

GDPR Compliance Statement

Contents

SBS Company Compliance Project.....	1
What action are we taking to prepare for the GDPR?	1
What technical and organisational security measures do we have in place to protect personal data?	1
What policies and procedures do we have in place to protect personal data?	2
How secure are our systems?	2
Data Processors for Schools	3
The subject matter, duration, nature and purpose of the processing.	3
The type of personal data being processed.	3
The categories of the data subjects.	3
The obligations and the rights of the data controller (the school).	3
SBS Systems Compliance – SBS Online.....	4
Processing conditions and security	5
Data sharing	5
Schools’ compliance support	5
Data storage & retention	6
Demonstration of compliance	6

SBS Company Compliance Project

What action are we taking to prepare for the GDPR?

School Business Services (SBS) has formed an internal focus group specifically for the GDPR. The focus group is currently working through the GDPR 12 steps guidance published by the ICO in order to be fully compliant by 25 May 2018. This includes, but is not limited to, data analysis, policies and procedures, business continuity, IT security/risk assessments (aka penetration testing), and staff training to mitigate risk.

SBS is contacting partners, suppliers and subcontractors to obtain evidence of their compliance but we understand everyone is in the same situation and working to the deadline, so request that extra time is given for this element of the legislation.

What technical and organisational security measures do we have in place to protect personal data?

SBS take data protection very seriously. The systems we use to store customer data have secure access controls, they are password protected with varying levels of access to sensitive information. Our servers are protected by firewalls. We have a comprehensive Business Continuity and Disaster Recovery Plan in place. SBS is ISO27001 compliant and staff are required to adhere to strict access controls including the physical security.

What policies and procedures do we have in place to protect personal data?

- Access policy
- Asset management and disposal policies
- Bring your own device policy
- Business continuity & disaster recovery plan
- Company values - Integrity
- Data protection policy
- Data storage, retention & disposal
- Employee handbook*
- Hospitality & gift policy (anti-bribery)
- Information Security Management Systems
- Password policy
- Privacy notice & policy
- Risk management procedure
- SBS Online security FAQs
- Supplier management policy

*Also, terms & conditions of employment, including data protection training; IT, internet, social media and email usage; and trust & confidentiality agreement.

How secure are our systems?

SBS has performed full risk assessments on all systems and are working through any areas identified for improvement, but are fully confident we have not uncovered any serious threats.

SBS keeps a non-conformance log of any threats and carry out root cause analysis of all incidents, large or small, and devise immediate and long-term corrective actions.

Staff are responsible for creating strong passwords, protecting their login information from unauthorised access and the management/HR teams ensure password renewals occur periodically and through the employee leaver policy.

Do we have any information management accreditation?

SBS has been accredited with [ISO 27001](#) information security management systems since 2015. The current certificate can be [accessed here](#) >

Data Processors for Schools

As we process personal data that customers share with us, we need to jointly agree:

The subject matter, duration, nature and purpose of the processing.

The subject matter, duration, nature and purpose of the processing on behalf of our schools is specific to the support service team or business unit. These can include school finance and contractual information, staff and pupil MIS data, employee information including performance, and purchase history.

The type of personal data being processed.

The type of personal data being processed will differ for each service but are likely to include salutation, full name, position, email address, location, IP address, social media profile, salary. On occasion this may include sensitive personal data from an MIS system such as gender, ethnicity, religion, mental health, performance history, offences or CCTV footage/images.

The categories of the data subjects.

The categories of the data subjects for which we process data on behalf of schools is, but not limited to, members of staff (past and present), pupils (past, present and future), parents, and suppliers and partners.

Legal bases for processing data includes performance of our contracted services, complying with legal obligations and proportionate processing for a legitimate business interest.

The obligations and the rights of the data controller (the school).

Under the terms of a **service support contract** the Client shall:

- Co-operate with SBS in all matters relating to the Services;
- Provide SBS, its employees, agents, consultants and subcontractors, with access to the Client's premises, office accommodation and other facilities as reasonably required by SBS;
- Provide SBS with such information and materials as SBS may reasonably require in order to supply the Services, and ensure that such information is accurate in all material respects;
- Obtain and maintain all necessary licences, permissions and consents which may be required before the date on which the Services are to start;
- Keep and maintain all materials, equipment, documents and other property of SBS ("SBS Materials") at the Client's premises in safe custody at its own risk, maintain the SBS Materials in good condition until returned to SBS, and not dispose of or use the SBS Materials other than in accordance with SBS's written instructions or authorisation.
- If SBS' performance of any of its obligations under this agreement is prevented or delayed by any act or omission by the Client or failure by the Client to perform any relevant obligation (Client Default): (a) SBS shall without limiting its other rights or remedies have the right to suspend performance of the Services until the Client remedies the Client Default; (b) SBS shall not be liable for any costs or losses sustained or incurred by the Client arising from SBS's said suspension; and (c) the Client shall reimburse SBS on written demand for any costs or losses sustained or incurred by SBS arising directly or indirectly from the Client Default. That the data processor (you, the supplier) processes data only on the documented instructions of the school

Under the terms of an **SBS Online budget management contract** the Client shall:

