General Data Protection (GDPR) Policy

Document number:	*11*
School:	*All Schools*
Issue:	*5-1*
Owner:	*The Data Protection Officer*
Approved by:	*The Executive Board*
Effective date:	*23/09/2026*
Next review due by:	*25/03/2027*

1. Summary

We are committed to engendering a culture of accountability, integrity and confidentiality in all aspects of the organisation in regard to personal data and security. All persons who process personal data with our permission must endorse and adhere to these principles at all times and especially when they obtain, handle, process, transfer, store or erase personal data:

- Fairness, lawfulness and transparency
- Purpose limitation
- Minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

The data controller is ultimately accountable for each of these principles and is obliged by law to be able to demonstrate compliance at all times. It is for this reason that everyone in the organisation is required to take responsibility for their own strict adherence to these principles.

This policy is not contractual as it may be subject to change.

2. Document Release

This document has been reviewed in accordance with the Educ8 Quality System and the requirements of this policy. Staff have been made aware of its issue, including any updates/amendments to its contents and where necessary appropriate training has been provided to those staff.

Where policies are available for download online, the previous version is removed and this new version replaces it.

The release of this document is indicated by the effective date.

This policy will be reviewed annually and approved by the Executive Board before release.

3. Purpose & Scope

We collect, store and process personal data (also referred to as personal information) relating to job applicants and about current and former employees, temporary and agency workers, contractors, interns, and volunteers for a number of specific lawful purposes, whilst carrying out our business activities.

This document is necessary to help ensure compliance with our legal obligations in respect of data processing and seeks to protect personal information relating to our workforce.

It is also intended to be a key tool toward demonstrating compliance measures to regulators and may be regarded by them as a top layer document and therefore

comprises part of our layered approach to documenting practices in this area. As well as ensuring our staff understand and comply with the rules regarding the collection, use and deletion of personal information for which they may have access to, through the course of their work.

Through this policy and other practices, the organisation aims to create and operate a culture of openness in respect of data processing.

Our Data Protection Officer is responsible for data protection compliance within the company. Should you have any questions or comments about this policy, or if you need further information you should contact **Tim Warner, tim.warner@educ8group.com 07817 641240**. More information about the role of the Data Protection Officer can be found in section 'Roles and Responsibilities'.

As a UK established organisation, this policy applies to all processing of personal data regardless of where in the world that processing, or any processing outsourced by us may take place.

This is an internal policy and it applies to the personal information of all job applicants, current and former employees, agency and temporary workers, contractors, interns, volunteers and any other internal persons for whom we collect, store and process personal information.

The document may be shared with third parties, contractors and other self-employed persons who will be asked to comply with the policy. Where the organisation does undertake the services of a third party, that party will be required to make adequate assurances to the data controller and/or processor that their own processing is compliant with current applicable data protection laws.

The policy applies to all data processes in general but particularly to all activities relating to the acquisition, recording, processing, sharing, storing and removal of personal data. In respect of carrying out general business activities and for illustrative purposes only, such processes include but are not limited to: recruitment activities, the collection of marketing data, student records, recording of attendance and qualification outcomes data etc.

Information that is already in the public domain is exempt from the Data Protection Act. This would include for example, information contained within externally circulated publications such as brochures and other sales and marketing literature or included on our website.

Any individual who has good reason for wishing their details not to be included in such publications should contact the DPO.

4. Policy

The Nominated Officer for Data Protection is: Tim Warner.

4.1 Statement

We are committed to engendering a culture of accountability, integrity and confidentiality in all aspects of the organisation in regard to personal data and

security. Our ultimate aim is to align every member of staff to these values such that they may be ambassadors of best practice data processing. We seek to achieve this by inducting new starters into our security practices and to maintain engagement and commitment to these values through transparent communication, providing regular training to staff and embedding privacy into our practices.

As an employer we process a significant amount of personal data about our staff. The type of information we require includes: nationality, date of birth, contact details and medical information. The grounds upon which this information is required will include legal and contractual obligations such as; demonstrating right to work checks, meeting statutory payment conditions and corresponding with individuals in respect of their employment.

Please refer to the section 'Roles and responsibilities' for the details of the Controller. For a list of your rights as a data subject, please refer to section 'The rights of data subjects'.

4.2 Training

We will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

4.3 Principles

All persons who process personal data with our permission must endorse and adhere to these principles at all times and especially when they obtain, handle, process, transfer, store or erase personal data.
The six fundamental principles of personal data processing are as follows:

Fairness, lawfulness and transparency
All personal data must be processed fairly, lawfully and transparently.

Purpose limitation
All personal data must be collected for specified, explicit and legitimate purposes and shall not be further processed in any manner that is incompatible with those purposes.

Minimisation
All personal data must be adequate, relevant and limited to what is necessary for the purpose for which they are processed.

Accuracy
All personal data must be accurate and where necessary, kept up to date with regards to the purposes. Every reasonable step to rectify or erase inaccurate personal data must be taken without delay.

Storage limitation
No personal data should ever be kept in a form which permits identification of a data subject for longer than is necessary to achieve the purpose.

Integrity and confidentiality
All personal data must be processed in a manner that ensures appropriate security of the personal data. At the very least, it must always be protected against unauthorised or unlawful processing, accidental loss, destruction or damage, by using appropriate technical and organisational measures.

