TASIS

THE AMERICAN SCHOOL IN ENGLAND

Data Protection Policy

Document

Information Sharing Category	PUBLIC
TASIS Document reference (Org, Doc, version, date)	TASIS_DPP_V3_0_14062017
Version	3.0
Date published	14-06-2017
Date ratified by Head of School	14-06-2017
To be reviewed before	Light touch: Annually from above date Full review: 5 years from above date
Responsible area	Head's Office

1. Use of Personal Data

1.1. TASIS England (the School) is an international co-educational day and boarding school, for children in the age range 3 to 18 years.

1.2. The School is committed to safeguarding and promoting the welfare of students and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.

1.3. The School processes personal data including names, addresses and contact numbers, both in electronic and paper form, in line with the conditions described within Data Protection Act 1998 (the Act) in order to:

a. provide education and pastoral care to day and boarding students and their parents, delivered by school staff;
b. provide academic, examination and career references for day and boarding students and staff;
c. fulfil its contractual or other legal and regulatory obligations towards current day and boarding students (both past and prospective) all staff, parents, Directors and others;
d. protect the vital interests of all students and all staff employed by the School.

2. Purpose

2.1. The School is registered as a Data Controller under the Act. This Policy is intended to operate in accordance with the provisions and spirit of the Act along with relevant guidance and good practice, paying particular regard to the 8 Data Protection Principles set out in the Act and summarised as follows:

a. Personal data will be processed fairly and lawfully and in compliance with Schedule 2 and/or Schedule 3 of the Act as applicable;
b. Personal data will be processed only for specified lawful purposes;
c. Personal data will be adequate, relevant and not excessive in regard to the purposes for which it is processed;
d. Personal data will be accurate and up to date;
e. Personal data will be kept only for as long as is necessary for the purpose for which it is processed;
f. Personal data will be processed only in accordance with the rights of the data subject;
g. The School, as the Data Controller, will take appropriate technical and organisational measures to ensure that data is secure and to prevent unauthorised or unlawful processing;

h. The School, as the Data Controller, shall not transfer personal data to another country unless it is satisfied that country has adequate levels of data protection for data subjects.

2.2. The School must maintain the trust and confidence of the whole school community and others with whom the School comes into contact. In all circumstances the welfare of students comes first, but the School is mindful of other legal requirements, such as duties owed to visitors, parents, staff and public authorities.

2.3. The School aims never to:

a. hold or use inaccurate or misleading data;
b. keep more data, more categories of data, or keep data for longer than is reasonably required in order to fulfil the 'Purpose' of this Policy;
c. disclose personal data to others except in accordance with this Policy;
d. use personal data to make any automated decision which significantly affects a student, member of staff or parent;
e. sell or transfer any part of its database/s for the purposes of direct marketing.

3. Access to Data

3.1. The Proprietary Board of Directors of the School is responsible for Data Control at the School.

3.2. A request for data held by the school about the individual making the request is termed a Subject Access Request (SAR).

3.3. Individuals are Data Subjects and as such are the 'owner' of the information that is being processed on their behalf by the Data Controller. This is true for all individuals, including children (students).

3.4. Any reasonable request by a student, (if deemed to be of an age and understanding that they can make such a request) parent or member of staff for access to personal data held about him/her/their child by the School should be made in writing to the Head of School at the School address.

3.5. It does not follow that, just because a child has the capacity to make a SAR, they also have capacity to consent to sharing their personal data with others, as they may still not fully understand the implications of doing so. This should be reviewed on a case-by-case basis.

3.6. Parent's making a SAR on behalf of a child should be advised that the child may be deemed to be of an age and understanding whereby consent should be sought. If

so, the consent and express permission of the child will be sought prior to any release of data.

3.7. Express permission should be in the form of a signed consent form.

3.8. If a SAR is made for information containing, in whole or in part, a pupil's 'educational record', a response must be provided within 15 school days.

3.9. 'School days' are days that the School is in usual operation. School holidays and bank holidays are not counted as 'school days'.

3.10. If a fee is levied for providing an educational record, a sliding scale of pence per page is attributed – up to 19 pages equals £1, plus £1 per 10 pages thereafter to a maximum of £50.

3.11. If the SAR does not relate to any information that forms part of the educational record, then the usual 40-day time limit for responding applies.