- The Client shall own all rights, title and interest in all of the Client Data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the Client Data.
- In the event of any loss or damage to Client Data, the Client's sole and exclusive remedy shall be for SBS to use reasonable commercial endeavours to restore the lost or damaged Client Data from the latest back-up of such Client Data maintained by SBS. SBS shall not be responsible for any loss, destruction, alteration or disclosure of Client Data caused by any third party.
- SBS shall, in providing the Services, comply with its Privacy Policy relating to the privacy and security of the Client Data available on request from SBS. Such document may be amended from time to time by SBS in its sole discretion.
- If SBS processes any personal data on the Client's behalf when performing its obligations under this agreement, the parties record their intention that the Client shall be the data controller and SBS shall be the data processor and in any such case:
 - The Client acknowledges and agrees that the personal data may be transferred or stored outside the EEA or the country where the Client and the Authorised Users are located in order to carry out the Services and SBS' other obligations under this agreement;
 - The Client shall ensure that it is entitled to transfer the relevant personal data to SBS so that SBS may lawfully use, process and transfer the personal data in accordance with this agreement on the Client's behalf;
 - The Client shall ensure that relevant third parties have been informed of, and have given their consent to, such use, processing, and transfer as required by all applicable data protection legislation;
 - SBS shall process the personal data only in accordance with the terms of this agreement and any lawful instructions reasonably given by the Client from time to time; and
 - Each party shall take appropriate technical and organisational measures against unauthorised or unlawful processing of the personal data or its accidental loss, destruction or damage.

[SBS Systems Compliance – SBS Online](#)

See separate SBS Online Budget Management Security FAQs document

Schools should never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system. All school employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information.

Under the terms of **all** contracts:

Each party shall keep the other party's Confidential Information confidential and shall not:

- Use such Confidential Information except for the purpose of exercising or performing its rights and obligations under this agreement; or
- Disclose such Confidential Information in whole or in part to any third party, except as expressly permitted by this clause.

Processing conditions and security

That the data processor (SBS) processes data only on the documented instructions of the school. And that the people who process the data are committed to confidentiality and that we take measures to ensure secure processing.

All SBS staff who process the data are committed to confidentiality and we take measures to ensure secure processing. New staff joining the business receive data protection and processing training and all staff undergo subsequent refresher training. Internal policies, staff contracts and job descriptions mandate strict obligations on the handling of client information and especially personal data.

SBS service managers are responsible for randomly sampling records to ensure that all required data has been captured, and that data is accurate and complete.

Data sharing

That SBS will not engage another processor without prior written authorisation from the school, and that if we do so, that processor will also be bound by the same data protection conditions as are in the contract with the school.

SBS will not share data with third parties without authorisation from the school/individual unless required for the delivery of contracted services, as specified in the contract terms and conditions, and that if we do so, that processor will also be bound by the same data protection conditions. As documented in the ISMS policy, it is the responsibility of all staff to ensure that all data is treated with the utmost confidentiality, and that no data is given out without the prior authority of any person affected.

On occasion, third parties may be engaged for system integration requirements; however schools will need to approve this directly with the third party.

Schools' compliance support

That SBS helps the school comply with requirements regarding the data rights of individuals (e.g. to access, delete or rectify data), secure processing, the reporting and communication of data breaches, and the conducting of impact assessments where relevant.

We work for you, the data controller, and process your data based on your instructions. We cannot give you advice on how to become nor make you compliant with any regulations, or devise/deliver processes or assessments on your behalf. However, in the course of our working relationship we will facilitate schools as much as we can insofar as can be handled by the system/platform utilised on behalf of the school.

We are investigating solutions, resources and support service providers for schools to help with compliance and will publish these on our website in due course.

Data storage & retention

That SBS deletes or returns the personal data to the school at the end of the provision of services.

This is not a current documented procedure as when processing data on behalf of schools this is completed using logins for their systems and accounts. By removing access we will no longer have access to this data. Any data exported from systems for reporting will automatically be deleted during our scheduled data retention and removal processes.

Demonstration of compliance

That we make information available to demonstrate compliance with the obligations in contracts, and allow customers or an instructed third party to conduct audits and inspections.

This FAQs document will be available on the corporate website and copies of non-sensitive policies are available on request. Third party audits and inspections are possible providing this does not compromise SBS' data and that of our other customers.

Contact

If you have any further queries please email feedback@schoolbusinessservices.co.uk

For service-specific enquiries please call 0345 222 1551 and select your dedicated Service Desk:

- Option 1 - ICT support
- Option 2 - Finance & Business
- Option 3 - SIMS (MIS) & FMS technical support
- Option 6 - HR & Payroll support
- Option 7 - Procurement
- Option 8 - SBS Online support

Or send us an email:

ICT: ictservicedesk@schoolbusinessservices.co.uk

Finance: financeservicedesk@schoolbusinessservices.co.uk

SBS Online: sbsonline@schoolbusinessservices.co.uk

MIS: misservicedesk@schoolbusinessservices.co.uk

HR & Payroll: hrrservicedesk@schoolbusinessservices.co.uk