Prime8 Education
Data Protection / Handling Policy

Introduction

Prime8 collects, stores and processes personal information about staff, students, parents or carers and other individuals who come into contact with the provision, in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.
This information is gathered in order to enable the provision of education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the provision complies with its statutory obligations. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

This data protection policy ensures Prime8:

- Complies with data protection law and follow good practice
- Protects the rights of staff and other professionals
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 2018 describes how organisations must collect, handle and store personal information. It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of data.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.
To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be specific for its purpose
3. Be adequate and only for what is needed
4. Be accurate and kept up to date
5. Not kept longer than needed
6. Take into account people's rights
7. Be kept safe and secure

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject- students and families	The identified or identifiable individual whose personal data is held or processed.
Data controller- management	A person or organisation that determines the purposes and the means of processing of personal data.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

This policy applies to:

- The admin of Prime8
- All staff and volunteers of Prime8
- All contractors, suppliers and other people working on behalf of Prime8.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- plus, any other information relating to individuals

Data protection risks

This policy helps to protect Prime8 from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Prime8 has some responsibility for ensuring data is collected, stored and handled appropriately.
Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, these people have key areas of responsibility:

The **Director** is ultimately responsible for ensuring that Prime8 meets its legal obligations.

The **management** is responsible for:

- Keeping the Director updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Prime8 holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

The **IT lead** is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.

- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

The **staff** are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the provision of any changes to their personal data, such as a change of address
- Contacting the managers in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed o If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside of UK
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

Third-Party Data Processors

Where external companies are used to process personal data on behalf of Prime8, responsibility for the security and appropriate use of that data remains with Prime8. Where a third-party data processor is used:

- a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
- reasonable steps must be taken that such security measures are in place;
- a written contract establishing what personal data will be processed and for what purpose must be set out;

Students are responsible for:

- familiarising themselves with the Data Protection Agreement
- ensuring that their personal data provided to Prime8 is accurate and up to date.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **Prime8 will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.

- Employees **should request help** from their line manager or the management if they are unsure about any aspect of data protection.

Data storage

Prime8 will only collect personal data for specified, explicit and legitimate reasons. These reasons will be explained to the individuals when data is first collected.

If Prime8 want to use personal data for reasons other than those given when first obtained, Prime8 will inform the individuals concerned beforehand and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the provision's record retention schedule.

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.
- When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers** and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones, without encryption.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

Personal data is of no value to Prime8 unless the Provision can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email without a password, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT lead can explain how to send data to authorised external contacts.
- Personal data should **not be transferred outside of the UK, without permission**
- Employees **should not save copies of personal data to their own computers**
- **Always access and update the central copy of any data.**

Data accuracy

The law requires Prime8 to take reasonable steps to ensure data is kept accurate and up to date.
The more important it is that the personal data is accurate, the greater the effort Prime8 should put into ensuring its accuracy.
It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a detail when they call.
- Prime8 will make it **easy for data subjects to update the information**
- Data should be **updated as inaccuracies are discovered**. For instance, if a family can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the manager's responsibility to ensure **databases are checked against industry suppression files** every six months.

Sharing Personal Data

Prime8 will not normally share personal data with anyone who is not linked to a student, but may do so where:

- There is an issue with a student or parent/carer that puts the safety of staff at risk
- Our suppliers or contractors need data to enable Prime8 to provide services to staff and students – for example, IT companies. When doing this, Prime8 will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

Prime8 will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud

- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

Prime8 may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects students or staff.

Where Prime8 transfers personal data to a country, we will do so in accordance with data protection law.

Subject Access Requests

All individuals and parents who are the subject of personal data held by Prime8 are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**.

Subject access requests from individuals should be made by email, addressed to the Director at info@prime8education.co.uk. The Director can supply a standard request form, although individuals do not have to use this.
The Director will always verify the identity of anyone making a subject access request before handing over any information.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of UK
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances) Individuals should submit any request to exercise these rights to the management. If staff receive such a request, they must immediately forward it to the management.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Prime8 will disclose requested data. However, the Director will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing Information

Prime8 aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

[This is available on request. A version of this statement is also available on the company's website.]