The data controller is ultimately accountable for each of these principles and is obliged by law to be able to demonstrate compliance at all times. It is for this reason that everyone in the organisation is required to take responsibility for their own strict adherence to these principles.

This policy is not contractual as it may be subject to change. However, it does indicate how we intend to meet our legal responsibilities for data protection. Therefore, any actionable points within it must be regarded as a legitimate management instruction. Explicit permission must always be sought and evidenced from a line manager before conducting yourself in a manner that varies from this policy. Failure to do so may result in disciplinary action.

We will review and update this policy in accordance with our data protection obligations. It does not form part of an employee's contract of employment, and we reserve the right to amend, update or supplement it from time to time. We will communicate any new or modified policy to employees before it is implemented. We will notify data subjects of any changes that apply to them where appropriate, personally and in writing.

4.4 In the context of safeguarding and child protection

Educ8 recognises that effective information sharing is essential for safeguarding and promoting the welfare of children.

Personal data may be processed and shared for safeguarding and child protection purposes where there is an appropriate lawful basis under UK GDPR and the Data Protection Act 2018. Depending on the circumstances, this may include legal obligation or public task and, where special category data is involved, an appropriate additional condition such as substantial public interest.

From **30 September 2026**, Educ8 will comply with the statutory **Information Sharing Duty under section 16LA of the Children Act 2004** where the duty applies.

Data protection legislation does not prevent lawful and necessary information sharing for safeguarding and welfare purposes. **Consent is not a prerequisite where another lawful basis for sharing applies.**

Staff must not allow uncertainty about data protection, confidentiality or consent to delay or prevent necessary safeguarding action.

Safeguarding information must be shared in accordance with Educ8's **Safeguarding and Child Protection Policy** and **Information Sharing Policy**, having regard to current statutory safeguarding and information-sharing guidance.

We will, through appropriate management arrangements, procedures and controls:

- ensure personal information is collected, processed and shared fairly and lawfully;
- clearly identify the purpose for which personal information is processed;
- collect, process and share only information that is relevant and necessary for the identified purpose;
- take reasonable steps to ensure information is accurate and, where appropriate, kept up to date;
- retain personal information only for as long as is necessary in accordance with Educ8's retention requirements;
- safeguard personal information through appropriate physical, technical and organisational security measures;
- ensure staff who manage or handle personal information understand their responsibilities and receive appropriate training and supervision;
- maintain appropriate procedures for responding to requests for information and data subject rights;
- regularly review and evaluate arrangements for handling personal information;
- use **written data-sharing agreements where appropriate for regular, systematic or ongoing information-sharing arrangements**;
- recognise that the absence of a written data-sharing agreement must **not delay or prevent lawful and necessary safeguarding information sharing**;
- ensure safeguarding information is shared securely and only with appropriate recipients;
- ensure significant safeguarding information-sharing decisions are appropriately recorded, including the rationale for decisions **to share or not to share**; and
- ensure any disclosure of personal data follows Educ8's approved safeguarding, information-sharing and data-protection procedures.

4.5 Roles & Responsibilities

Data Controller

The Company's Data Controller is Tim Warner. Tim can be directly contacted by email at tim.warner@educ8group.com or by telephone on 07817 641240.

The Role:

The Data Controller is the key decision maker in respect of why and how personal data is used and handled. The Data Controller will ensure that, both in the planning and implementation phases of processing activities, data protection principles and appropriate safeguards are addressed and implemented and that records of processing activity are kept.

Overview of Responsibilities:

- To be ultimately accountable for the Company's compliance with the six principles (see section 'Principles').
- To be able to demonstrate compliance with the six principles and therefore the proper handling and processing of all personal data. This will include information about the various data protection management resources that have been put into place and take the primary responsibility for the internal data protection framework.
- To implement appropriate technical and organisational measures to ensure processing is performed in accordance with data protection laws. These measures will take into account the nature, scope, context and purposes of the data processing and the risks to the rights and freedoms of individuals.
- To adopt measures to protect against any high levels of risk identified by a Privacy Impact Assessment, such as; discrimination, identity theft or significant legal, social or economic disadvantage.
- To implement internal data protection policies; assign protection responsibilities and to ensure adequate training on data protection is provided and carried out by all staff.
- To ensure that any international transfer of personal data complies with the requirements of UK GDPR and applicable UK data protection legislation.
- To ensure that personal data breaches are assessed and, where required by data protection legislation, reported to the Information Commissioner's Office (ICO) and communicated to affected data subjects within the applicable statutory timescales.
- To determine how and ensure that data subjects may exercise their rights regarding their personal data, including rights of access, rectification, erasure, restriction, data portability, objection and those related to automated decision making.
- To communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data has been disclosed unless this proves impossible or involves disproportionate effort.
- The controller shall inform the data subject about those recipients if the data subject requests it.

Data Processor

The role:

This role processes personal data on behalf of and further to documented instruction given by the Controller.

Overview of Responsibilities:

- To only process personal data as instructed by the Data Controller (unless otherwise required by law).
- To take all measures required to ensure their own compliance with data protection legislation regarding security.
- To make available all information necessary to demonstrate compliance with data protection legislation and to permit an audit should the Controller wish to further ensure compliance.

