Purple Ruler Data Protection Policy & Privacy Notice

Effective Date: 30/01/2023
Last Review Date: 30/01/2025
Next Review Date: 30/01/2026
Policy Owner: Data Protection Officer (DPO)
ICO Registration Reference: ZB398374

1. Overview

Data protection for our schools and clients are extremely important. Schools work with an incredible amount of personal data. This includes information such as pupil names, addresses, medical information, images, and more. Additionally, information related to job applicants, governors, staff, and volunteers is often stored within a school database.

The Data Protection Act (DPA) was designed to protect the privacy of individuals. When the DPA was updated to the GDPR in May 2018, the regulations around data protection changed throughout Europe. Schools handle what the GDPR classifies as ‘special category data,’ detailing pupil information such as ethnicity, race, biometric data, and trade-union membership

in some instances. This data is subject to strict controls, and therefore, schools need to adhere to GDPR guidelines and protect this information efficiently.

Data protection refers to safeguarding private and important information from compromise, corruption, and loss. Data protection is becoming ever more important in today' s data-driven society, as the amount of information created and stored expands year on year.

Our organisation aims to ensure that all personal data collected about clients, staff, pupils, parents, governors, visitors and other individuals are collected, stored and processed in accordance with UK data protection law and US FERPA, and PPRA respectively to the locations of our clients.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Schools and clients we serve provide us with varying amounts of data and information from their records. We adhere to the above principles to ensure that no matter what is passed to us, we interact with it in a manner supported in law.

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)
- UK ICO Guidelines
- Education (Pupil Information) (England) Regulations 2005
- British Association for Counselling & Psychotherapy (BACP) Ethical Guidelines

In addition, this policy complies with our funding agreement and articles of association. We are registered with the ICO. ICO Registration Reference: ZB398374

3. Data Protection Principles

Purple Ruler follows six key principles under the UK GDPR:

1. Lawfulness, Fairness, and Transparency – Data is processed legally and transparently.
2. Purpose Limitation – Data is collected for specific, legitimate purposes only.
3. Data Minimisation – We only collect the necessary data.
4. Accuracy – We ensure data is accurate and up to date.
5. Storage Limitation – Data is not kept longer than necessary.
6. Integrity and Confidentiality – Data is protected from unauthorised access or breaches.

4. Terms and Definitions

1. Data controller: A data controller is an individual or organisation that manages how data is processed and is responsible for complying with data protection regulations.
2. Data processor: The data processor is a person or other body, other than an employee of the data controller, who processes identifiable personal data on behalf of the data controller.
3. Data subject: The identified or identifiable individual whose personal data is held or processed.
4. Personal data: Any information that relates to a living individual which identifies them such as; name (including initials), identification number/s, their location data or online identifier, such as a user name. It may also be specific factors such as an individual' s medical, economic, cultural, physical or genetic identity.
5. Personal data breach: A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
6. Processing: Processing is when anything is done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. This can be manual or automated.
7. Special categories of personal data: This is personal data which is of a more sensitive nature and needs further protection such as; race, political views, religious or spiritual beliefs, genetics, medical and health records, sexual orientation, genetic information, biometric information, membership of specific groups such as trade unions.

5. Roles and responsibilities

This policy applies to all staff, contractors, in addition to any external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Data Controller

Purple Ruler (Enlai International Ltd and Purple Ruler LLC) is the Data Controller responsible for determining the purposes and means of processing personal data.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is Bella Ma and is contactable via bella.ma@purpleruler.com.

5.3 Data Processors

We use third-party data processors, including:

- Lessonspace (for online learning sessions, recording, and analytics).
- Lark (for communication and data storage).
- Microsoft (for communication, email exchanges between stakeholders).

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the organisation of any changes to their personal data, such as a change of address.
- Contacting the DPO in the following circumstances:
    - 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 the 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.
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.

