



Data Protection Policy

September 2026

1. Purpose of this Policy

This policy sets out how Prime Tutors Nottingham Ltd (“the Organisation”) collects, stores, uses, shares, and protects personal data in accordance with the UK GDPR and the Data Protection Act 2018.

Data protection ensures that personal information is processed fairly, lawfully, securely, and responsibly. This policy ensures that all staff, tutors, contractors, and volunteers understand their responsibilities and follow safe data-handling practices.

Prime Tutors Nottingham Ltd is **registered with the Information Commissioner’s Office (ICO)** as a Data Controller.

2. Scope

This policy applies to:

- All staff, tutors, contractors, volunteers, and directors
- All personal data processed by Prime Tutors Nottingham Ltd
- All systems used by the Organisation, including:
 - **Google Workspace (Google Drive, Gmail, Docs, Sheets)**
 - **WhatsApp** (for essential internal communication only)
 - Secure organisational email accounts

It covers personal data relating to:

- Students
- Parents/carers
- Staff and tutors
- Applicants
- Partner organisations
- Any other individuals whose data we process

3. Definitions

Personal Data

Information relating to an identified or identifiable individual, including names, contact details, identification numbers, online identifiers, and more sensitive information such as health or safeguarding data.

Special Category Data

Includes:

- Health information
- Ethnicity
- SEND information
- Safeguarding information
- Other categories listed under UK GDPR

Data Subject

Any living individual whose personal data we process.

Processing

Any action performed on personal data, including collecting, storing, sharing, deleting, or organising.

Data Controller

Prime Tutors Nottingham Ltd acts as the Data Controller for all personal data processed by the Organisation.

4. Data Protection Principles

Prime Tutors Nottingham Ltd adheres to the seven UK GDPR principles:

1. **Lawfulness, fairness, transparency**
2. **Purpose limitation**
3. **Data minimisation**
4. **Accuracy**
5. **Storage limitation**
6. **Integrity and confidentiality**
7. **Accountability**

We take responsibility for how personal data is processed and ensure compliance can be demonstrated.

5. How We Collect and Use Personal Data

We collect only the minimum data required to deliver safe, effective alternative provision.

5.1 Student Data

We collect:

- First name
- Year group / key stage
- Subject(s)
- Essential learning needs
- SEND information (where relevant)
- Safeguarding information (where relevant)

Data minimisation:

Tutors receive **first-name-only identifiers** and only essential information required to teach safely and effectively.

5.2 Parent/Carer Data

- Name
- Contact details
- Billing information (where applicable)

5.3 Staff and Tutor Data

- Name and contact details
- DBS status
- Qualifications
- Contractual information
- Training records

Storing DBS outcomes constitutes processing “criminal offence data,” even when no convictions are present.

6. Lawful Bases for Processing

We rely on the following lawful bases:

- **Public task / legitimate interests** – delivering education services
- **Legal obligation** – safeguarding, DBS checks, tax and employment law
- **Contract** – providing tuition services
- **Consent** – optional communications, use of photos, testimonials

7. Data Storage and Security

7.1 Google Drive & Google Workspace

All organisational data is stored within **Google Workspace**, which provides:

- Encrypted cloud storage
- Access controls
- Audit logs
- Two-factor authentication

Access is restricted to authorised staff only.

7.2 Email

Emails containing personal data:

- Use first-name-only identifiers where possible
- Avoid special category data unless necessary
- Are sent only via secure organisational accounts

7.3 WhatsApp (Internal Communication Only)

WhatsApp may be used for essential internal communication between staff and tutors.

To ensure safe use:

- Only organisational WhatsApp accounts may be used
- No full student profiles are shared
- Only essential teaching information is shared
- Staff must ensure their device is password-protected and locked when not in use
- Staff must delete messages containing personal data once no longer required

WhatsApp must **never** be used to store or transfer safeguarding documents, SEND reports, or any special category data.

7.4 Devices

Staff must:

- Use password-protected devices
- Enable screen-lock and encryption
- Avoid storing personal data locally unless necessary
- Report lost or stolen devices **immediately to the Director**

8. Data Sharing

We share personal data only when necessary and proportionate.

8.1 Internal Sharing

Tutors receive:

- First name
- Essential learning information
- SEND or safeguarding information only where required for safe practice

8.2 External Sharing

We may share data with:

- Local authorities (for safeguarding)
- Commissioning schools
- Emergency services
- HMRC (employment/tax compliance)

Safeguarding guidance states that **fears about sharing information must not prevent necessary safeguarding action.**

9. Data Retention

We retain data only for as long as necessary.

Retention periods:

- **Student records:** 3 years after last contact
- **Safeguarding records:** in line with statutory guidance
- **Staff records:** 6 years after employment ends
- **DBS records:** outcome only, retained in line with DBS Code of Practice

10. Data Subject Rights

Individuals have the right to:

- Be informed
- Access their data
- Rectify inaccuracies
- Request erasure (where applicable)
- Restrict processing
- Object
- Data portability

Requests must be submitted to the Data Protection Officer (DPO).

We respond within statutory time limits.

11. Data Breaches

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access.

11.1 Internal Reporting

All staff **must report suspected breaches immediately to the Director and the DPO.**

Staff are personally responsible for:

- Protecting any data they handle
- Reporting concerns straight away
- Cooperating fully with breach investigations

11.2 ICO Notification

We will notify the ICO within **72 hours** where a breach is likely to pose a risk to individuals.

11.3 Informing Data Subjects

Where there is a high risk, affected individuals will be informed without undue delay.

12. Data Protection Officer (DPO)

Prime Tutors Nottingham Ltd appoints a DPO in accordance with Article 37 UK GDPR.

The DPO must have expert knowledge of data protection law and operate independently.

DPO contact details are published on:

- The Organisation's website
- All privacy notices

13. Staff Responsibilities

All staff and tutors must:

- Complete annual data protection training
- Follow this policy and related procedures
- Use only approved systems (Google Workspace, email, WhatsApp)
- Report concerns or breaches **immediately to the Director**
- Maintain confidentiality at all times

14. Policy Review

This policy is reviewed annually or sooner if:

- Legislation changes
- New systems are introduced
- A significant incident occurs