To assist the controller in compliance with its obligations under data protection legislation regarding;

- security of processing
- assist in meeting any rights exercised by a data subject e.g. subject access request
- notification of a personal data breach to the supervisory authority
- communication of a personal data breach to the data subject
- any necessary Data Protection Impact Assessments
- consultation with the supervisory authority about any processing that should be identified as being ‘high risk’

To ensure that on instruction from the Controller, any personal data held on behalf of a client for whom we act as a processor, is deleted and returned to that client, unless we are prohibited by data protection legislation.

To ensure data transfers outside of the UK are authorised by the Data Controller and complies with the UK GDPR transfer provisions.

To immediately inform the Controller if it believes any instruction given by the Controller would be in breach of data protection legislation.

Any processors are not permitted to appoint another processor without prior written agreement from the Company. Equally when we act as a processor we will not appoint another processor without written agreement of the Controller we act on behalf of.

4.6 Conditions for processing data

Under data protection legislation, personal data must only be processed where an appropriate lawful basis applies. There are six lawful bases for processing personal data under UK GDPR.

There are six potential legal bases for processing.

In relation to any processing activity, we will, before the processing starts for the first time, and then regularly whilst it continues, review the purposes of the processing activity, and select the most appropriate lawful basis (or bases) for the processing.

Except for when the processing is on the lawful basis of consent, we will satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose).

We shall document our decision as to which lawful basis applies so that we can demonstrate our compliance with the data protection principles.

Information about the purposes of the processing and the lawful basis for it, will be included in our relevant privacy notice(s).

In the processing of sensitive personal information and criminal offence information, we shall identify a lawful special condition for processing that information and document that condition.

All persons authorising the processing of personal data must be assured that at

least one of the following bases applies:

Legal bases for personal data processing:

Consent
The data subject must have given consent for specific purposes and be given the option to withdraw consent at any time. Lawful consent may only be obtained if prescribed conditions set out by data protection laws have been met. Consent must always be explicit and may not be implied.

Contract
The processing must be necessary to enter into or adhere to a contract which the data subject is party to. For example, to enter into a contract of employment or when a product or service is purchased by the data subject and personal data is required to provide or perform it.

Legal Obligation
The processing must be necessary to comply with a legal obligation that you are bound to. For example, tax obligations, evidencing the right to work or to ensure compliance with the Working Time Directive etc.
A legal obligation relied upon for this lawful basis must arise under UK law or applicable law recognised for this purpose under UK data protection legislation.

Vital interests
The processing is necessary to protect vital interests of the data subject. For example, subjects who are unable to make decisions in the best interests of their health.

Public Task
The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This must be sufficient to reasonably override the interests and rights of the data subjects concerned. It may be used for the defence of a legal claim.

Legitimate interest
The processing must be necessary to pursue a legitimate interest, except where it is overridden by fundamental rights and freedoms of the data subject. (This is not applicable to public authorities.) When a legitimate interest is determined as a lawful basis for processing data, a record of the decision will be held and will be subject to regular review.

4.7 Special category data

Special category personal data requires additional protection under UK GDPR and the Data Protection Act 2018.

Educ8 will only process special category personal data where an appropriate lawful basis under Article 6 UK GDPR applies and an additional condition for processing under Article 9 UK GDPR is met. Where required, an appropriate condition under the Data Protection Act 2018 will also be identified.

Special category data may include information revealing racial or ethnic origin,

political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data used for identification, health information, or information concerning a person's sex life or sexual orientation.

Where special category information is processed for **safeguarding or child protection purposes**, this may include processing that is necessary for reasons of substantial public interest. Consent is not a prerequisite where another appropriate lawful basis and condition for processing applies.

Appropriate safeguards must be applied to the collection, access, use, storage and sharing of special category data.

Conditions under which special category data may be processed are:

The data subject has given explicit consent to the processing of personal data for one or more specified purposes, and there is no overriding legal prohibition.

Processing is necessary to carry out obligations and specific rights of the controller or of the data subject in the field of employment, social security and social protection law. Appropriate safeguards are imperative.

Processing is necessary to protect the vital interests of the data subject or of another person who is physically or legally incapable of giving consent. For example, in a medical emergency.

Processing relates to personal data which are obviously made public by the data subject.

Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts make instructions to the Company when acting in their judicial capacity.

Processing is necessary for reasons of substantial public interest, on the basis of UK law, and the relevant requirements and safeguards under the Data Protection Act 2018 are met.

4.8 Criminal convictions and offences

Personal data relating to criminal convictions and offences requires additional protection under UK GDPR and the Data Protection Act 2018.

Educ8 will only process criminal offence data where there is an appropriate lawful basis and the relevant requirements of the Data Protection Act 2018 are met.

Criminal offence data may be processed where necessary in connection with:

- safer recruitment and employment checks, including DBS requirements;
- safeguarding and child protection;
- allegations or concerns relating to adults working with children;
- child-on-child abuse or harmful behaviour;
- police, youth justice or other statutory agency involvement;
- the prevention or detection of crime; or
- other legal, regulatory or safeguarding responsibilities.

Where criminal offence information is processed for safeguarding purposes,

consent is not a prerequisite where another appropriate lawful basis and condition for processing applies.

Access to criminal offence data must be restricted to those with an appropriate need to know. Information must be stored, accessed and shared securely and only to the extent necessary and proportionate for the identified purpose.

4.9 Processing which does not require identification

Where personal data can be fully anonymised so that an individual is no longer identifiable, either directly or indirectly, the information will no longer constitute personal data for the purposes of UK GDPR.

