General Data Protection (GDPR) Policy

Document number:	*11*
School:	*All*
Issue:	*4.2*
Owner:	*Data Protection Officer*
Approved by:	*The Executive Board*
Effective date:	*01 September 23*
Next review due by:	*15 August 2024*

1. Contents

2. Issue and 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

3. 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.

4. Document Release

This document has been reviewed in accordance with the Educ8 Quality System and the requirements of this policy/procedure. 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.

5. Purpose

We collect, store and process information relating to individuals (personal data) whilst carrying out our business activities. This document is necessary to help ensure compliance with our legal obligations in respect of data processing.

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.

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

6. Scope

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 all employees, workers and any other internal persons who may have responsibility for or a vested interest in the operations of the organisation.

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.

7. Definitions and Acronyms

Personal Data	Any ‘data’ relating to a ‘data subject’ who can be directly or indirectly identified by reference to a piece of data. This includes a name, identification number, location data or online identifier. It may be an identifier that relates to physical, physiological, genetic, mental, economic, cultural or social identity. It may also apply to data that has been pseudonymised. The nature of the definition of data and personal data means that the expression of opinion or view about a data subject may also be regarded as personal data.
Data Controller	Any person or organisation that uses personal information is known as a data controller.
ICO	Information Commissioners Office
Data	Information which is processed or is intended form part of a filing system. This applies to electronic or hard copy formats.

Data Subject	An identified or identifiable, natural, legal person.
GDPR	General Data Protection Policy
DPIA	A Data Protection Impact Assessment (DPIA) is also known as a Privacy Impact Assessment (PIA). It is a method which may be used to ensure privacy by design by conducting a prescribed risk assessment on data processes and making necessary adaptations, thereby implementing appropriate safeguarding measures. A DPIA is made mandatory by law in certain circumstances.
Privacy by Design	The concept of ensuring that security, confidentiality and integrity of personal data is prioritised within the heart of the methods used for processing the data.
Processing Data	Any activity which is performed on personal data whether or not this is manual or automated, such as: recording, organising, structuring, storing, updating, retrieving, disclosing or erasing. Examples may include; sorting email addresses into categories for marketing campaigns, recording absences from work, monitoring vehicle tracking etc.
Pseudonymised	To adapt how personal data is processed and presented such that the data cannot be attributed to a specific data subject, without additional personal data. The additional personal information must be kept separately and securely using appropriate technical and organisational measures.
Data Recipient	A natural person or organisation to whom personal data is disclosed or made available to. A recipient is not necessarily a third party with who the Company has professional dealings.

8. Policy

The Nominated Officer for Data Protection is: Tim Warner.

8.1 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’.

8.2 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.

Any additions or revisions to this policy will be communicated to staff where appropriate. We will notify data subjects of any changes that apply to them where appropriate, personally and in writing.

8.3 Roles & Responsibilities

8.3.1 Data Controller

The Company's Data Controller is **Tim Warner**, Director of Internal Operations. 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 determine how data subjects may exercise their rights.

8.3.2 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 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 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.

8.4 Conditions for processing data

Under data protection legislation the processing of personal data is prohibited unless there is a legitimate legal basis upon which the data is being processed. There are six potential legal bases for processing.

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 in to 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. Legal obligations imposed by a country outside of the EU may not be justified under this legal basis.

- 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 interest

The processing is necessary to perform a task either in the public interest or under instruction from an official authority or regulatory body. 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.) It is likely to be appropriate where people's data is used in a way in which they may reasonably expect, with minimum impact to their privacy, or where there is a compelling justification for the processing.

8.4.1 Special category data

The processing of special category or 'sensitive data' is strictly prohibited under UK and EU data protection laws. There are limited circumstances in which it is permissible to process special category data. If any of the conditions are met, then all other conditions and protections afforded to regular personal data will also apply. Some provisions including security, should be imposed more strictly.

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 data protection legislation. Advice from the relevant supervisory authority may need to be sought in advance to agree the appropriateness of this condition.

8.4.2 Criminal convictions and offences

Personal data of this nature shall be handled with a greater level of protection than that which may be adequate for the processing of standard personal data.

The Company shall only process data of this nature where there is a legitimate requirement to do so, namely in respect of its duties as an employer. Where there is a legal obligation for the Company to review or record data of this nature an appropriate member of staff may seek to establish the required information from the employee, worker, self-employed person, contractor or any other third party.

Examples of when this may be necessary include; when the performance of a duty requires a criminal record check.

8.4.3 Processing which does not require identification

When processing information, if you can remove all personal data which identifies the data subject, then you will no longer be required to adhere to the conditions for processing detailed in this policy.

If a data subject becomes identifiable then the conditions for processing will apply.

8.5 Collecting data

8.5.1 Transparency principle

Anyone acting on behalf of the company is expressly required to make sure that any information they provide to a data subject or supervisory authority is done so in a manner that is: concise, transparent, intelligible, uses clear and plain language and is provided in an easily accessible form.