- If they have any concerns that this policy is not being followed.
- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure

6. Third-Party Data Processor Compliance and Non-Compliance Actions

6.1 Compliance Requirements for Third-Party Processors

All third-party service providers that process personal data on behalf of Purple Ruler (Enlai International Ltd and Purple Ruler LLC) must comply with the following:

- UK GDPR & Data Protection Act 2018
- FERPA & PPRA (for U.S. student data)
- Contractual Data Processing Agreements (DPAs)
- Any other applicable laws and regulations based on the location of data processing

6.2 Monitoring and Compliance Assessment

To ensure compliance with our data protection and privacy standards, all third-party processors are:

- Required to complete a Vendor Compliance Assessment (VCA) before onboarding.
- Subject to annual compliance reviews to confirm ongoing adherence to regulations.
- Expected to provide evidence of compliance (such as GDPR certifications, SOC 2 reports, or ISO 27001 accreditation) when requested.
- Required to notify Purple Ruler’ s Data Protection Officer (DPO) of any changes that could impact compliance.

6.3 Actions Taken If a Third-Party Fails to Comply

If a third-party processor fails to meet compliance requirements, the following steps will be taken:

Step 1: Investigation & Risk Assessment

- The DPO will conduct an immediate review of the compliance failure.
- A Data Protection Impact Assessment (DPIA) will be initiated if the non-compliance poses a risk to data subjects.
- The third-party processor will be asked to submit a corrective action plan within 30 days.

Step 2: Corrective Action and Temporary Restrictions

- If the third party can demonstrate that they will implement corrective actions within 30 days, we may allow continued service use under restricted conditions.
- If necessary, Purple Ruler will restrict the processor' s access to certain categories of personal data until compliance is restored.

Step 3: Suspension or Termination of Contract

- If compliance cannot be achieved within 30 days, Purple Ruler reserves the right to suspend or terminate the data processing agreement with the third party.
- If termination occurs, Purple Ruler will:
  - Securely transfer or delete affected data from the third party' s systems.
  - Notify impacted schools, students, and staff if their data was compromised or at risk due to non-compliance.
  - Seek alternative compliant vendors for continued service provision.

6.4 Reporting Obligations and Data Breach Notifications

- If the non-compliance results in a data breach, Purple Ruler will notify the ICO (UK) or U.S. regulatory bodies (FERPA/PPRA compliance offices) within 72 hours.
- Affected individuals and organisations will be informed as soon as possible, with details of what data was impacted and mitigation steps taken.

8. Accountability and Legal Actions

- Any third-party processor that repeatedly fails to comply may face legal actions under contractual obligations.
- Purple Ruler may seek compensation for damages if the non-compliance causes financial or reputational harm.
- We will update our Approved Vendor List to reflect any service suspensions or removals.

7. Record of Processing Activities (ROPA)

The table below categorises the processing activities conducted by Purple Ruler.

Data Category	Purpose of Processing
Student Information	- To identify and enrol students into appropriate educational and therapy services. - To communicate with students, school and parents regarding lesson schedules, progress, and feedback.

	- To track and report attainment data for educational development and regulatory compliance.
Special Category Data (SEND, EHCP, Medical Needs)	- To assess individual learning needs and ensure appropriate educational support is provided. - To develop personalised learning plans and reasonable adjustments. - To ensure compliance with the Equality Act 2010 and SEND Code of Practice (UK). - To facilitate safeguarding measures and ensure the safety of vulnerable learners.
Lesson Recordings	- To ensure quality assurance and uphold educational standards. - To review and evaluate teaching effectiveness. - To investigate safeguarding concerns and ensure student and staff welfare. - To comply with legal and regulatory standards for online education.
Therapy Notes (Session Records, Clinical Assessments, Progress Reports)	- To track therapy progress and monitor student well-being. - To support safeguarding measures and ensure the safety of students. - To provide ethical and legal documentation for professional accountability under BACP. - To evidence interventions in case of legal inquiries or safeguarding reviews.
Teacher/Staff Data	- To manage HR records, including employment history, training, and qualifications, and to comply with safer recruit policies and regulations. - To process payroll, pensions, and tax obligations. - To monitor staff performance and ensure compliance with safeguarding policies in addition to the code of conduct and other obligations. - To investigate misconduct, safeguarding concerns, or disciplinary issues.
Parental & Guardian Data	- To communicate important updates related to student progress and wellbeing. - To obtain necessary consent for participation in lessons and therapy. - To comply with legal obligations regarding safeguarding and parental rights under UK GDPR and FERPA (US).
Safeguarding Records	- To protect at-risk children and comply with safeguarding obligations under KCSIE (Keeping Children Safe in Education 2023) and Children Act 1989/2004. - To document safeguarding interventions and referrals to relevant authorities. - To fulfil legal obligations in child protection cases and liaise with local authorities, social services, and law enforcement.

