and follow SOP 08. Tell the privacy contact immediately, do not try to fix it quietly, and write down exactly what was sent, to whom, and when.

Records: Keep a note of the identity check in the request log, including what was checked and the outcome. Delete any copies of identity documents as soon as the request is closed.