Data protection policy

Telford Japanese School
Date:5/1/2019

Our school aims to ensure that all personal data collected about staff members, students, parents, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

1. Legislation and guidance

This policy is designed to meet the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. We, however, do not assign Data Protection Officer (DPO) nor register to ICO.

2. Definitions

2.1 "Staff members" within this policy refers to teachers, the Headmaster, the school clerk, governing board members including parents assigned as activity organizers and parents representatives.

2.2 "Students" refers to all children who belongs to Nursery, Primary and Secondary sections of Telford Japanese School.

2.3 "Personal data" means any information relating to an identified, or identifiable, individual. Personal data that we handle includes, but not limited to:

- Name
- Identification number
- Location data
- Contact details
- Online identifier, such as a username
- Name of the organization which the individual belongs to

2.4 "Special categories of personal data" means personal data which is more sensitive and so needs more protection, including information about an individual's:

- Information relating to race or ethnic background
- Information relating to health

2.5 "Processing" refers to anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

2.6 "Data subject" refers to the identified or identifiable individual whose personal data is held or

processed.

2.7 “Data controller” is a person or organisation that determines the purposes and the means of processing of personal data.

2.8 “Personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

3. The data controller

Our school processes personal data relating to parents, students, staff members members, visitors and others, and therefore is a data controller.

4. Roles and responsibilities

This policy applies to all staff members members and to external organisations or individuals working on our behalf.

4.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

4.2 All staff members

Staff members are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the Governing board in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent.
    - If they need to deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

5. Data protection principles

The GDPR is based on data protection principles that our school must comply with. The principles

say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

6. Collecting and processing personal data

6.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 'lawful bases' (legal reasons) to do so:

- The data needs to be processed so that the school can fulfill a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual
- The data needs to be processed so that the school can carry out its intended functions
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

6.2 Special category of personal data

We will only process special category of personal data, if at least one of the following is satisfied.

- If the individual expresses clear consent to the processing of a specific purpose
- When processing is necessary for the purpose of providing preventive or occupational medicine, for the assessment of the working capacity of the employee
- Processing is necessary for public benefit in public health, such as protection from serious threats and health care

6.3 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary. Staff members members must only process personal data where it is necessary in order to do their jobs. When staff members members no longer need the personal data they hold, they must ensure it is deleted or anonymised.

7. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- We need to liaise with Midlands Japanese Association or other schools.
- Embassy, Ministries or other Organizations of Japan need data to provide services or support to our staff members and students.
- Our suppliers or contractors need data to enable us to provide services to our staff members and students – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us
- We may share personal data with other bodies where necessary to do so. We will seek consent before doing this.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation.

8. Subject access requests and other rights of individuals

8.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or the criteria used to determine this period

Subject access requests must be submitted in writing, either by letter, email or fax to the Governing

board. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

8.2 Students and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

8.3 Responding to subject access requests

When responding to requests, we:

- Will respond without delay and within 1 month of receipt of the request, except for school holidays.
- Will provide the information free of charge

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would not meet the best interest of the child
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it.

8.4 Other data protection rights of the individual

Individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data
- Challenge processing which has been justified on the basis of public interest
- Prevent processing that is likely to cause damage or distress

Individuals should submit any request to exercise these rights to the Governing board.

9. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Examples include;

- Outside of school by external agencies such as the newspapers, magazines, and campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

10. Data security and storage

We will protect personal data from unauthorized or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss or destruction.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- On-line storage service may be used only after assessing that the security is fully maintained by the service provider. Password to access on-line storage is regularly updated and shared only between members of staff members memberss who require data processing on daily basis.
- Passwords are used to access school laptops and other electronic devices where the data is stored.
- Encryption software is used to protect removable media, such as USB memory devices. and HDD drives.
- Staff members or students who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

11. Disposal of data

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

12. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. Such breaches in a school context may include, but are not limited to:

- Safeguarding information being made available to an unauthorized person
- The theft of a school laptop containing non-encrypted personal data

13. Training

All staff members are provided with data protection training as part of their induction process.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff members member or data processor must immediately notify the Governing board.
- The Governing board will investigate the report, and determine whether a breach has occurred. To decide, the Governing board will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The Governing board will make all reasonable efforts to contain and minimise the impact of the breach.
- The Governing board will assess the potential consequences, based on the severity and likelihood of potential and actual impact.
- The Governing board will also assess the risk to individuals, again based on the severity and likelihood of impact. If the risk is high, the Governing board will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the representative of Governing board
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The Governing board will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Governing board will document each breach. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- The Governing board will to review what happened and how it can be stopped from happening again.