8. Lawful Bases for Data Processing

8.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that the organisation can fulfil a contract with the client, or the client has asked Purple Ruler to take specific steps before entering into a contract.
- The data needs to be processed so that the organisation can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the client, individual or another person i.e. to protect someone' s life.
- The data needs to be processed so that the organisation, as a public authority, can perform a task in the public interest or exercise its official authority.
- The data needs to be processed for the legitimate interests of the organisation (where the processing is not for any tasks the organisation performs as a public authority) or a third party, provided the individual' s rights and freedoms are not overridden.
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent.
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law.
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made manifestly public by the individual.
- The data needs to be processed for the establishment, exercise or defence of legal claims.
- The data needs to be processed for reasons of substantial public interest as defined in legislation.
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent.
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made manifestly public by the individual.
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights.
- The data needs to be processed for reasons of substantial public interest as defined in legislation.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

8.2 Limitation, minimisation and accuracy

- We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
- If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.
- Staff must only process personal data where it is necessary in order to do their jobs.
- We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.
- In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymise it.
- Lesson recordings and all associated lesson data with either be anonymised or deleted upon the expiry of the working relationship of the organisation with any given school or client.
- All associated data obtained from the school by the organisation pursuant to the education provision requested by the school is held in such a way as to be automatically deleted upon the expiry of the working relationship between Purple Ruler and the School or Client.

9. Data security and storage of records

Purple Ruler is committed to ensuring the highest level of data security and compliance with all UK (GDPR, DPA 2018) and US (FERPA, PPRA) regulations, as well as industry-specific guidance from BACP, KCSIE, and NHS DSPT. This section defines our approach to data storage, access control, retention, anonymisation, and disposal to prevent unauthorised access, loss, or breaches.

9.1 General Data Security Measures

We will protect all personal data by implementing technical, administrative, and organisational security controls.

1. Access Controls

- Data access is strictly role-based.
- Multi-Factor Authentication (MFA) is mandatory for all users accessing data processing platforms.
- All access to Lessonspace, Lark, and Microsoft platforms is logged and monitored.

2. Data Encryption and Security Standard:

- All stored student data, therapy records, and lesson recordings are protected with AES-256 encryption both at rest and in transit.
- Cloud storage providers used by Purple Ruler, including Lark and Lessonspace, adhere to ISO 27001 and SOC 2 compliance.
- Therapy notes stored in Lark Secure Cloud are separated from general student records and encrypted individually for an additional layer of protection.

3. Network Security

   Purple Ruler ensures secure IT infrastructure by implementing Cyber Essentials standards and using Sophos Endpoint Security on staff devices handling sensitive data.

4. Staff Security Responsibilities

   Staff are prohibited from storing student personal data on personal devices. Only approved, secure platforms may be used for processing and storing student data.

9.2 Student Data Storage and Processing Transparency

Purple Ruler ensures full transparency in how student data is processed, retained, and accessed.

1. Post-Service Data Retention

- Lesson Recordings: Stored for 12 months post-lesson for safeguarding and quality assurance.

- Student Records: Retained for 7 years post-service.
- Safeguarding Records: Retained in accordance with KCSIE guidelines, usually until the individual turns 25 or longer in cases of ongoing risk assessments.
- Storage method: Lesson recordings will be stored on Lessonspace cloud storage, other student information will be stored on Lark cloud storage.

2. Access Control & Anonymisation

- Only named personnel will be granted the permission to access the data that is relevant to them. This includes, safeguarding leads, school-authorised personnel, Quality Assurance team, Academics team, admin and compliance team.
- Anonymisation Process:
  - Upon data retention expiration, all identifiable student data is permanently erased.
  - Any retained lesson data is pseudonymised and used solely for training, research, or compliance verification.

9.3 Secure Storage of Counselling & Therapy Notes

1. Separation from Educational Data (BACP Compliance)

- Therapy notes must not be stored with general student records. It will be stored for 7 years post-therapy termination to comply with BACP.
- Therapy records are only accessible to:
  - The assigned therapist/counsellor.
  - The Designated Safeguarding Lead (DSL) (only in cases of safeguarding intervention).

