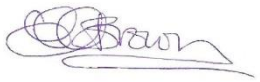
SCHOOL BUSINESS SERVICES – DATA PROTECTION POLICY

This policy has been approved by SBS directors and any amendments to it require directors' approval.

Version	Issued	Reason	Reviewed	Approved
1.1	09/2014	Initial version		MT
1.2	09/2015	Update and review		MT
1.3	10/2016	Update and review		MT
1.4	07/2017	Update and review		BH/ISO
1.5	05/2018	Update and review - GDPR	BH	SEC
1.6	03/2019	ISO Audit Review	RP	BH
1.7	03/2020	ISO Audit Review	BH	CC
2.1	04/2021	New procedure via SEG – not audited	BH	TB

Next Document review date: June 2021

Reviewed By:	Date Approved:	Approved by:
Becky Hall	20/04/2020	Tina Brown – Chief Executive 

Document Owner and Approval

The Data Protection Officer is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff on relevant Company Intranet, HR system or shared drive.

This policy was approved by the SEG Board of Directors on 13/10/2018 and is issued on a version-controlled basis under the signature of the Chief Executive Officer (CEO).

DATA PROTECTION POLICY

1. Introduction

The purpose of the General Data Protection Regulation (GDPR), enacted in the UK by the Data Protection Act 2018 is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge.

1.1 Scope

This policy sets out data protection standards which should be followed across Supporting Education Group (the Group). References to Company is to each individual Company within the Group.

This policy applies to all staff within the Group who should become familiar with and comply with its terms. Staff includes employees, temporary and agency works, other contractors, interns and volunteers.

Material scope – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behavior of data subjects who are resident in the EU.

Staff are expected to familiarise themselves with the provisions set out and fully understand their individual responsibilities under the GDPR. Any breach of the GDPR will be dealt with under the Group's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

1.2 Definitions

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special category data – personal data revealing the data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical and mental health, sex life, sexual orientation, biometric or genetic data.

Criminal offence data - personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

Data controller – the organisation storing and controlling such information is referred to as the Data Controller. This could be Supporting Education Group or any of the Companies within the Group. Each are data controllers in their own right.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Automated decision making and profiling – two forms of automated processing.
Automated decision making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances. Profiling is also based on automated processing where it is used to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

2. Core Principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in the GDPR. The Group's policies and procedures are designed to ensure compliance with those principles. The principles that must be adhered to are set out below.

2.1 Personal data must be processed lawfully, fairly and in a transparent manner

2.1.1 **Lawful** – identify a specific ground before you can process personal data. These are often referred to as the "lawful bases" for processing. The lawful bases for personal data are: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law;
- For the purposes of the organisation's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

For special category data, we can only process this data provided one of the above lawful conditions are met and one of the lawful bases for special category data is met. These conditions can be found here.

For criminal offence data, we can only process this data provided one of the above lawful conditions are met and there is a legal or official authority to process this data. These conditions can be found here.

See 2.1.4 below for more detail about consent.

2.1.2 **Fairly** – in order for processing to be fair, personal data will be handled in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.

2.1.3 **Transparently** – i.e. to be clear, open and honest with data subjects about who we are, and how and why we use their personal data. The GDPR includes rules on giving privacy information to data subjects, placing an emphasis on making privacy notices understandable and accessible.

The Group will issue privacy notices from time to time, informing data subjects about the personal information that we collect and hold, how they can expect their personal information to be used and for what purposes.

The Group take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

2.1.4 **Consent** – Where the Group relies on consent as a lawful basis for processing (as set out above), it will adhere to the requirements set out in the GDPR. Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. The Group will keep records of consents obtained in order to demonstrate compliance with consent requirements under the GDPR.

Where the Group provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16.

2.2 Personal data can only be collected for specific, explicit and legitimate purposes

Personal data will not be processed in any matter that is incompatible with the legitimate purposes. The Group will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless they have informed the data subject of the new purpose (and they have consented where necessary).

2.3 Personal data must be adequate, relevant and limited to what is necessary for processing

2.3.1 The Group will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

2.3.2 When personal data is no longer needed for specified purposes, the Group shall delete or anonymise the data.

2.3.3 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be include a fair processing statement or link to privacy statement and approved by the Data Protection Officer (DPO).

2.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

2.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

2.4.2 The DPO is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

2.4.3 It is also the responsibility of the data subject to ensure that data held by the Group is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

2.4.4 Employees, temporary workers, contractors, clients, candidates and any other interested parties should be required to notify the Group of any changes in circumstance to enable personal records to be updated accordingly. The Group will ensure that any notification regarding change of circumstances is recorded and acted upon.

2.4.5 The Group is responsible for responding to requests for rectification from data subjects within one month (please see the Data Requests Procedure for further details on this process).

2.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

2.5.1 Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The Group will ensure that they adhere to legal timeframes for retaining data.

2.5.2 Where personal data is retained beyond the processing date, it will be minimised in order to protect the identity of the data subject in the event of a data breach.

2.5.3 Personal data will be retained in line with the Group Data Retention Policy and each Company's data retention schedule. Once a retention date is passed, it must be securely destroyed as set out in this procedure.

