BOSSS Guardians

Data Protection and Privacy Policy

Guardianship Organisation · AEGIS Accredited

Document reference	Policy 2.10
Version	0.7
Date	September 2026
Policy owner	Tina Wong, Data Controller
Policy Reviewer	Victoria Barfoot-Saunt, Compliance Director
Next review	September 2027
Applies to	All directors, staff, volunteers, homestays, students, parents and agents

Statutory and regulatory basis. This policy has been written to align with the UK GDPR, the Data Protection Act 2018, Information Commissioner's Office guidance on children's information, special category data and safeguarding information sharing, Keeping Children Safe in Education 2026 (in force 1 September 2026), Working Together to Safeguard Children, Department for Education information-sharing guidance, and the AEGIS Code of Practice and Guardianship Organisation Quality Standards, including the standards on information sharing and data protection.

A note on applicability. Keeping Children Safe in Education, referred to throughout as KCSIE, is statutory guidance for schools and colleges. BOSSS UK is a guardianship organisation and is not a school, so KCSIE does not apply to it directly. BOSSS UK nevertheless adopts KCSIE as its safeguarding standard because AEGIS requires accredited guardianship organisations to align with it, and because our staff and homestays care for the same children outside term time. Where a statutory duty or guidance is written for schools, colleges, local authorities or other statutory safeguarding partners, we apply the equivalent proportionate arrangement that is relevant to a guardianship organisation and say so.

1 Who we are

1.1 This is the privacy notice of BOSSS UK. In this document, "we", "our" or "us" refers to BOSSS (UK) Limited.

1.2 We are company number 4487010, registered in England and Wales as BOSSS (UK) Limited. Our registered office is:

C/O The Cousins, Office No 216, Building 1 Chalfont Park, Chalfont St. Peter, Gerrards Cross, Buckinghamshire, England, SL9 0BG

1.3 We are registered with the Information Commissioner's Office under registration reference ZA139160. Our Data Controller is Tina Wong.

1.4 You can contact us about anything in this policy by post at the address above, by email at bosss.guardian@outlook.com or by telephone on +44 (0)1202 980804.

1.5 Our staff have access to personal confidential information that we collect about homestays, students, overseas parents and other staff members. This information is gathered in order to enable us to provide a guardianship service and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that BOSSS UK complies with its statutory obligations.

1.6 This policy is available on our website at www.bosssuk.co.uk and is made available to our parents, students, staff, homestays and partner schools. It must be read alongside the Data Retention Policy and the Safeguarding and Child Protection Policy 8.1.

2 The law that applies

2.1 The EU General Data Protection Regulation replaced the Data Protection Directive 95/46/EC and was designed to harmonise data privacy laws across Europe, to protect and empower data privacy, and to reshape the way organisations approach data privacy.

2.2 Following the United Kingdom's withdrawal from the European Union, the EU GDPR no longer applies to the UK. Because we operate inside the UK, BOSSS UK complies with UK data protection law. The provisions of the EU GDPR were incorporated into UK law and now form the UK GDPR. In practice there is little change to the core data protection principles, rights and obligations.

2.3 The Data Protection Act 2018 came into force on 25 May 2018 and replaced the Data Protection Act 1998. The UK GDPR sits alongside the Data Protection Act 2018, with technical amendments so that it works in a UK-only context.

2.4 The Information Commissioner's Office remains the independent supervisory body for the UK's data protection legislation.

2.5 Information is stored and processed in accordance with the UK GDPR and the Data Protection Act 2018.

2.6 Because we provide services to children, this policy must also be read in the context of safeguarding law and guidance, including the Children Act 1989, section 11 of the Children Act 2004, the Safeguarding Vulnerable Groups Act 2006, statutory and non-statutory information-sharing guidance issued by the Department for Education, and ICO guidance which confirms that

data protection law enables proportionate information sharing where this is necessary to safeguard a child or young person.

2.7 Where electronic marketing, newsletters or similar direct communications are sent, BOSSS UK also follows the Privacy and Electronic Communications Regulations 2003, as amended, and uses consent or another lawful permission where required.

3 The data protection principles

Everyone responsible for using data follows the data protection principles, to make sure that information is:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with those purposes. Further processing for archiving purposes in the public interest, or for scientific, historical research or statistical purposes, is not considered incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed, subject to the archiving exception above and to appropriate technical and organisational measures; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4 Definitions

4.1 The UK GDPR applies to personal data, meaning any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier.

4.2 This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data and online identifier, reflecting changes in technology and the way organisations collect information about people.

4.3 The UK GDPR applies both to automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

4.4 Special category data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, together with genetic data, biometric data used for identification, data concerning health, and data concerning a person's sex life or sexual orientation. Personal data relating to criminal convictions and offences is not special category data, but similar extra safeguards apply to its processing.

5 What we process

5.1 BOSSS UK processes and stores personal information and data including:

- personal details;
- family, lifestyle and social circumstances;
- business activities of the person whose personal information we are processing;
- goods and services provided;
- financial details;
- education details; and
- employment details.

5.2 BOSSS UK also processes special category and other sensitive information and data, which may include:

- dietary, medical, physical or mental health details;
- offences and alleged offences;
- racial or ethnic origin;
- religious or other beliefs of a similar nature;
- sanctions matters; and
- safeguarding information.

5.3 Special category data is stored in access-controlled, encrypted systems, is not held in general email inboxes or on unencrypted local drives, and is accessible only on a need-to-know basis. Hard copies of medical forms are stored in locked filing. Further detail is in the Data Retention Policy.

