Data Protection and Privacy Policy (2.10)

1. This is the privacy notice of BOSSS UK. In this document, “we”, “our”, or “us” refer to BOSSSUK.

2. We are company number 4487010 registered in the UK as BOSSS (UK) Limited. Our registered office is: 42A Packhorse Road, Gerrards Cross, England, SL9 8EB, UK.

3. Our staff will have access to personal confidential information that we collet on host families, students, overseas parents and other staff members. This information is gathered in order to enable it 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 Guardians complies with its statutory obligations.

4. We are registered with the Information Commissioners Office (ICO) and information will be stored and processed in accordance with the General Data Protection Regulation (GDPR) 25 May 2018 and the Data Protection Act (DPA) 2018. Our registration reference is ZA139160 and our Data Controller is Betty Stevens.

5. The EU GDPR replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.

6. The DPA 2018 came into force on 25th May 2018 and replaces the DPA 1998.

7. This Data Protection policy is available on our website www.bosssuk.co.uk and is made available to our parents, students, staff, homestays and partner schools.

8. GPDR Principles

8.1. Everyone responsible for using data will follow the ‘data protection principles’ to make sure that the information is:

8.2. Processed lawfully, fairly and in a transparent manner in relation to individuals

8.3. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

8.4. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

8.5. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

8.6. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational

measures required by the GDPR in order to safeguard the rights and freedoms of individuals

8.7. 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."

9. GPDR Definitions

9.1. Personal data

9.2. The 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.

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

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

9.5. Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

9.6. Sensitive personal data

9.7. The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9).

9.8. The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

9.9. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

10. GDPR includes the following rights for individuals:

10.1. The right to be informed

10.2. The right of access

10.3. The right to rectification

10.4. The right to erasure

10.5. The right to restrict processing

10.6. The right to data portability

10.7. The right to object

10.8. The right not to be subject to automated decision-making including profiling

11. BOSSS UK processes and stores personal information and data including:

11.1. Personal details

11.2. Family, lifestyle and social circumstances

11.3. Business activities of the person whose personal information we are processing

11.4. Goods and services provided

11.5. Financial details

11.6. Education details

11.7. Employment details

12. BOSSS UK also processes sensitive information and data which may include:

12.1. Dietary, medical, physical or mental health details

12.2. Offences and alleged offences

12.3. Racial or ethnic origin

12.4. Religious or other beliefs of a similar nature

12.5. Sanctions breaches or policy

12.6. Safeguarding issues

12.7. Complaints

13. BOSSS UK will when necessary need to share the personal information we process with the individual and also with other organisations. Where this is necessary we are required to comply with all aspects of the General data protection Regulation (GDPR) 25 May 2018. Consent will be sought appropriately when required.

14. **Use of student photographs for publicity**

14.1. We will not use any photographs of the student for publicity without the parent's prior permission.

14.2. In the event we would like to use a photograph of your child for our publicity material we would seek the parent's permission in writing and confirm the anticipated way in which the photograph will be used.

15. Exemptions

15.1. GPDR Article 23 enables Member States to introduce derogations to the GDPR in certain situations.

15.2. Member States can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a

democratic society to safeguard:

15.2.1. National security;

15.2.2. Defence;

15.2.3. Public security;

15.2.4. The prevention, investigation, detection or prosecution of criminal offences;

15.2.5. Other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;

15.2.6. The protection of judicial independence and proceedings;

15.2.7. Breaches of ethics in regulated professions;

15.2.8. Monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;

15.2.9. The protection of the individual, or the rights and freedoms of others; or

15.2.10. The enforcement of civil law matters.

16. GPDR Chapter IX provides that Member States can provide exemptions, derogations, conditions or rules in relation to specific processing activities. These include processing that relates to:

16.1. Freedom of expression and freedom of information;

16.2. Public access to official documents;

16.3. National identification numbers;

16.4. Processing of employee data;

16.5. Processing for archiving purposes and for scientific or historical research and statistical purposes;

16.6. Secrecy obligations; and

16.7. Churches and religious associations.

17. Breaches

17.1. The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

17.2. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

17.3. You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or

not you need to notify the relevant supervisory authority and the affected individuals.

17.4. You must also keep a record of any personal data breaches, regardless of whether you are required to notify.