Where information is **pseudonymised**, or where an individual could still be identified using other information reasonably available, the information remains personal data and must continue to be processed in accordance with this policy and applicable data protection legislation.

Staff must ensure that information is genuinely anonymised before treating it as information to which UK GDPR no longer applies.

4.10 Safeguarding records

Safeguarding and child protection records must be maintained securely, accurately and in accordance with current statutory guidance, data protection legislation and Educ8's Records Retention Policy.

Child protection files will normally be retained **until the child's 25th birthday**. Where a child protection file relates to **child sexual abuse, records will be retained until the child's 75th birthday**, in accordance with current Department for Education record-keeping guidance.

Records may be retained for longer where there is a lawful and documented reason to do so, including where records are subject to an ongoing investigation, inquiry, litigation, legal hold or other statutory requirement.

Where a child transfers to another education setting, the child protection file must be transferred securely and separately from the main pupil file in accordance with Keeping Children Safe in Education and Educ8's Safeguarding and Child Protection Policy and Information Sharing Policy.

Safeguarding records must be disposed of securely when the applicable retention period has expired and there is no continuing lawful reason for retention.

4.11 Collecting data

Transparency principle

Educ8 will ensure that information provided to data subjects about the collection and processing of their personal data is **concise, transparent, intelligible,**

easily accessible and written in clear and plain language.

Information provided to the Information Commissioner's Office or another relevant supervisory authority will also be clear, accurate and provided in accordance with applicable data protection requirements.

4.12 Collecting personal data from the subject

Where Educ8 collects personal data directly from an individual, the individual must be provided with appropriate privacy information, including:

- the identity and contact details of the Data Controller and, where applicable, the Data Protection Officer;
- the purposes for which the personal data will be processed;
- the lawful basis for the processing;
- where legitimate interests are relied upon, details of those legitimate interests;
- the recipients or categories of recipients of the personal data, where applicable;
- details of any intended international transfer of personal data and the appropriate safeguards or other lawful transfer mechanism relied upon, where applicable;
- the period for which the personal data will be retained, or the criteria used to determine that period;
- information about the individual's applicable data protection rights;
- the right to lodge a complaint with the Information Commissioner's Office (ICO);
- whether the provision of personal data is a statutory or contractual requirement and, where appropriate, the possible consequences of failing to provide it; and
- the existence of any automated decision-making, including profiling, where applicable.

This information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

4.13 Collecting personal data from a source other than the subject

Where Educ8 obtains personal data about an individual from a source other than the individual, appropriate privacy information must normally be provided to them.

In addition to the information set out in section 4.12, this should include:

- the categories of personal data obtained;
- the source from which the personal data originated; and
- where applicable, whether the information came from a publicly accessible source.

The information must normally be provided:

- within a reasonable period after obtaining the personal data and no later

than one month;
- at the time of the first communication with the individual, where the information is to be used to communicate with them; or
- before or at the time of the first disclosure to another recipient, where the information is to be disclosed.

There may be circumstances where data protection legislation permits information not to be provided, including where providing it would be impossible, involve disproportionate effort, or where another applicable statutory exemption applies.

In a safeguarding or child protection context, staff must not provide information to a child, parent/carer or other individual where doing so could place a child or another person at risk, prejudice safeguarding activity or an investigation, or where another lawful restriction or exemption applies. Advice should be sought from the DSL and/or Data Protection Officer where necessary.

4.14 Privacy and fair processing notices

Educ8 will maintain appropriate privacy notices to explain how and why personal data is collected, used, stored and shared.

Privacy notices will:

- identify the purposes for which personal data is processed and the applicable lawful bases;
- identify relevant categories of recipients with whom information may be shared;
- explain applicable retention arrangements and data subject rights;
- provide details of the Data Protection Officer and the right to complain to the Information Commissioner's Office (ICO);
- provide information about international transfers where applicable; and
- be reviewed and updated where legislation, statutory guidance or Educ8's processing activities materially change.

Privacy information will be provided at the appropriate time and in a concise, transparent, intelligible and easily accessible form using clear and plain language.

Where personal data is processed or shared for safeguarding and child protection purposes, relevant privacy information will reflect that such information may be shared without consent where there is another appropriate lawful basis and where sharing is necessary for safeguarding or promoting the welfare of a child.

Privacy notices must not prevent, delay or restrict lawful and necessary safeguarding information sharing

4.15 The purpose changes

Where Educ8 proposes to process personal data for a purpose other than that for which it was originally collected, the compatibility and lawfulness of the new

purpose must be considered before the further processing takes place.

Where required, the data subject will be informed of:

- the new purpose for processing;
- the applicable lawful basis;
- any relevant changes to how their personal data will be used or shared; and
- any other information necessary to ensure the processing remains fair and transparent.

Where the further processing is required or permitted by law, including for safeguarding or child protection purposes, Educ8 will process and share the information in accordance with the applicable legal requirements and Educ8's safeguarding, information-sharing and data-protection procedures.

4.16 Multiple controllers

Where Educ8 acts jointly with another organisation in determining the purposes and means of processing personal data, the respective data protection responsibilities of each organisation will be clearly identified and documented as required by data protection legislation.