6 Lawful basis for processing

We rely on the following lawful bases under Article 6 of the UK GDPR:

Basis	Examples
Article 6(1)(a), consent	Use of photographs, marketing communications
Article 6(1)(b), contract performance	Guardianship agreements, homestay arrangements
Article 6(1)(c), legal obligation	DBS checks, HMRC records, UKVI requirements
Article 6(1)(f), legitimate interests	Internal training records, operational logs

For special category data, including health, medical, dietary, SEND and safeguarding information, processing relies on an Article 6 lawful basis and a separate Article 9 condition. The principal Article 9 conditions used by BOSSS UK are Article 9(2)(a), explicit consent, where consent is appropriate and can be freely given; Article 9(2)(b), employment, social security and social protection obligations where applicable; Article 9(2)(g), substantial public interest, where processing is necessary and proportionate

for safeguarding or other statutory purposes; and Article 9(2)(h), health or social care, where relevant to the provision of care or support. Where a Data Protection Act 2018 Schedule 1 condition is required, BOSSS UK documents the condition relied on and maintains an appropriate policy document. Criminal offence data, including DBS information and information about alleged offences, is processed under Article 10 of the UK GDPR and the relevant Schedule 1 conditions in the Data Protection Act 2018. Safeguarding of children and individuals at risk is a processing condition which permits the sharing of special category data, including without consent where there is good reason to do so and the sharing is necessary, relevant and proportionate.

7 Individual rights

The UK GDPR provides the following rights for individuals:

- the right to be informed;
- the right of access, exercised through a data subject access request;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making, including profiling.

A request to exercise any of these rights may be made to the Data Controller using the contact details at paragraph 1.4. We respond within one calendar month. The right to erasure does not override a legal obligation to retain information: for example, a request to delete a safeguarding record cannot override the retention requirements set out in the Data Retention Policy. Each request is assessed individually by the Data Controller.

8 Disclosing your information

8.1 Where applicable, we may disclose your personal information to any member of our group, including any subsidiary, our holding company and its other subsidiaries.

8.2 We may also disclose your personal information to third parties:

- where we sell any or all of our business or assets to a third party;
- where we are legally required to disclose your information;
- to assist fraud protection and minimise credit risk;
- where you are applying as a homestay or staff member, in order to create a homestay or staff profile, shared only with relevant parties in relation to hosting students;
- in processing your application and as part of our safer recruitment policy, in order to undertake a DBS check as an essential part of our screening process; and

- as part of our accreditation process, in order to share contact details with AEGIS head office and with lead and supporting inspectors. We permit them to process your data only for specified purposes and in accordance with the UK GDPR, and we share the minimum amount necessary.

8.3 We may also share information with a school, local authority, police, health service, statutory safeguarding partner, AEGIS inspector or another safeguarding agency where it is relevant to safeguarding or promoting the welfare of a child. KCSIE 2026 and Department for Education information-sharing guidance reinforce the expectation that relevant information is shared in a timely way, governed by necessity, relevance, accuracy and proportionality. ICO guidance is clear that data protection law should not be treated as a barrier to sharing information needed to keep a child safe. Part 12 of the Safeguarding and Child Protection Policy 8.1 sets out how we do this, including the transfer of information when a student changes school.

9 Artificial intelligence tools

This section is new in version 0.6. Staff must never enter personal data, special category data or safeguarding information into a public or consumer artificial intelligence tool. Information entered into such a tool may be retained by the provider, may be used to train models, and leaves our control, which would constitute an unauthorised disclosure. Where BOSSS UK wishes to adopt an AI tool that processes personal data, the Data Controller must first complete a Data Protection Impact Assessment. We follow the Department for Education guidance on generative artificial intelligence in education.

10 Retention and disposal

Retention periods for every category of record are set out in the Data Retention Policy, which must be read alongside this policy. In summary: records are kept only as long as necessary; safeguarding records are subject to extended retention and must never be destroyed without written sign-off from the Data Controller; a copy of a DBS certificate must not be retained beyond six months from issue; and disposal is by permanent deletion for digital records and by cross-cut shredding or a certified confidential waste contractor for paper records, logged in the Secure Disposal Register.

11 Data breaches

Article 33 of the UK GDPR requires that breaches likely to result in a risk to individuals' rights and freedoms are reported to the Information Commissioner's Office within 72 hours of discovery. Breaches likely to result in high risk must also be communicated to affected individuals without undue delay. All staff must report any suspected or actual breach to the Data Controller immediately, and must not attempt to investigate or resolve a breach without notifying the Data Controller first. All breaches are recorded in the Data Breach Log, even where no report to the Commissioner is required.

12 Complaints

If you are unhappy with how we have handled your personal data, please contact the Data Controller using the details at paragraph 1.4, or use our Complaints Policy 9. You also have the right to complain directly to the Information Commissioner's Office at www.ico.org.uk or on 0303 123 1113. You do not need our permission to do so.

Change control

Date	Version	Name	Change control comments
June 2022	0.5	Victoria Barfoot-Saunt	Previous approved version
September	0.6	Victoria Barfoot-Saunt	No substantive change since previous review.
12/09/2026	0.7	Victoria Barfoot-Saunt	Registered office updated to C/O The Cousins, Office No 216, Building 1 Chalfont Park, Chalfont St. Peter, Gerrards Cross, Buckinghamshire, England, SL9 0BG. Contact routes for exercising rights added at 1.4 and 7. Special category data defined at 4.4 and handling added at 5.3. Lawful basis table added at 6. New section 9 on artificial intelligence tools. New section 10 cross-referring to the Data Retention Policy. New section 11 on data breaches. New section 12 on complaints, including the right to complain to the Information Commissioner directly. Safeguarding information sharing added at 8.3 following KCSIE 2026. Typographical error "collet" corrected

End of policy