2.6 Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

2.6.1 In order to assure the protection of all data being processed, the Group will develop, implement and maintain technical security measures. This includes using measures such as: -

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the purpose for which it is processed; and
- Identifying appropriate international security standards relevant to the Group.

2.6.2 When assessing appropriate organisational measures the Group will use the following: -

- Training and awareness for staff;
- Data protection clauses within employment contracts;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper-based records;
- Adoption of a clear desk policy;
- Storing of paper-based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

The Group's compliance with this principle is contained in its information security policies.

2.7 <u>The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)</u>

2.7.1 The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

2.7.2 The Group will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, conducting regular data audits, ensuring appropriate staff training, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

2.7.3 The Group have appointed a Data Protection Officer (DPO) whose details are as follows: -

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174
Lead Contact: Craig Stilwell

2.7.4 The DPO is responsible for overseeing this policy and developing data related policies and guidelines. If you have any data related queries please do direct these to the DPO in the first instance. In particular, please contact the DPO if: -

- If you are unsure of the lawful basis being relied on by the Group to process personal data;
- If you need to draft privacy notices or fair processing notices;
- If you are unsure about the retention periods for the personal data being processed;
- If you are unsure about what security measures need to be put in place to protect personal data;
- If there has been a personal data breach and would refer you to the procedure set out in the Group's data breach procedure;
- If you are unsure on what basis to transfer personal data outside the EEA;
- If you need any assistance dealing with any rights invoked by a data subject (and would refer you to the data requests procedure);
- Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;
- If you plan to undertake any activities involving automated processing or automated decision making;
- If you need help complying with applicable law when carrying out direct marketing activities;
- If you need help with any contracts or other areas in relation to sharing personal data with third parties.

3. Data Subjects' Rights

3.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

3.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.
3.1.2 To prevent processing likely to cause damage or distress.
3.1.3 To prevent processing for purposes of direct marketing.
3.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.
3.1.5 To not have significant decisions that will affect them taken solely by automated process.
3.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.

3.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.

3.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.

3.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

3.1.10 To object to any automated decision making or profiling that is occurring without consent.

3.2 The Group have a Data Requests Procedure which provides further detail on how an individual can make a data request.

4. Data Breaches

4.1 The GDPR requires the Group to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

4.2 The Group have a Data Breach Procedure which details how to deal with any suspected personal data breach. Staff should familiarise themselves with this procedure and notify breaches promptly in accordance with it. The Group will notify data subjects or any applicable regulator where we are legally required to do so.

4.3 If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO and the person designated as the key point of contact for personal data breaches. See also Data Breach Procedure.

5. Security of data

5.1 All staff are responsible for ensuring that any personal data that the Group holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the Group to receive that information and the relevant safeguards have been put in place (for example a data sharing agreement).

5.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. Personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access
- if computerised, password protected in line with corporate requirements in the Access Control Policy; and/or
- stored on computer media which are encrypted.

5.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised users (including other staff). All staff are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

5.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving.

5.5 Personal data may only be deleted or disposed of in line with retention procedures and guidelines. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.

5.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

6. Disclosure of data

6.1 Staff must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the Group's business.

6.2 Examples of steps to be taken by the Group include: -

- Checking that sharing the data processed complies with the privacy notice/sharing agreement and, if required, the data subject's consent has been obtained;
- Confirming that third parties comply with required security standards and have policies, privacy notices and training in place;
- Executing a data sharing agreement;
- To check that cross-border transfer restrictions are complied with;
- Conducting a data protection impact assessment (DPIA).

6.3 There may be circumstances where the Group is required either by law or in the best interests of individuals to pass information onto external authorities, for example, law enforcement or the department of health.

7. Retention and disposal of data

7.1 The Group shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected. Staff should follow the Group Retention Policy and Company retention schedule in order to adhere to this requirement.

7.2 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.

8. Privacy by design and Data Protection Impact Assessments (DPIAs)

8.1 The Group adopt a privacy be design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

8.2 Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the Group takes into account the nature and purposes of the

processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

8.3 In order to achieve a privacy by design approach, the Group conduct DPIAs for any new technologies or systems being used which could affect the processing of personal data. In any event the Group carries out DPIAs when required by the GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies which significantly affect personal data;
- For the use of automated processing;
- For large scale processing of special category data;
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

8.4 Should a staff member be required to complete a DPIA they should use the Group DPIA form and consult with the DPO.

9. International transfers

9.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects". The exception to this is if data is transferred to someone employed within the same Company.

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

9.1.1 An adequacy decision - The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances, no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union.* *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*

9.1.2 Binding corporate rules – The Group may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval. This is for internal transfers between branches of multinational organisations.

9.1.3 Standard contract clauses – the Group may adopt approved standard contractual clauses for the transfer of data outside of the EEA. Standard clauses are those adopted by the Commission and are available on the ICO website. In the absence of an adequacy decision, standard contractual clauses are the most likely option for international data transfers. The DPO can help implement these clauses when required.

9.1.4 Exceptions - in the absence of any of the above, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

10. Information asset register/data inventory

10.1 The Group are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention.

10.2 The Group has established a data inventory and data flow process which contains:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the Group throughout the data flow;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

10.3 In addition each Company also retains their own records of processing activities as required by the ICO. SBS has been registered with the ICO since 2008 and renews annually.