Ian Stokes
Education Ltd
expert independent data analysis & training

ian@ianstokes.org
www.ianstokes.org
07954 139274

Ian Stokes Education Ltd
Data Protection Policy

Signature: *Ian Stokes* **(Director)**

Next Review Date: November 2026

Executive Summary

This Data Protection Policy serves as a comprehensive framework for our company to ensure that all personal data handled within the business environment is managed in a manner that complies with all relevant data protection laws.

The company is committed to fostering a culture of data protection and privacy, recognising the importance of safeguarding personal information belonging to students, parents, staff, and other stakeholders. This policy outlines our approach to collecting, processing, storing, and sharing data, ensuring that rights and freedoms are respected.

Key Objectives of the Policy

- **Transparency**: We aim to communicate clearly how and why personal data is collected and used, ensuring that individuals are informed and can exercise their rights.
- **Data Integrity and Security**: We implement robust security measures to protect personal information from unauthorised access, loss, or misuse.
- **Compliance**: We adhere to all legal and regulatory requirements related to data protection, including conducting regular audits and training staff on best practices.
- **Rights of Individuals**: We empower students, parents, and staff to understand their rights regarding their personal data, including the right to access, rectify, and delete their information upon request.

This policy is an essential element of our commitment to creating a safe and secure environment for our staff and customers. It is reviewed annually or as needed to accommodate changes in legislation or business operations.

Contents

1. Aims

This Data Protection Policy outlines our commitment to maintaining the privacy and protection of personal data in accordance with the Data Protection Act (2018) and UK General Data Protection Regulation (UK GDPR) as amended by the Data (Use and Access) Act 2025 and relevant data protection legislation.

The policy is intended for:

- Staff: All employees who handle personal data
- School Leaders and other customers: Individuals responsible for overseeing and ensuring compliance with data protection practices
- Third Party – Contractors: External organisations or individuals processing data on behalf of the business must understand their responsibilities under this policy.

We aim to make sure that all personal information is collected, stored, and used according to UK data protection laws. This policy covers all personal data, whether it is on paper or stored electronically.

2. Legislation and guidance

This policy meets our obligations under the:

Data Protection Act 2018 (DPA 2018)
UK General Data Protection Regulation (UK GDPR)
Date (Use and Access) Act 2025 (DUAA)

It is based on guidance published by the Information Commissioner's Office (ICO), which following the enactments of the DUAA will be replaced by the Information Commission, UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education. It also reflects the ICO's guidance for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living 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	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our business handles personal data provided by customers about students, which makes it a data controller. It also handles data about our staff. This is called processing within the legislation. The business is registered with the Information Commissioner's Office (ICO) and will pay the required registration fee each year or as legally needed.

5. Roles and responsibilities

This policy applies to all staff and to any outside organisations or individuals working for the company. Staff who do not follow this policy may face disciplinary action.

5.1 Directors

The Directors of the company are responsible for ensuring the business meets all data protection requirements. The Directors also have overall operational responsibility for day-to-day data privacy and control matters.

5.2 Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for overseeing this policy, making sure we follow data protection laws, and creating related policies and guidelines as needed.

The DPO will submit an annual report on their work to the Directors and will also share any advice or recommendations on data protection issues when relevant.

The first point of contact for individuals whose data is processed by the business is the data protection lead. This is the Director. However, individuals may contact the DPO direct if the need arises. The DPO is first point of contact for the ICO.

Full details of the DPO's responsibilities are set out in the Service Level Agreement.

Our DPO is Bywater Kent Support Services Ltd and is contactable via email at DPO@bywaterkent.co.uk

The business is registered with the ICO (Information Commissioner's Office) and has paid the required data protection fee.

5.3 Staff

All staff are responsible for:

- Collecting, storing, and using any personal data in line with this policy.
- Letting the company know about any changes to their personal information, like a new address.
- Contacting the DPO in the following cases:
    - If they have questions about how this policy works, data protection law, keeping data, or data security.

- If they're concerned that the policy isn't being followed.
- If they're unsure whether they have legal permission to use personal data in a specific way.
- If they need to seek consent, create a privacy notice, address data protection rights someone has requested, or transfer personal data outside the UK.
- If there has been a data breach.
- If they're starting a new activity that might impact individuals' privacy rights.
- If they need help with contracts or sharing personal data with outside parties.

6. Data protection principles

The UK GDPR is founded on data protection principles that our business is required to follow. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the business aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the company can fulfil a contract with the customer, or the customer has asked the company to take specific steps before entering into a contract
- The data needs to be processed so that the company can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the company 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 company or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer or school when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer or school 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 or school 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.

7.2 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 their permission, 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 anonymised. This will be done in accordance with the company's record retention schedule.