Where Educ8 regularly or systematically shares personal data with another organisation, appropriate information-sharing or data-sharing arrangements will be established where required or appropriate. These arrangements should clearly identify:

- the purpose of the information sharing;
- the respective roles and responsibilities of the organisations involved;
- the lawful basis for processing and sharing;
- the information that may be shared;
- appropriate security and information-sharing routes;
- relevant retention and disposal arrangements; and
- appropriate points of contact.

This may include arrangements with **commissioning organisations, alternative provision providers, local authorities and other education, safeguarding or welfare partners**, where applicable.

The absence of a formal data-sharing agreement must **not delay or prevent lawful and necessary safeguarding information sharing**.

Where safeguarding information is shared, Educ8's Safeguarding and Child Protection Policy and Information Sharing Policy must also be followed.

4.17 Employee Records

We hold personal information about all employees as part of our general employee records. This includes address and contact details, age, date of birth, marital status or civil partnership, educational background, employment

application, areas of expertise, details of salary and benefits, bank details, performance appraisals and salary reviews, records relating to holiday, sickness, and other leave, working time records and other management records. We may receive and/or retain this information in various forms (whether in writing, electronically, verbally, or otherwise).

This information is used for a variety of administration and management purposes, including payroll and benefits administration, facilitating the management of work and employees, performance, and salary reviews, complying with record keeping and other legal obligations.

We also process information relating to employees' health, some of which may fall under the definition of 'sensitive personal data'. This typically includes pre-employment health questionnaires; records of sickness absence and medical certificates (including self-certification of absence forms) night worker assessments; VDU assessments; noise assessments and any other medical reports. This information is used to administer any contractual and Statutory Sick Pay, monitor, and manage sickness absence and to comply with our obligations under health and safety legislation and the Working Time Regulations.

From time to time, we may ask employees to review and update the personal information we hold about them and will at least annually ask them to update their basic personal data. However, we ask that employees do not wait until asked to update this information but inform us immediately of any significant change(s).

4.18 Health and criminal records

Educ8 will only collect or process health information and criminal offence data where there is a lawful and necessary reason to do so.

This may include processing required for:

- safer recruitment and DBS checks;
- safeguarding and child protection responsibilities;
- occupational health and fitness for work;
- sickness absence and statutory employment requirements;
- health and safety responsibilities;
- reasonable adjustments and support; or
- other legal or regulatory obligations.

Where such information is required, Educ8 will identify the appropriate lawful basis and, where applicable, the relevant additional condition for processing special category or criminal offence data.

Information will only be collected to the extent necessary for the identified purpose and will be stored, accessed and shared securely with appropriately authorised persons.

4.19 Privacy by design and by default

The Company embeds data protection into the design of every system that uses personal data, so that it is protected throughout its entire lifecycle. To maintain this principle, all members of staff are required to:

- Ensure personal data is mapped, classified into either personal or special category data, labelled, stored and accessible so that it is easily found if need be (eg in the event of a subject access request, the need to remove the data or the need to update the data).
- Ensure our systems continue to function so that any personal data that is added may be deleted automatically (where appropriate).
- Ensure that any new documentation which collects personal data is drafted in such a way that no personal data is requested in excess of what is necessary to achieve the purpose.
- Ensure that a data subject is only identified for as long as necessary. This may include removing an identifier such as a name or date of birth.
- Ensure that any new system will process data in a format that is commonly used.

4.20 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) has been carried out in respect of processing that is considered likely to put the rights and freedoms of data subjects at a high risk.

A Data Protection Impact Assessment must always be completed if the processing of personal data is likely to be high in risk to the rights and freedoms of the data subject. Examples of processing that may be high risk include systematic monitoring of publicly accessible information on a large scale, or profiling that may significantly affect individuals.

Before any new technology or working practice is introduced, the manager responsible should contact the Data Protection Officer in order that a DPIA can be carried out.

4.21 Information Security

As a company we regularly review our approach to information security and stay up to date with developments in the field and emerging threats. To secure the information we hold we are committed to allocating sufficient resources (including time and budget) to ensure that robust and high-quality tools and processes are implemented.

The Company takes all reasonable steps to protect and maintain the integrity, confidentiality and availability of personal data. For the purposes of this policy, organisational and technological security measures are in place to protect and secure against: accidental loss, damage, destruction, theft or unsanctioned disclosure, publication or transfer of personal data.

Protection: All members of staff and any associated third parties are made aware of their responsibilities and are required to exercise and uphold every applicable security measure.

Integrity: All members of staff and any associated third parties are made aware of their responsibilities and are required to securely update and maintain completeness of personal data.

Confidentiality: All members of staff and any associated third parties are made aware of their responsibilities and are required to only access personal data which they are authorised to process. Those with authority to process personal data will only make personal data available to recipients (other colleagues, third parties etc) if those recipients are authorised to access or process the data.

Availability: **Availability:** The Company has taken measures to prevent accidental and deliberate unauthorised access. **This includes appropriate disaster recovery and business continuity arrangements.** All members of staff, agency workers and any associated third parties are made aware of their responsibilities and are required to maintain the measures put in place by the Company to physically and virtually secure information. If they detect any threats to the continued availability of access to assets, systems and information, they must report this to a line manager so that it may be escalated appropriately. Threats may include damage to a computer filing system, faulty locks, viruses or malware.

We will also ensure that, where possible, personal information is pseudonymised or encrypted and that company processes and technical and organisational measures are regularly tested, assessed and evaluated for their effectiveness in ensuring the security of processing.