2. Therapy Notes Storage & Security Protocols

- Digital Storage: Therapy notes are stored encrypted on Lark cloud storage. This includes, written notes by the therapist, recordings of the therapy session with the clients and other notes recorded regarding specific clients in the supervision sessions.
- Audit Logs: All access to therapy notes is monitored and logged to prevent unauthorised access.
- At the end of the 7-year retention period, all therapy notes will be permanently erased.
- Secure deletion will be audited and documented by the Data Protection Officer (DPO).

3. Supervision Record Storage

- Clinical supervision notes are stored separately from therapy session notes and student education records.

- Supervision records are accessible only to the Clinical Supervisor and DSL.
- Therapists cannot access their own supervision notes, in compliance with BACP record-keeping standards.

4. Secure Access & Retention

- Supervision notes include: Key discussion points, learning outcomes, therapist development progress.
- Retention Period: 7 years, then securely deleted.

9.4 Employee Monitoring Transparency

If Purple Ruler monitors employee emails, meetings, or work activity, the following must be explicitly stated.

1. Employee Awareness & Justification

- Employees must be informed of all monitoring activities.
- Purpose of Monitoring:
  - To ensure compliance, safeguarding, and security.
  - Not for intrusive surveillance.

2. Monitoring Scope

1. Emails & Communications: Emails and conversation exchanged via Microsoft Outlook, Lark, or other platforms may be subject to security audits for safeguarding and compliance.
2. Meeting Recordings & Logs: Meetings held with school leaders, therapists, or staff via Microsoft Teams, Zoom, or Lark should be recorded by default, unless any participant has denied permission to record. This is for note keeping, training and referencing.
3. Work Activity Monitoring: If employee work activity is monitored (e.g., tracking system logins, lesson engagement data), it will be for safeguarding, compliance, quality assurance and operational efficiency.

3. Employee Rights & Access to Monitoring Data

Employees have the right to:

- Request access to monitoring logs.
- Be notified when monitoring is in effect.
- Challenge unjustified or excessive monitoring.

All monitoring activities will strictly adhere to:

- UK GDPR (Article 6).
- ICO Employment Practices Code.

9.5 Data Disposal & Secure Destruction

- Personal data that is no longer needed will be securely deleted or anonymised.
- Data must not be retained beyond legal and regulatory requirements.
- Upon expiration of the retention period, all personal data will be securely erased using GDPR-compliant deletion methods (e.g., high levels of encryption before deletion, hard drive sanitisation, paper shredding for physical records).
- A data deletion log will be maintained by the Data Protection Officer (DPO) to audit compliance with retention policies.

10. Sharing personal data

We will not share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT services. When doing this, we will:
    - Establish a contract with the supplier or contractor 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
- For safeguarding reasons.

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

11. Subject access requests and other rights of individuals

At Purple Ruler, we prioritise the privacy and rights of individuals regarding their personal data. Our processes for responding to information rights requests are comprehensive, ensuring compliance with GDPR and other relevant data protection regulations. These processes are designed to handle requests efficiently and transparently, providing individuals with timely access to their data and the ability to exercise their rights.

11.1 Types of Information Rights Requests

The types of requests we manage include:

- Subject Access Requests (SARs)
- Requests for Rectification
- Requests for Erasure (Right to be Forgotten)
- Requests for Restriction of Processing
- Requests for Data Portability
- Objections to Processing
- Rights Related to Automated Decision-Making and Profiling

11.2 Submission of Requests

- Requests can be sent in writing to DPO@purpleruler.com.
- We may ask for 2 forms of proof of identity to process the request (e.g., a copy of an ID card or passport).
- Clear and specific details about the request, including the type of information sought, corrections needed, or other rights being exercised.

11.3 Acknowledgment

- Requests are acknowledged within 5 business days of receipt.
- The DPO verifies the identity of the requester and the validity of the request.
- Each request is logged in our Data Protection Management System, noting the date of receipt, type of request, and details provided.

11.3.1 Subject Access Requests (SARs)

- Data Compilation: Gather all relevant personal data held by Purple Ruler.
- Data Review: Ensure no third-party personal data is disclosed without consent.
- Response: Provide a copy of the requested data, an explanation of how it is used, and who it has been shared.

