Data Protection Policy

Amplify Yourself Ltd takes the privacy of personal data very seriously. We know what personal data we hold and we take steps to make sure it is handled legally, securely, efficiently and effectively.

1. Purpose

UK GDPR requires us to consider data protection and privacy up front for any personal data we process. We follow a 'privacy by design' approach, and the Data Protection Impact Assessment (DPIA) is a key tool for doing this.

2. Scope

This policy applies to everyone working for or on behalf of Amplify Yourself Ltd — directors, employees, associates, freelancers and contractors — and covers our apps, consultancy, training, research and evaluation work.

3. Our Principles

1. We collect only the personal data we need, for a clear and lawful purpose.
2. We keep data accurate, secure and only for as long as necessary.
3. We are open about what we collect and why.
4. Personal data in our apps belongs to the person who created it. Names are swapped for roles before reflections are saved, and organisation leads see only anonymised, aggregated trends.
5. Reflections are never used to train AI models.

4. Definitions

Personal data — information that identifies a person, on its own or combined with other information. Special category data (such as health or ethnicity) is more sensitive and processed only in limited circumstances.

Data Protection Policy

Amplify Yourself Ltd takes the privacy of personal data very seriously. We know what personal data we hold and we take steps to make sure it is handled legally, securely, efficiently and effectively.

Initiative — any new or changed product, feature, process, project, system, research study or supplier.

DPIA — a systematic process for identifying and reducing the data protection risks of an initiative, focusing on the likelihood and severity of harm to individuals.

5. When we carry out a DPIA

We carry out a DPIA before any processing that is likely to result in a high risk to individuals, and as good practice for every new initiative involving personal data. This includes new app features using AI, any work involving children or vulnerable adults, research and evaluation projects, and new suppliers who process personal data for us.

Risks do not have to be eliminated, but they must be reduced to an acceptable level. If a high risk cannot be reduced, we consult the Information Commissioner's Office (ICO) before processing begins.

6. The DPIA process

Data Protection Policy

Amplify Yourself Ltd takes the privacy of personal data very seriously. We know what personal data we hold and we take steps to make sure it is handled legally, securely, efficiently and effectively.

1. Describe the initiative: what data, whose, why, how it flows and who can access it.
2. Check necessity and proportionality: is each item of data really needed?
3. Identify risks to individuals and rate their likelihood and severity.
4. Agree measures to reduce each risk and record who is responsible.
5. Sign off, record the outcome and review the DPIA whenever the initiative changes, and at least annually.

7. Organisations using our apps

When schools, trusts or organisations license our apps, they are the data controller and we act as their data processor under a written agreement. We provide a DPIA pack to support their own assessment.

8. Roles and responsibilities

Director — overall accountability for data protection and sign-off of DPIAs.

Everyone working with us — understand this policy, recognise when a DPIA may be needed and raise it before work starts.

9. Your rights

You can ask to see, correct, export or delete your personal data, or object to how it is used, by emailing hello@amplifyourself.com. You can also complain to the ICO at ico.org.uk.