Data Protection Policy

Name of Unit/Premises/Centre/School	The Toynbee School
Date of Policy Issue/Review	Spring 2022 / Spring 2024
Name of Responsible Manager/Headteacher	Headteacher
Governors' Sub-Committee	Welfare & Guidance

This policy sets out how Toynbee School, the data controller, deals with personal information correctly and securely and in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

The Toynbee School processes personal data about its pupils and is a "data controller" in respect of this for the purposes of the Data Protection Act 1998. It processes this data to:

- support pupils' teaching and learning;
- monitor and report on their progress;
- provide appropriate pastoral care; and
- assess how well the school as a whole is doing.

This data includes contact details, national curriculum assessment results, attendance information, characteristics such as ethnic group, special educational needs and any relevant medical information.

This data may only be used or passed on for specific purposes allowed by law. From time to time the school is required to pass on some of this data to local authorities, the Department for Children, Schools and Families (DCSF), and to agencies that are prescribed by law, such as the qualifications and Curriculum Authority (QCA), Ofsted, the Learning and Skills Council (LSC), the Department of Health (DH), Primary Care Trusts (PCT). All these are data controllers in respect of the data they receive, and are subject to the same legal constraints in how they deal with the data.

Pupils, as data subjects, have certain rights under the Data Protection Act, including a general right to be given access to personal data held about them by any data controller. A parent at the Toynbee School would need to formally request data on behalf of their child in writing.

All matters relating to Data Protection are now subject to the General Data Protection Regulation (GDPR) Policy

The GDPR establishes six principles that must be adhered to at all times. These principles require Personal Data to be:

1. processed lawfully, fairly and in a transparent manner;

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

3. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;

4. accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;

5. kept for no longer than is necessary for the purposes for which it is being processed; and

6. 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.

In addition to complying with the above requirements the School also has to demonstrate that it complies with them and thus shows accountability on the School's part.

DEFINITIONS

Data Breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data Controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

EEA – European Economic Area

ICO – The Information Commissioner's Office, the UK's data protection regulator.

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.

Processing Data – 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, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or other making available, alignment or combination, restriction, erasure or destruction.

Sensitive Personal Data – data revealing ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic or biometric data, data containing health or a person's sex life or sexual orientation.

HOW TO ACCESS DATA

If a parent wishes to access their own personal data, or that of their child, then they will need to contact The Toynbee School in writing where a hard copy can be obtained from the School Office.

The parent's attention is drawn to the Fair Processing/Privacy Notice, which gives supplementary information about the processing of pupil data by the organisations mentioned above, and which gives greater details of how the pupil data is processed, and the rights of parents and pupils. Either can be obtained through the School Office.

RECIPIENTS OF DATA

Personal data will not be disclosed to other third parties without the consent of the parent / legal guardian, unless obliged by law and unless it is in the best interest of the child. If the data subject is aged 16 or over they have permission to request access to their own records. Personal data will therefore be accessed and disclosed as follows:

a) Access:- Restricted staff members of the school will access personal data on a need to know basis in the course of executing their duties. The professional staff requiring such data are fully aware of the obligations the school has under the Data Protection Act, and they will only use the data for the purposes for which it was collected.

b) Disclosure:- The school endeavours to inform students and their parents/legal guardians when there is a possibility that personal data may be disclosed to third parties, and will ask for consent where applicable. However, there are instances where personal data will have to be disclosed without consent to the following third parties:

c) Education Division - to evaluate and develop education policies related to state schools, to enforce the Education Act where required, and to monitor the national educational system.

d) Other schools - where a student is transferred to another school, all academic records and other data related to the welfare and health of the student are forwarded to the other school, for continuation purposes.

e) Examination Authorities – to enable our students to sit examinations as part of the examinations process.

f) Health Authorities – to avoid contagious diseases or epidemics as obliged under health legislation in the interest of public health.

g) Hospitals / Clinics / other medical professional – where a student needs medical treatment due to illness or injuries suffered by him / her. Health inspections are also conducted as part of the health monitoring programme for school children.

h) Police – in cases of criminal investigations and in the interest of law and order.

i) Social workers / Support agencies – where the welfare of the student is not being maintained and in cases of child abuse.

j) Courts – as ordered.