8.5.2 Collecting personal data from the subject

If during the course of your employment you are required to collect personal data, you must ensure that the data subject is advised or made aware of each of the following:

- The identity and contact details of the controller
- The purposes and legal basis of the processing
- If the legal basis is the Company's legitimate interest, the interest must be detailed
- The recipients or categories of recipients of the personal data, if any
- Whether there is an intention to transfer personal data outside the European Economic Area and if so, whether an adequacy decision by the European Commission exists in relation to the transfer, or alternatively reference to the appropriate or suitable safeguards relied upon by the Company and how these can be obtained

To ensure fair and transparent processing, the following information must also be provided to the data subject:

- The length of time the personal data will be stored for or the criteria used to determine the length of time it will be stored for.
- Details of their rights (see 4.10).
- Any existence of automated decision-making including profiling, particularly if the profiling produces legal effects or significantly affects a data subject or involves special categories of personal data.

8.5.3 Collecting personal data from a source other than the subject

When information of this nature is collected, the subject must be provided with all the information in the above clause as well as the information below. This should be provided at the time it is obtained, in concise and plain language:

- The categories of the personal data collected

- The source of the data (and whether it was publicly available)

In these circumstances, the information must be provided within a reasonable period after obtaining the personal data, but at the latest within one month. However, if the data shall be used to communicate with the subject, then the information must have been provided by the first communication. If it shall be disclosed to another party, then the information must have been provided by the first disclosure.

8.5.4 Privacy and fair processing notices

The Company uses privacy notices to convey the information listed in the sections above at the point of data collection.

8.5.5 The purpose changes

If the original purpose for which the data that was collected changes, then the data subject must be informed of the new purpose. They must also be informed of any changes to the information already provided under the points in this section.

8.5.6 Multiple controllers

In a situation where the Company should act jointly with other organisations as a controller, then respective responsibilities will be clearly laid out between the parties.

8.6 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.

8.7 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: The Company has taken measures to prevent accidental and deliberate unauthorised access. <Optional: 'This includes 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 of filing system, faulty locks, viruses or malware.
This section is applicable to self-employed persons and contractors in so far as they will be asked to ensure compliance with these points and our security measures. In any event, they will be required to uphold obligations under applicable data protection laws at all times and without exception. Failure to do so will enable the Company to terminate the service agreement without notice and the incident may be reported to the relevant supervisory authority.

8.8 Record Keeping

The Company maintains records of data processing activities in accordance with data protection legislation. Record keeping is carried out for the following processing activities:

- Processing of personal data which is likely to result in a risk to the rights and freedoms of data subjects
- Processing of personal data which is regular and frequent
- Processing of personal data which includes special category data
- Processing of personal data which includes data about criminal convictions

8.9 Breach and Incident Reporting

Serious breaches must be reported to the relevant supervisory authority within 72 hours of becoming aware of the breach. Therefore, all employees and workers must immediately report an incident that may potentially or actually put personal data at risk of a data breach. This is never more imperative than when it is suspected that there may be actual loss, theft unauthorised disclosure or inappropriate use of personal data, either wholly or partly. In this event you must immediately refer to and follow the Company's Breach and Incident and Reporting Procedure.

Where a third-party service provider notifies you of an incident that may affect the Company and its responsibilities, you must immediately report the incident. In this event you must immediately refer to and follow the Company's Breach and Incident Reporting Procedure.

8.10 The rights of data subjects

The Company shall be diligent in providing data subjects information about their rights and in complying with any appropriate assertions of their rights.
All reasonable efforts will be made to verify the identity of the data subject before carrying out any requests or disclosures of information made by them. These efforts may include the request for additional personal information if necessary.
The following rights apply to all data subjects:

- Right of transparent communication
- Right of access
- Right to rectification
- Right to erasure (right to be forgotten)
- Right to restriction of processing
- Obligation to notify recipients
- Right to data portability
- Right to object
- Right to not be subject to automatic decision making

8.11 Subject access requests

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 Controller <Insert if applicable: 'or 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 e-mail) 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.

8.12 General guidance for employees

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.

8.13 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.

8.14 Non-compliance

- This policy along with associated documents, seeks to guide and instruct all member 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).

8.15 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.

8.16 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,
80 Jackson Road,
Leicestershire,
LE67 1HL

or by email to tim.warner@educ8group.com

9. Metrics

The following metrics are applicable to this procedure:

Number of SARs

Number of Data Breaches

10. Quality Records

The following Quality Records shall be generated and managed:

Required Record	Custodian
Registration with ICO as a Data Controller	DPO
Breach Reports	DPO
Data Requests	DPO

11. Form(s)/Template(s)

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

Form Number	Title
F0017DP	Serious Breach Notification Form