This section is applicable to self-employed persons and contractors insofar as they are required to comply with these requirements and Educ8's security measures. They must uphold their obligations under applicable data protection legislation. Failure to do so may result in termination of the service agreement and, where required, the incident may be reported to the relevant supervisory authority.

4.22 External Organisations

Where we use external organisations to process personal information on our behalf, we will implement additional security arrangements in contracts with those organisations to safeguard the security of personal information. We will ensure contracts with external organisations will provide:

- the organisation may act only on our written instructions;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with our prior consent and under a written contract;
- the organisation will assist us in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- the organisation will assist us in meeting our obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the organisation will delete or return all personal information to us as requested at the end of the contract; and
- the organisation will submit to audits and inspections, provide us with whatever information we need to ensure that we are both meeting our data protection obligations, and tell us immediately if it is asked to do something

infringing data protection law.
- Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the DPO

4.23 Transferring personal data to a country outside the EEA

Educ8 will ensure that any international transfer of personal data complies with UK GDPR and applicable UK data protection legislation.

Before making a restricted transfer of personal data to a separate organisation outside the UK, Educ8 will ensure that an appropriate lawful transfer mechanism is in place. This may include:

- UK adequacy regulations;
- appropriate safeguards in accordance with UK GDPR; or
- an applicable exception where permitted by data protection legislation.

Where appropriate safeguards are relied upon, Educ8 will complete any required transfer risk assessment/data protection test and implement any additional technical, organisational or contractual protections identified as necessary.

Staff must not transfer, store or make personal data accessible outside the UK through unapproved systems, applications or services without appropriate authorisation and, where necessary, advice from the Data Protection Officer.

Relevant privacy information and records of processing will be updated where required to reflect international transfers.

4.24 Record Keeping

Educ8 will maintain appropriate records of its personal data processing activities in accordance with UK GDPR and applicable data protection legislation.

These records will include, where applicable:

- the purposes of processing;
- categories of data subjects and personal data;
- categories of recipients to whom personal data is disclosed;
- details of international transfers where applicable;
- applicable retention periods; and
- a general description of the technical and organisational security measures in place.

Safeguarding and Information-Sharing Records

Significant safeguarding information-sharing decisions must be appropriately recorded on CPOMS or within the relevant safeguarding record.

The record should include, where applicable:

- what information was considered and/or shared;
- who the information was shared with;
- the date of the sharing;
- the purpose and reason for sharing;
- the rationale for the decision, including the lawful basis where relevant;
- any actions or outcomes arising from the information sharing; and
- confirmation of receipt where this is necessary or appropriate.

Where a decision is made not to share safeguarding information, the decision and the rationale for not sharing must also be recorded.

Records must provide a sufficient audit trail to demonstrate how significant information-sharing decisions were made.

Recording requirements must not delay urgent safeguarding action. Where information has to be shared immediately to protect a child or another person, the decision and rationale must be recorded as soon as reasonably practicable afterwards.

Further requirements are set out in Educ8's Safeguarding and Child Protection Policy and Information Sharing Policy.

4.25 Breach and Incident Reporting

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.

All actual or suspected personal data breaches must be reported **immediately to the Data Protection Officer (DPO)** in accordance with Educ8's data breach procedures.

The DPO will ensure that the breach is appropriately investigated, contained and assessed, including consideration of the likelihood and severity of any risk to the rights and freedoms of individuals.

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, Educ8 will notify the **Information Commissioner's Office (ICO)** without undue delay and, where feasible, no later than **72 hours after becoming aware of the breach**.

Where a breach is likely to result in a **high risk** to the rights and freedoms of affected individuals, Educ8 will also inform those individuals without undue delay, unless an applicable exception applies.

Educ8 will maintain a record of all personal data breaches, whether or not they are reported to the ICO. The record will include the nature and circumstances of the breach, its effects, the risk assessment undertaken, action taken to contain or mitigate the breach and the rationale for any decision to report or not to report it.

Where a breach involves safeguarding or child protection information, the DPO and DSL will work together to ensure that the response appropriately addresses

both data protection and safeguarding risks. Action necessary to protect a child or another person must not be delayed while the data breach assessment is undertaken.

4.26 School Processing of Personal Data

Educ8 processes personal data relating to pupils, parents/carers, staff and other individuals where this is necessary for the operation of its schools and provisions and to meet its legal, regulatory, safeguarding and educational responsibilities.

This may include personal data processed in connection with safeguarding and child protection, low-level concerns, allegations relating to adults working with children, whistleblowing, attendance, behaviour, SEND, safer recruitment and other statutory or operational responsibilities.

Personal data will only be processed where an appropriate lawful basis applies. Where special category data or criminal offence data is processed, the additional requirements set out elsewhere in this policy will also apply.

Individuals have rights under UK GDPR in relation to their personal data, which may include:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights relating to automated decision-making and profiling.

These rights are **not absolute** and may be subject to conditions, limitations or exemptions under data protection legislation.

In particular, safeguarding, child protection, low-level concern, allegation or other records will not be erased, restricted or disclosed where doing so would conflict with a legal or regulatory requirement, prejudice safeguarding activity or an investigation, or otherwise fall within an applicable exemption.

Requests to exercise data protection rights will be handled in accordance with Educ8's procedures and, where appropriate, referred to the Data Protection Officer.