11.3.2 Requests for Rectification

- Data Verification: Verify the data that needs correction.
- Amendment: Correct inaccuracies or incomplete data.
- Notification: Inform the individual of the rectification and any relevant third parties.

11.3.3 Requests for Erasure

- Eligibility Check: Determine if the data qualifies for erasure under GDPR.
- Data Removal: Securely delete the data from all systems.
- Confirmation: Notify the individual of the data erasure.

11.3.4 Requests for Restriction of Processing

- Temporary Suspension: Temporarily restrict the processing of the data.
- Assessment: Review the grounds for restriction.
- Outcome Communication: Inform the individual of the restriction status and any subsequent steps.

11.3.5 Requests for Data Portability

- Data Preparation: Compile the data in a structured, commonly used, and machine-readable format.
- Transfer: Send the data to the individual or a designated third party securely.
- Confirmation: Notify the individual once the transfer is complete.

11.3.6 Objections to Processing

- Assessment: Evaluate the grounds for objection.
- Decision: Cease processing if the objection is upheld, or provide a justification if processing continues.
- Notification: Inform the individual of the decision and any actions taken.

11.3.7 Processing Time

- We aim to process and complete all requests within 30 working days Processing Requests.
- If a request is complex or numerous, an extension of up to 60 days may be applied. In such cases, an administration fee may be charged for the completion of the process.
- If the request is unfounded or excessive, we may refuse to act on it. We will take into account whether the request is repetitive in nature when making this decision.

- When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

11.4 Communication, Data Security and Confidentiality

- Provide regular updates to the requester on the status of their request. Ensure all communications are clear and transparent.
- Use encryption for all data transfers.
- Limit access to personal data to authorised personnel only.
- Ensure no unauthorised disclosure of personal data during the request process.
- We may not disclose information for a variety of reasons, such as if it:
- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would include another person’ s personal data that we can’ t reasonably anonymize, and we don’ t have the other person’ s consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

11.5 Other data protection rights of the individual

In addition to the right to make a subject access request, 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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

12. Data Protection Impact Assessment (DPIA) Procedure

Purple Ruler is committed to ensuring that all personal data processing activities comply with the UK GDPR, Data Protection Act 2018, ICO guidance, and sector-specific regulations (Education, Therapy, and Online Learning). A Data Protection Impact Assessment (DPIA) is required whenever data processing poses a high risk to the rights and freedoms of individuals, particularly children.

A DPIA is a systematic process to identify, assess, and mitigate risks before implementing any new data processing activity, system, or technology. This ensures compliance with data protection laws and safeguards student, staff, and client data.

12.1 DPIA Process

The DPIA process consists of **six key steps**, ensuring that risks are identified, assessed, and mitigated effectively.

Step 1: Identify the Need for a DPIA

- The DPO, in consultation with relevant teams, will determine if a DPIA is required.
- A preliminary risk assessment will be conducted based on ICO guidance.

Step 2: Describe the Processing Activity

The DPIA report must include:

- Purpose of processing
- Categories of data processed
- Data subjects
- Third parties involved
- Storage location and retention period

Step 3: Assess Risks to Individuals

Each processing activity will be evaluated for risks to personal data, including:

- Risk of unauthorised access or breaches
- Risk of data being exposed or misused
- Risk of non-compliance with company policies

Step 4: Identify and Implement Risk Mitigation Measures

To reduce risks, the following security and compliance measures may be implemented:

- Encryption & Access Controls
- Data Minimisation, Anonymisation or pseudonymisation
- Setting Permissions Levels for different personnel accessing data.
- Third-Party Processor Compliance
- Parental & Student Rights Protections
- Automated Risk Alerts Step 5: Approvals and Documentation
- The DPO must approve all DPIAs before implementing new data processing activities.
- A DPIA Report must be documented, outlining:
  - The identified risks
  - Mitigation measures
  - Justification for proceeding with the processing activity
- If the risks cannot be fully mitigated, the ICO must be consulted before proceeding.