Technology

Photographs and videos

As part of provision activities, Prime8 may take photographs and record images of individuals within the provision.

Written consent will be obtained from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where parental consent is needed, Prime8 will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where parental consent is not required, Prime8 will clearly explain to the student how the photograph and/or video will be used.

Uses may include:

- Within provision on notice boards and in provision e-newsletters, etc.
- Outside of provision by external agencies such as the provision photographer, newspapers, campaigns
- Online on Prime8 website

Consent can be refused or withdrawn at any time. If consent is withdrawn Prime8 will delete the photograph or video and not distribute it further.

When using photographs and videos in this way Prime8 will not accompany them with any other personal information about the student, to ensure they cannot be identified.

See Prime8's child protection and safeguarding policy for more information on the use of photographs and videos.

Data protection by design and default

Prime8 will put measures in place to show that integrated data protection is in place into all data processing activities, including:

- Appointing a suitably qualified staff, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing privacy impact assessments where the provision's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the management will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and ensure compliance

- Maintaining records of processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the provision and management and all information required to share about the use and process of personal data (via privacy notices)
    - For all personal data that are held, maintaining an internal record of the type of data, data subject, how and why the data is used, any third-party recipients, how and why data is stored, retention periods and how data is kept secure

Disposal of data

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where Prime8 cannot or do not need to rectify or update it.

For example, Prime8 will shred or incinerate paper-based records, and overwrite or delete electronic files. Prime8 may also use a third party to safely dispose of records on the provision's behalf. If so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Breaches

All staff members have an obligation to report data protection breaches or contact the management if they have concerns of such a breach (info@prime8education.co.uk). This will allow the appropriate personnel to investigate further and take the appropriate steps to fix the issue in a timely manner.

What to do if staff fail to comply?

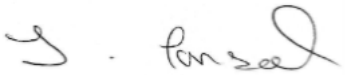
If data protection is not followed, this will be discussed in supervision meeting with staff and may involve staff warnings.

Staff training

Staff will have regular updates and training in GDPR.

Reviewing:

This guide and policy will be reviewed and updated if necessary, every two years. The Freedom of Information publication scheme will be reviewed regularly, with staff checking if they add a new piece of recorded information to the provision's portfolio that this is covered within the scheme.

Date of Completion	1.9.25	Signed:  Debbie Crookes (Tutor)
Date of Ratification	1.9.2025	Signed:  Julie Townsend (Director)
Date for Review	August 2026	

Appendix 1:

Requests for information

- The Freedom of Information Act came into force on 1st January 2005. Under this Act, all provisions that receive a written or emailed request for information which they hold or publish, are required to respond within 20 working days
- The provision will provide information on where to access the information required, e.g., the website link, or details of a charge if the publication/ information is charged or send any free information. If the item is charged the provision does not need to provide it until the payment is received
- A refusal of any information requested must state the relevant exemption which has been applied or that the provision does not hold the information, and must explain what public interest test has made if this applies
- If the information is published by another organisation the provision can direct the enquirer to the organisation which supplied the information or publication unless it is legal and possible to provide the information directly
- It will not be legal to photocopy a publication in its entirety and supply this to an enquirer unless the provision owns the copyright
- The provision will keep the original request and note against this who dealt with the request and when the information was provided
- Any complaint about the provision of information will be handled by the Head of Provision or a delegated member of the Senior Leadership Team. All complaints should be in writing and documented.
- All enquirers should be advised that they may complain to the information Commissioner if they are unhappy with the way their request has been handled.

[Your full address]
[Phone number]

[The date]

Prime8 Education
Unit 5, Stirling Road
Retford
Nottinghamshire
DN22 7SN

Dear Sir or Madam

Subject access request

[Your full name and address and any other details to help identify you and the information you want.]