4.27 Fulfilling a SAR

Individuals have the right to request access to personal data that Educ8 holds about them. A Subject Access Request (SAR) may be made verbally or in writing and does not need to refer specifically to data protection legislation to be valid.

All SARs must be forwarded promptly to the Data Protection Officer (DPO) so that

they can be recorded and managed within the statutory timescale.

Educ8 will respond to a valid SAR without undue delay and normally within **one month**, in accordance with applicable data protection legislation.

Where necessary, Educ8 may extend the response period by up to a further **two months** where the request is complex or the individual has made a number of requests. The individual will be informed of the extension and the reasons for it within the applicable initial response period.

Where Educ8 reasonably requires clarification about the information requested in order to respond effectively to a SAR, clarification may be sought from the individual. Where permitted by data protection legislation, the response period may be paused until the necessary clarification is received.

Educ8 may request reasonable and proportionate evidence to verify the identity of the person making the request or, where a request is made on behalf of another individual, evidence of their authority to act. The statutory response period will be calculated in accordance with applicable data protection legislation once any necessary information has been received.

Educ8 will undertake a **reasonable and proportionate search** for personal data falling within the scope of the request.

Information relating to other individuals will be considered carefully before disclosure and will be redacted or withheld where required or permitted by data protection legislation.

Particular care will be taken where a SAR involves **safeguarding, child protection, allegations, low-level concerns or other sensitive information**. Information will not be disclosed where an applicable exemption or restriction permits or requires it to be withheld, including where disclosure could prejudice safeguarding activity or adversely affect the rights and freedoms of another person.

In most circumstances, Educ8 will not charge a fee for responding to a SAR. A reasonable fee may be charged where permitted by data protection legislation, including where a request is manifestly unfounded or excessive or where further copies of information are requested.

Where Educ8 refuses to act on a request, or relies upon an applicable exemption or restriction, the decision and rationale will be documented and the individual will be provided with the information required by data protection legislation, including information about their right to complain to the **Information Commissioner's Office (ICO)**.

Information provided in response to a SAR will be supplied securely and in a clear and accessible format.

Making a request

If you wish to make a subject access request to verify the lawfulness and accuracy of the personal data we hold about you, then you are encouraged to put your request in writing (letter or email) and submit it to ‘the Data Protection

Officer'.

Your request should be specific about the nature and the type of data you require. Every attempt will be made to comply with your request in a timely manner and without undue delay.

Upon receipt of the information you are encouraged to check the accuracy of the information and to advise the Company of any updates that may need to be made.

A fee will not be charged for an access request, except where a request is deemed to be 'manifestly excessive' or you have already been provided with the information.

Receiving a request

If you receive a request, you should pass it to 'the Data Protection Officer' immediately.

Requests must be acknowledged upon receipt.

Requests must be complied with in a timely manner and without undue delay. If it is anticipated that compliance with a request is not going to be immediate then the Controller should be notified and informed of the legitimate reasons for this. The information requested must be provided within one month of receipt of the request.

If an extension to the time-line is absolutely necessary under exceptional circumstances, then any extension must be agreed by the data subject and signed off by the Data Protection Officer within one month of the request. If an extension is agreed, then the information must be provided within a maximum of three months from the receipt of the request.

If a request is received electronically (eg via email) then the request must be responded to electronically.

The data must be provided in a common format (eg a paper file, a pdf document etc.).

Only personal data pertaining to the individual who made the request should be released.

If there is any doubt over the identity of the individual making the access request, then reasonable steps must be taken to verify their identity, before complying with the request.

When the personal data is provided, the individual must be informed of the right to lodge a complaint with the relevant supervisory authority and the existence of the right to objection, rectification, erasure and restriction of the data.

The data subject may be directed to the relevant privacy/fair processing notice which will provide advice on the conditions for processing.

If requested, the following information must be provided as part of the response:

- The purpose of the data
- The categories of data that which are held
- The recipients of the data (past, present and intended in the future)
- The criteria that determines how long the data is retained for
- The source of the data if not collected from the individual directly

4.28 The school's filtering and monitoring systems

The school's filtering and monitoring systems generate data such as online activity logs and safeguarding alerts. Personal data processed through filtering and monitoring systems will be processed in accordance with UK GDPR and the Data Protection Act 2018. Educ8 will identify and document the appropriate lawful basis for the processing and, where special category or criminal offence data is involved, any additional condition required by data protection legislation.

We recognise that there are different areas in the organisation where members of staff may be responsible for processing personal data in different ways. We also recognise that responsibilities and nuances in processing are likely to vary across specialisms and levels of seniority.

The Company will provide guidance to staff when processing personal data specific to their job. This information shall include:

- A description of the limitations which surround how personal data can be used.
- The steps that must be followed to ensure that personal data is maintained accurately.
- A comprehensive discussion of security obligations, including all reasonable steps that should be taken as a minimum to prevent unauthorised access or loss.
- A signpost to the Company's Information Security Policy.
- Confirmation of whether the transfer of personal data shall be permitted. Transfer of personal data is prohibited unless specific legitimate grounds have been established.
- Specific information regarding the way in which personal data should be handled when it is destroyed or deleted.

4.29 General responsibilities of management

All members of the senior management are responsible for championing and enforcing this policy to all other staff within the Company, whenever appropriate.