Step 6: Ongoing Monitoring & Review

DPIAs must be regularly reviewed and updated when:

- A new forms of data, system or technology is introduced to the existing operational procedures
- A significant change occurs in data processing activities
- A data breach or security incident occurs related to a previously assessed process

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, 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 data protection impact assessments where the organisation' s processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO 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 make sure we are compliant
- Data is stored exclusively in our servers physically located on the premises of our institutional investor, ADM Computer Services Limited.
- Maintaining records of our processing activities, including:
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure
- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

14. Training

- All teaching staff, contractors and third party service providers are required to read this policy thoroughly before engaging with Purple Ruler.
- All full time staff who will have access and require management of personal and sensitive data are provided with data protection training as part of their induction process.
- Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school’ s processes make it necessary.

15. Monitoring arrangements

- The DPO is responsible for monitoring and reviewing this policy.
- This policy will be reviewed annually or when it is necessary to reflect changes in practice or legislation and approved by the CEO.

16. Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner’ s Office (ICO).

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the data protection officer (DPO) by making direct contact via Lark messenger. The DPO will advise the reporter on the required information necessary for the investigation.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Director's team.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from third party providers).
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO’ s self-assessment tool.
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on Lark.
- Where the ICO must be notified, the DPO will do this via the ‘report a breach’ page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the organisation’ s awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO

- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the organisation’ s awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the organisation is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
  - A description, in clear and plain language, of the nature of the personal data breach
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored set out where you will keep these records – for example, on the school’ s computer system, or on a designated software solution.

- The DPO and CEO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and CEO will meet regularly quarterly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches
- Purple Ruler conducts annual data breach simulations to test response readiness.
- Staff receive mandatory annual training on identifying and responding to data security incidents.
- All breach response procedures are logged and reviewed quarterly.

17. Appendix 2: Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school’ s email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it’ s appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

18. External Data Processing and Risk Controll

External Processor	Purpose for processing	Risk Mitigation
Lark Information Technologies	Information sotrage and general communication internally	Seperated Server under our own controll. 3rd party cannot access.
The Lessonspace	Running Lessons online. Reviewing taught lessons.	Personal Information anonomysed. Data cannot be downloaded

19. Appendix 3: Data Security Incident Response Policy

The Data Security Incident Response Policy at Purple Ruler is designed to provide a structured approach to identifying, managing, and mitigating data security incidents. This policy ensures compliance with current data protection legislation, including GDPR and ICO codes of practice. It applies to all employees, contractors, volunteers, and third-party partners.

1. Incident Identification

- Implement continuous monitoring tools to detect unusual activities or potential security breaches.
- Encourage employees and partners to report any suspicious activities or potential data breaches immediately through established reporting channels.

2. Incident Reporting

- All incidents must be reported to the Data Protection Officer (DPO) within 24 hours of detection. Use the designated incident reporting form or dedicated email (DPO@purpleruler.com).
- The DPO will conduct an initial assessment to determine the severity and scope of the incident, within the initial 48 hours of receiving the report.

3. Incident Classification

- Classify incidents based on their impact and urgency. Categories may include minor, significant, and critical incidents.
- Maintain detailed records of each incident, including time of occurrence, affected systems, and initial assessment results.

4. Response and Containment

- Implement measures to contain the incident, such as isolating affected systems, revoking compromised credentials, and applying necessary patches.
- Inform relevant stakeholders, including affected individuals, management, and regulatory bodies, as required.

5. Investigation and Analysis

- Conduct a thorough investigation to determine the root cause of the incident.
- Utilise data forensics tools to analyse affected systems and recover evidence.
- Document findings and lessons learned to prevent future occurrences.

6. Mitigation and Recovery

- Develop and implement remediation plans to address identified vulnerabilities.
- Ensure affected systems are securely restored to normal operations.
- Update security policies and procedures based on incident analysis.

7. Communication and Reporting

- Regularly update internal stakeholders on the status of the incident and recovery efforts.
- Report significant incidents to the Information Commissioner’ s Office (ICO) within 72 hours, as required by GDPR. Notify affected individuals promptly.

20. Appendix 4: Information Security Management Policy

The Information Security Management Policy ensures the protection of Purple Ruler’ s information assets against all internal and external threats. This policy is applicable to all employees, contractors, volunteers, and third-party partners.

1. Information Security Objectives

- Ensure that sensitive information is accessible only to those authorized to access it.
- Safeguard the accuracy and completeness of information and processing methods.
- Ensure that authorised users have access to information and associated assets when required.