8. Sharing Personal Data

We usually don't share personal data with others, but we may do so in certain cases, such as:

- When our suppliers or contractors need data to help provide services to staff, like IT support. In these cases, we will:

- Only hire suppliers or contractors that can prove they follow UK data protection laws
- Set up a data sharing agreement, either in the contract or as a separate document, if we are sharing significant or sensitive data, to ensure data is handled fairly and legally
- Only share the data the supplier or contractor needs to provide their service and any necessary information to keep them safe

We will also share personal data with law enforcement or government bodies if legally required to do so.

In emergencies affecting our staff, we may share personal data with emergency services and local authorities to assist them in their response.

If we transfer personal data internationally, including to countries in the European Economic Area, we will follow UK data protection laws.

9. Subject access requests and other rights of individuals

9.1 Subject Access Requests (SARs - also called Data Subject Access Requests or DSARs)

Individuals have the right to request access to personal information that the company holds about them**.**

- This may include:
- Confirmation that their data is being used
- Access to a copy of their data
- The reasons for data processing
- The types of data being processed
- Who the data is shared with
- How long the data will be kept, or how this period is decided
- The right to request changes, deletion, restrictions, or to object to data processing
- The right to file a complaint with the ICO or other relevant authority
- The source of the data if not provided by the individual
- Whether automated decision-making affects their data and what impact it may have
- Any protections in place if their data is shared internationally

Subject access requests can be submitted in any format, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name/ Contact address/ Phone number and email
- Information being requested
- Reason for requesting the information (so that we locate and prioritise the datasets that will be of most value).

If staff receive a subject access request in any form, they must forward it to the data protection lead immediately.

9.2 Children and Subject Access Requests

A child's personal data belongs to the child, not to their parents or carers. For a parent or carer to make a request for a child's data, the child must either not understand their data rights or have agreed to the request.

Generally, children under 12 are considered too young to fully understand these rights, so most requests from parents for pupils' data may be granted without the child's direct permission. However, this is assessed on a case-by-case basis.

9.3 Responding to Subject Access Requests

When we respond to requests:

- We may ask the individual for a form of ID.
- We may contact them by phone to confirm the request
- We will respond within 1 month of receiving the request or required identification
- We will provide the information at no cost
- If the request is complex, we may take up to 3 months and will inform the individual within 1 month, explaining the need for extra time

We may not provide information if it:

- Could seriously harm the physical or mental health of the student or another person
- Involves child abuse details where sharing would not be in the child's best interests
- Contains personal data about someone else that cannot be anonymised, and we do not have consent to share it
- Is part of certain sensitive documents like legal, crime, immigration, management, or exam-related records

If the request is unreasonable or repeated, we may refuse or charge a fee to cover costs. If we refuse a request, we will explain why and inform the individual of their right to contact the ICO or to seek a legal resolution.

The Data Protection Officer shall provide guidance and oversee the response ensuring that this is within the spirit of the principles of the UK GDPR and in accordance with the legislation.

9.4 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request, individuals also have the right to:

- Withdraw their consent to data processing at any time
- Ask for correction, deletion, or limited processing of their data (in certain cases)
- Prevent their data from being used for direct marketing

- Object to data processing based on public interest or legitimate interests
- Challenge decisions made by automated data processing with no human involvement
- Be notified of a data breach (in some cases)
- Submit a complaint to the ICO
- Request that their data be transferred to another party in a structured, common, and machine-readable format (in certain cases)

Individuals can submit requests for these rights to the data protection lead or to the DPO. If staff receive such a request, they should forward it to the data protection lead who will consult the DPO.

10. Biometric recognition systems and Artificial intelligence

10.1 Biometric recognition systems

If staff members or other adults use the school's biometric systems, we will also get their permission before they start using it, and we will offer alternatives if they prefer not to participate.

Staff can withdraw consent at any time, and the company will delete any related data already collected.

10.2 Artificial Intelligence (AI)

AI tools are now common and easy to use. Staff may be familiar with generative AI chatbots like ChatGPT and Copilot, the company understands that AI can help with our work, but it also has risks for personal and sensitive information.

To keep this information safe, no one is permitted to enter personal or sensitive data into unauthorised AI tools or chatbots. If anyone does enter such data into an unauthorised generative AI tool, the company will treat it as a data breach and will follow the procedures for handling personal data breaches outlined in Appendix 1.

11. CCTV

If we have CCTV installed, we may use CCTV in different areas around the premises to help keep the site safe. We follow the ICO's guidelines on using CCTV and comply with data protection rules. We don't need to get permission from individuals to use CCTV, but we make it clear where people are being recorded. Security cameras are easy to see, and there are clear signs explaining that CCTV is in use.
If you have questions about the CCTV system, please contact the Directors**.**

12. Photographs and videos

As part of our business activities, we may use photos and videos of people in documents produced for customers.

All images will be obtained from sources that are already in the public domain (e.g. school website, or documents published on the school website).

When we use photos and videos in this way, we will not include any other personal information about the child to keep them anonymous.