Particular roles within senior management are responsible for assessing the business risk arising as a result of processing personal data. These roles include:

- The Directors,
- Executive Board Members,
- Managers,
- Heads of Schools,
- Site Coordinators etc.

Those members of senior management identified above are required to work with the Company to develop procedures and controls to identify and address risks appropriately.

Responsibility will be allocated to individual roles for determining risk-based technical, physical and administrative safeguards including safeguards for equipment, facilities and locations where personal data is stored; establishing procedures and requirements for collecting, transporting, processing, storing, transferring (where appropriate) and destroying personal data.

These considerations must also be given when dealing with any third parties who may be authorised or obligated to process personal data on behalf of the Company.

4.30 Non-compliance

This policy along with associated documents, seeks to guide and instruct all members of staff on how they ensure compliance with data protection laws to which the Company is subject.

If a member of staff should fail to comply with applicable data protection laws, they may subject the Company and themselves as individuals to civil and criminal penalties. This is likely to jeopardise the reputation of the Company and as a result may impact on the operational and performance capabilities of the business.

As the ramifications of non-compliance are potentially severe, any failure to comply with this policy or reasonable instruction given in connection with the protection and security of personal data, may result in disciplinary action. Serious, deliberate or negligent transgressions may be regarded as gross misconduct and if substantiated, may result in summary dismissal (without notice).

4.31 Third parties, contractors and self-employed persons

If any self-employed person, contractor or third party is found to be failing to meet obligations with applicable data protection laws then notice may be served on the contract for service.

Serious, deliberate or negligent transgressions may permit the Company to terminate the contract for service with immediate effect. In this event, all reasonable steps will be taken to recover and protect the personal data concerned and the relevant supervisory authority will be notified. Where the rights and freedoms of data subjects are likely to be at risk, the data subjects will be notified without delay.

4.32 Further Information

Any queries or comments about this policy, or any concerns that the policy has not been followed, should be addressed to:

The Data Protection Officer,
Educ8 Group,
Mill House,
Nailstone Road,
Carlton
Warwickshire,
CV13 0DH

or by email to tim.warner@educ8group.com

5. Metrics

The following metrics are applicable to this procedure:

- Number of SARs
- Number of Data Breaches

6. Forms & Templates

There following form(s)/template(s) are required for this document:

- F0017DP Serious Breach Notification Form

Issue & Revision History

Issue	Description	Author	Effective Date
1.0	Initial Release	T. Warner	10/03/11
1.1	Annual Review	J. Payne	25/07/12
1.2	Annual Review	J. Payne	04/08/13
2.0	Annual Review – Policy update	T. Warner	02/09/14
2.1	Annual Review	T. Warner	30/09/15
2.2	Annual Review	T. Warner	30/09/16
2.3	Annual Review	D.Payne	30/09/17
3.0	Total re-write due to GDPR	T. Warner	25/05/18
3.1	Annual Review	T. Warner	30/05/19
3.2	Annual Review	T. Warner	12/06/20
4.0	Annual Review	T. Warner	18/06/21
4.1	Annual Review	T. Warner	01/09/22
4.2	Annual Review	T. Warner	01/09/23
4.3	Annual Review 5. Purpose - updated 6. Scope - addition of paragraphs 4 - 6 7 Definitions & Acronyms - personal data updated, data subject updated, Special category data (sensitive data) added, Data protection legislation added Addition of 8.2 Training 8.3 Principles - updated final paragraph Addition of 8.4 Handling of personal data 8.5.1 Addition of responsibilities 8.5.2 Addition of responsibilities 8.6 Additions of paragraphs 2-6, Legitimate interest updated, 8.6.1 Addition of paragraph 2 Addition of 8.7.7 Addition of 8.7.8 Addition of 8.9 Data Protection Impact Assessments Addition of 8.6.4 Retention and destruction 8.10 Updated Addition of 8.11 External Organisations Addition of 8.12 Transferring personal data to a country outside the EEA 8.14 addition of paragraph 2 8.15 Bullets updated 8.16 Updated 8.21 Address updated	T. Warner	26/08/24
4.4	Annual Review	T. Warner	26/08/25

	Summary updated Section 8.4 – Added clarification on the lawful basis under GDPR and its safeguarding context to align with Article 6. Section 8.6.4 – Referenced statutory guidance to justify the 25-year retention period for safeguarding records. Section 8.15 – Specified how low-level concerns are stored and differentiated from formal disciplinary records. Section 8.16 – Noted that SAR exemptions in safeguarding cases should be documented by DSL or DPO. Section 8.17 – Linked filtering and monitoring to DfE standards and relevant internal policies for clarity.		
5.0	Annual Review Comprehensive update reflecting UK GDPR and Data Protection Act 2018, strengthened safeguarding alignment (KCSIE 2026), clarified lawful bases, enhanced data subject rights procedures, and integrated supporting policies including SAR, breach reporting, retention, information sharing and CCTV.	T. Warner	25/03/26
5.1	Updated to reflect the statutory Information Sharing Duty under section 16LA of the Children Act 2004, effective from 30 September 2026. Strengthened requirements relating to safeguarding information sharing, recording decisions to share or not to share, data-sharing arrangements, privacy information and secure information handling. Updated UK GDPR terminology and international transfer requirements, strengthened data breach and subject access provisions, and removed outdated and duplicated content.	T. Warner	23/09/26