2. Roles and Responsibilities

- Data Protection Officer (DPO) oversees the implementation of the Information Security Management Policy and ensures compliance with relevant regulations.
- Employees and Contractors: Required to adhere to security policies and report any security incidents or vulnerabilities.

3. Risk Management

- Risk Assessment: Conduct regular risk assessments to identify potential security threats and vulnerabilities.
- Risk Mitigation: Implement appropriate controls to mitigate identified risks, including technical, administrative, and physical safeguards.

4. Access Control

- User Access Management: Ensure that access to information systems is granted based on the principle of least privilege.
- Authentication and Authorization: Use strong authentication methods and ensure that access rights are regularly reviewed and updated.

5. Data Protection

- Encryption: Encrypt sensitive data both in transit and at rest to protect against unauthorized access.
- Data Minimization: Collect and retain only the minimum amount of data necessary for business operations.
- Data Retention and Disposal: Establish and enforce data retention schedules and ensure secure disposal of data that is no longer needed.

6. Network Security

- Firewall and Intrusion Detection: Implement firewalls, intrusion detection, and prevention systems to protect the network from unauthorized access and attacks.
- Secure Configuration: Ensure that all network devices and systems are securely configured and regularly updated.

7. Physical Security

- Secure Facilities: Ensure that all facilities housing information systems are physically secure and access is restricted to authorized personnel.
- Environmental Controls: Implement controls to protect against environmental threats such as fire, flood, and power outages.

8. Incident Management

- Incident Response Plan: Develop and maintain an incident response plan to handle security incidents promptly and effectively.
- Incident Reporting: Ensure that all security incidents are reported, documented, and investigated.

21. U.S. Education Data Privacy Policy Addendum (15/ October / 2023)

Purple Ruler is committed to protecting the privacy of student data and ensuring compliance with applicable U.S. laws, including the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA), as part of our service to school districts providing tutoring services.

Collection and Use of Information

As a third-party provider to school districts, Purple Ruler collects only the necessary personal information to facilitate effective tutoring services. This includes:

- Student Names: To personalize and tailor the tutoring sessions to individual students.
- Email Addresses: To communicate with students regarding scheduling, feedback, and support for their tutoring sessions.
- Academic Information: To assess the needs of students and provide customized tutoring that addresses their specific academic challenges.

Rights and Responsibilities

Parental Rights: Under FERPA, parents have the right to inspect and review their child's education records maintained by Purple Ruler. Requests for access to records must be submitted in writing and will be fulfilled within a reasonable time frame, not exceeding 45 days.

Student Rights: Students who are aged 18 or older, or attending a postsecondary institution, are considered "eligible students" and may exercise rights to inspect and review their educational records directly.

Disclosure of Information: Purple Ruler may disclose personal information from education records without consent to the extent permitted under FERPA regulations. This includes disclosures to:

- Officials with legitimate educational interests;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- Compliance with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies;
- State and local authorities, within a juvenile justice system, pursuant to specific State law.

Data Protection: Purple Ruler employs industry-standard security measures to protect the integrity and confidentiality of student information. Access to data is limited to authorized

personnel who are trained in compliant data handling practices.

Opt-Out Rights

Under PPRA, parents and eligible students have the right to opt out of any survey, analysis, or evaluation that reveals information concerning:

- Political affiliations or beliefs;
- Mental or psychological problems;
- Sex behavior or attitudes;
- Illegal, anti-social, self-incriminating, or demeaning behavior;
- Critical appraisals of other individuals with whom respondents have close family relationships;
- Legally recognized privileged relationships;
- Religious practices, affiliations, or beliefs;
- Income for program eligibility determination.

Amendments and Updates to Personal Information

Parents and eligible students have the right to request the amendment of records that they believe to be inaccurate, misleading, or in violation of the student’ s privacy rights. Such requests must be made in writing and will be reviewed promptly. If the request is denied, the parent or eligible student will be provided with information on how to request a formal hearing.

22. Contact Information

For questions or concerns regarding this policy or the handling of personal information, please contact our Data Protection Officer at:

DPO@purpleruler.com

This policy complements our comprehensive GDPR-compliant data protection policy, ensuring adherence to specific U.S. regulatory requirements while safeguarding the rights and privacy of our users.