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 (see section 6)
- Completing privacy impact assessments where the company'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
- Putting appropriate checks in place if we transfer any personal data outside the UK where no adequacy agreements are in place
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our company and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will keep personal data safe from unauthorised access, changes, processing, or sharing, and protect it from accidental loss, destruction, or damage. In particular: paper records and portable electronic devices, like laptops and hard drives with personal data, will be kept locked when not in use. Papers with confidential personal data should not be left on office desks, or in any place that is easily accessible. If personal information needs to be taken off our premises, staff must ensure it is appropriately secured. Where possible we will implement multi-factor authentication and strong passwords to access school computers, laptops, and other devices. Staff are reminded not to reuse passwords from other sites. We use encryption software to protect all portable devices and removable media, such as laptops and USB drives. Staff who store personal information on their personal devices must follow the same security rules as those for company equipment (see our online safety policy / ICT & internet acceptable use / ICT & communications policy). When we need to share personal data with a third party, we check that they will store it securely and take steps to protect it (see section 8).

15. Disposal of records

We will securely dispose of personal data that is no longer needed. Personal data that is inaccurate or out of date will also be safely disposed of if it cannot be corrected or updated. For example, we will shred paper records and overwrite or delete electronic files. We may hire a third party to help dispose of records safely for the company. If we do this, we will ensure that the third party guarantees they follow data protection laws.

16. Personal data breaches

The company will do everything reasonable to prevent personal data breaches. If we suspect a data breach, we will follow the steps outlined in appendix 1. If we assess the breach to meet the threshold for reporting, we will report the breach to the Information Commissioner's Office (ICO) within 72 hours of finding out about it.

Examples of breaches in a business setting may include but are not limited to:

- A dataset that is not anonymous being posted on the company website,
- showing the exam results of students eligible for pupil premium
- The theft of a company laptop that has unencrypted personal data.

17. Training

All new staff are provided with data protection training as part of their induction process. In line with the ICO recommendation, refresher training will be provided to all staff regularly and not less than every 2 years , forming part of continuing professional development.

The Directors will take strategic responsibility to ensure that they have a good understanding of their duties and obligations.

18. Making and Handling Complaints about Personal Data

In accordance with Section 164a of the Data (Use and Access) Act 2025 organisations are now required to include information on how to raise a complaint relating to data protection – see below.

How to Make a Data Protection Complaint

- **Your Right to Complain**
  You have the right to make a complaint if you believe school have handled your personal data in a way that breaches the UK GDPR or Part 3 of the Data Protection Act.
- **How to Make a Complaint**
  A complaint can be made using the template form in Appendix 2. Once complete, this should be submitted to (ian@ianstokes.org)
- **Acknowledging a Complaint**
  The company will acknowledge receipt of a complaint within **30 days**.
- **Responding to a Complaint**
  Complaints will be investigated as quickly as possible and without undue delay, this will include taking the necessary steps to investigate and deal with any concerns.
- **Keeping You Informed**
  As part of handling your complaint, we may make enquiries to better understand what has happened and keep you updated on the progress of our investigation. Once complete, you will be informed of the outcome.
- **Escalation to the ICO**
  If a complaint is not resolved by the DPO, the data subject can escalate it to the Information Commissioner for further investigation.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and not less than every two years in accordance with the recommendations for statutory policies and will be presented to Directors for approval.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the data protection lead person in the school/organisation, who will contact the DPO.

1. The DPO will assist in the investigation of 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
2. The DPO will determine whether to alert the Directors.
3. The DPO will assist in making all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
4. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
5. The DPO will determine whether the breach meets the threshold to be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms using the ICO's self-assessment tool.
6. The DPO will ensure that the decision is documented (either way); in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the company's computer system, or on a designated software solution.
7. Where the ICO must be notified, the DPO will do this by telephone or via the 'report a breach' page of the ICO website within 72 hours. 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
8. If all the above details are not yet known, the DPO will report as much as they can within 72 hours. 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
9. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact and ensure that any decision on whether to contact individuals is documented. If the risk is high, the DPO, or data protection lead will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out in plain language:
    - 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

10. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
11. The data protection lead person, with advice and/or support from 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 on the company's computer system, or on a designated software solution.

- In the case of a significant breach, the DPO & Directors will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, 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 data protection lead person as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the data protection lead will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the data protection lead will 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.
- Written confirmation that the email has been deleted will be requested from all the individuals who received the data, confirming that they have complied with this request
- In the case of a serious breach, we will arrange for an internet search to be conducted 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

Other types of breach that you might want to consider could include:

- Non-anonymised pupil exam results or staff pay information being shared
- A company laptop containing non-encrypted sensitive personal data being stolen or hacked

Appendix 2: Complaints Form

Data Protection Complaint Form

Your Details

Name:

_____

Email:

_____

Phone:

_____

Date of Incident: _____

Type of Issue

☐ Unauthorised access
☐ Data loss/theft
☐ Improper sharing
☐ Consent issue
☐ Other: _____

Declaration:

Summary of Incident

I confirm this information is accurate

Signature: _____ Date: _____

Submit this form to ian@ianstokes.org who will acknowledge receipt of the complaint within the period of 30 days from when the complaint is received.