3.12. If a fee is levied to this kind of SAR, the maximum amount for dealing with the request is £10.

3.13. The School shall not be required to disclose data which is exempt or partially exempt from disclosure. For instance:

a. where applicable, when disclosure of particular data would be likely to cause serious harm to the health of the person requesting disclosure or to someone else;
b. examination scripts within a specific timeframe of the examination;
c. employment references made by the School which remain in the control of the School;
d. planning information relating to staff, if it may be deemed to damage school business to disclose it;
e. when the data is held for national security reasons;
f. if it is in the public interest.

3.14. The School may also withhold medical data if it is held under the professional jurisdiction of the School Doctor/Medical Officer. In those circumstances, the parent, student or member of staff (as appropriate) may be required to contact the School Doctor/Medical Officer direct in order to arrange access to this data.

3.15. Decisions about disclosing third-party information should always be on a case-by-case basis. A blanket policy of withholding it must not be applied.

3.16. For more information please see the latest version of the *Subject Access Code of Practice* published on the Information Commissioner's Office website - www.ico.org.uk.

4. Security

4.1. The School shall do all that it can to ensure that Personal Data is not lost, damaged, or accessed or used without proper authority, and the School shall take appropriate steps to prevent these events happening.

4.2. Paper records which include confidential information shall be kept in a cabinet and/or office which is kept locked when unattended. All paper records should be kept in a secure location.

4.3. Paper records that include safeguarding, child protection and sensitive information relating to safeguarding are kept in a locked cabinet in a locked office

4.4. The School uses an array of measures to protect personal data stored on computers, and internal IT systems including file encryption, anti-virus and security software, user passwords, audit trails, backup systems and 2 factor authentication where required.

4.5. Staff must keep any passwords secure. Staff should be mindful that passwords are not always effective and are not a substitute for encryption.

4.6. Staff should not remove personal data from the School's premises unless it is stored on a password protected computer or memory device.

4.7. All laptops and PCs are secured with the requirement for login and passwords.

4.8. Sensitive information held electronically should be individually password protected as an additional layer of security.

4.9. Persons who process (store or use) personal data on behalf of the School have a responsibility to ensure that the Data Protection Principles are observed and must comply with this Data Protection Policy and any associated record keeping and confidentiality policies.

4.10. Persons who work for and on behalf of the School ('third parties') who may have access to or process personal data in connection with the School should operate in accordance with the Data Protection Act and this policy. Third parties include suppliers or service providers.

5. CCTV

5.1. CCTV at TASIS is operated in accordance with DPA and ICO

5.2. All TASIS Security Guards are qualified to monitor and operate CCTV.

5.3. Specific procedures are in place for the CCTV operator on duty to sign in, log in and report CCTV faults, report to Security Manager any requests of viewing CCTV footage.

5.4. CCTV at TASIS is configured to provide surveillance of:

a. priority Security doors and gates that provide access to critical areas in which school functions are carried out;
b. areas where business critical activity is carried out.

5.5. CCTV provides:

a. Identification of persons entering and leaving the main entrances.
b. Identification of staff entering and leaving the main entrances.
c. Identification of persons moving between the boundary of public and private space.
d. Observation of courier entrances/drop off points.
e. Monitoring of external and internal parking.

5.6. Areas where CCTV surveillance systems are installed are clearly marked by relevant signs advising that such systems are in place.

6. References

6.1. References given by any member of School staff, whether for staff or students, may be given only with the consent of the Head or Deputy Head of School or the HR Manager unless the reference is written by the Head or Deputy Head or HR Manager, in consultation with other staff where appropriate. Any reference will be fair, balanced, reasonable and will be provided in good faith.

6.2. A request for a reference to be provided to an employer or institution overseas will be taken as the applicant's confirmation that the receiving country ensures an adequate level of protection for the rights and freedoms of *data subjects*.

6.3. In exceptional circumstances the Head of School or the HR Manager may agree to provide a written testimonial. It should be noted that this does not constitute a reference or an open reference.

7. Governance

7.1. This Policy is one of several information sharing and information management policies and protocols approved by the Proprietorial Board of Directors and its Sub-Committees.

7.2. This Policy will be reviewed with other information sharing and information management compliance policies within 5 years by the Proprietorial Board of Directors and a designated Sub Committee.

7.3. A 'light touch' review will occur every 12 months to ensure current legislation, regulation and practice are reflected.

7.4. All Senior Managers are responsible to the Proprietorial Board of Directors for ensuring compliance with this Policy.