Please supply the information about me I am entitled to under the GDPR relating to:
[give specific details of the information you want], for example

- your personnel file;
- emails between 'A' and 'B' (between 1/6/11 and 1/9/11);
- your medical records (between 2006 & 2009) held by Dr 'C' at 'D' hospital;

If you need any more information from me, or a fee, please let me know as soon as possible.

It may be helpful for you to know that a request for information under the GDPR should be responded to within 40 days.

If you do not normally deal with these requests, please pass this letter to your Data Protection Officer. If you need advice on dealing with this request, the Information Commissioner's Office can assist you and can be contacted on 0303 123 1113 or at ico.org.uk

Yours faithfully

[Signature]

DATA BREACH FORM

Complete this form and email it to the Data Protection Officer (DPO)

Please report a breach as soon as possible and in all cases within 24 hours. A breach has to be reported to the ICO within 72 hours. It is crucial to receive the notification of a possible reportable breach as early as possible to be compliant with the ICO 72 hours reportable regulations.

Notification of the Breach

Date & Time Breach discovered		Date & Time Breach reported to DPO	
Date & Time of the Breach		Place of Incident	
Name of Person reporting the Breach		Reporting persons contact details (email, telephone no)	
Brief Description & discovery of the incident			

Details of the Breach

Nature of the breach:- ☐Data was disclosed to an unauthorised person (Breach of Confidentiality) ☐Data was accessed by an unauthorised person (Breach of Confidentiality) ☐Data was altered (Breach of Integrity) ☐Data was lost (Breach of Availability) ☐Data was destroyed (Breach of Availability) *Root cause of breach:-* ☐Human error☐System Malfunction☐Cyber Attack☐Lost/Stolen IT equipment ☐Lost/Stolen Documents☐Other – Details:-
Brief Description of any action taken at the time of the discovery
Details of the information involved in the breach

Number of Data Subjects affected		Has any personal data been placed at risk? If so provide full details	
What is the nature of the information lost?			

Does the breached information contain any of the following sensitive information:-☐**Yes** ☐**No** ☐Racial or ethnic origin☐Political opinions or religious beliefs☐Trade Union Membership ☐Genetics☐Biometrics (where used for ID purposes)☐Sex Life / Sexual Orientation
Is there a possibility the information breached could be used to commit identity fraud?☐**Yes**☐**No** ☐Personal bank account☐Other financial information☐National Insurance Number ☐Copies of passports☐Copies of visas
Personal Information relating to vulnerable adults and children☐**Yes**☐**No**
Detailed Profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person(s) if disclosed☐**Yes** ☐**No**
Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals ☐**Yes**☐**No**
Security information that would compromise the safety of individuals if disclosed☐**Yes**☐**No**

Assessment of Data Breach by Data Protection Officer

Investigating Data Protection Officer is	
Incident Number	Date:

Assessment

Action taken
Severity of the Breach to data subject(s) and the organisation
Mitigation Actions
Assessment of risk to the rights and freedoms of data subjects: ☐Unlikely to result in a risk to the rights and freedoms of natural persons ☐Likely to result in a risk to the rights and freedoms of natural persons ☐Likely to result in a high risk to the rights and freedoms of the natural persons *Justification of decision*:
Details of any delay in reporting the breach within the 72 hour time frame if applicable

Notifications to	Date & Notes
☐Notification to Data Subjects ☐Notification to ICO ☐Notification to College Executive Committee ☐Incident reported to Police ☐Other Stake Holders (provide details)	
ICO Assessment details	**Date & Notes**
ICO data breach assessment has been conducted ICO data breach assessment has been completed ICO Assessment attached	

Outcomes

Follow up Action Required ☐**Yes (list below)**☐**No**	Date(s)
Staff Member involved in the breach received data protection training in the last 2 years? ☐Yes ☐No Detail any additional training / measures to be taken:-	

Risk Assessment of Data Breach ☐**Low** ☐**Medium** ☐**High**	**Risk Assessment rationale** **DPO Data Breach Completion Date**
OFFICE USE ONLY:- **Date DB Log Updated: Name:** **Record any follow ups by DPO on calendar:**	