RETENTION OF PERSONAL DATA

The school does not hold any data longer than necessary, having considered the purposes for processing.

In this regard, all personal data relating to students and their parents / legal guardian will be held for the period during which the student attends this school, with the exception of records selected to be kept for historic record purposes, and statistical data. Visual images not selected for historic record purposes will be kept for three years only.

Marks obtained by students in examinations are also kept for the duration of their attendance at this school, with the exception of results of the last scholastic year which are held for a period of five years only. It is therefore very important that all certificates, results and any other record indicating the educational progress of the student, is to be appropriately preserved by the parents / legal guardian for future use by the student.

PRACTICE

In managing and using personal data Toynbee School collects and uses personal data about staff, students, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school is required by law to collect, use and share certain information.

This policy and practice also include past or present and potential members of the groups mentioned above.

In operating this policy the school as the controller has the following responsibilities:

1. To register as a Data Controller, with the Information Commissioner's Office (ICO). Details are available on the ICO website. The Headteacher is the designated Data Protection Officer (DPO). Who can be contacted in writing or via e-mail at admin@Toynbee.hants.sch.uk .

2. Issue a Privacy Notice (previously known as a Fair Processing Notice) to all students and parents – this privacy notice can also be found on the School's website; this summarises the information held on students, the legal basis for processing personal data, why it is held and the other organisations to whom it may be passed on to.

3. Also to issue a privacy notice to all staff.

4. Inform individuals (Data Subjects) when their information is shared, and why and with whom unless the GDPR provides a reason not to do this.

a) Inform Data Subjects of their rights, which are:
b) The right to be informed.
c) The right to access.
d) The right to rectification.
e) The right to erasure (the right to be forgotten).
f) The right to restrict processing.
g) The right to data portability.
h) The right to object.
i) Rights related to automated decision making including profiling.

5. Check the accuracy of the information it holds and reviews it at regular intervals.

6. Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.

7. Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.

8. Ensure that personal information is not retained longer than it is needed and that Data Subjects are informed how long their data will be stored (via the privacy notice on the school's website).

9. Ensure that when information is destroyed that it is done so appropriately and securely.

10. Share personal information with others only when it is legally appropriate to do so.

11. Comply with the duty to respond to requests for access to personal information, known as Subject Access Requests in accordance with the GDPR.

12. Ensure that personal information is not transferred outside the EEA (European Economic Area) without the appropriate safeguards.

13. Ensure all staff and governors are aware of and understand these policies and procedures.

14. Complete data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new systems that change the processes for handling data.

15. Deal with complaints relating to this policy in accordance with the school's complaints policy.

MONITORING

1. The policy will be reviewed at any time in the light of any new changes to national legislation in relation to data protection and any national or local recommendation for improvements to operational procedure as best practice.

2. The Deputy Headteacher shall undertake an annual review of the practice of Guidance and Pupil Services staff to ensure practice is in line with policy.

3. The Bursar shall undertake an annual review of the practice of key HR staff to ensure practice is in line with policy.

4. Annually the Headteacher will report to the governing body on the school's data handling practice and if any concerns have been raised. Serious breaches will be reported to the Chair of Governors immediately and at the next appropriate Full Governing Body meeting.

RELATED POLICIES/PROCEDURES

- Confidentiality Policy & Procedures
- Privacy Notice
- Staff and Pupil ICT Acceptable User Policy
- Manual of Personal Practice (EPS) – Model Code of Conduct
- Safeguarding Policy
- Freedom of Information Policy
- Complaints Policy
- Data Breach Procedure
- Data Subject Access Request Procedure