- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft, and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Set out procedures to ensure the right to object, the right to rectification and the right to be forgotten
- Ensure awareness and understanding of the school's policies and procedures

Staff should contact the DPL 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 they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the UK and 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. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of pupils or staff at risk
- The school needs to liaise with other agencies – it will seek consent as necessary before doing this
- A suppliers or contractors needs data to enable the school to provide services to its staff and pupils – for example, IT companies. The school 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 the German School

The German School will also share personal data with law enforcement and government bodies where it is 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 the German School's safeguarding obligations

- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

In emergency situations that affect any of the school's pupils or staff, personal data may be shared with emergency services and local authorities to help them respond appropriately.

International transfers of personal data only occur where data servers are located outside of the UK and we refer to safeguards provided by Microsoft and the German Foreign Office.

6. Subject access requests and other rights of individuals

Individuals have the right to request access to their personal information held by the school, including the purposes of the data processing, who the data has been or will be shared with, and how long the data will be stored. Requests must be made in writing to the DPL and should include the individual's name, address, contact details, and details of the information requested. Subject access requests for a child must either be made by the child themselves or by a parent or guardian, if the child is considered too young to fully understand the process. The school will respond to requests within one month, but this may be extended to three months for complex or numerous requests. The school may refuse to disclose information in certain circumstances, and if a request is deemed unfounded or excessive, the school may refuse to act on it or charge a reasonable fee. The individual has the right to complain to the ICO.

7. Biometric recognition system

The school uses an automated biometric recognition system, where pupils can pay for cafeteria purchases and other materials using their fingerprints instead of cash. Parents/guardians are notified beforehand and must give written consent for their child's biometric data to be processed. They have the right to opt out of using the system at any time, the school will then not process their biometric data. Members of staff can also use the system to pay and to obtain entry to the school premisses. They must also provide consent to participate, and can withdraw it at any time, with relevant data being deleted.

8. CCTV

The school uses CCTV to increase the safety of the premises, in compliance with the ICO's CCTV-code of practice.
A designated team manages the data, which is only shared in response to security or emergency incidents. The CCTV system is used for preventing, detecting, and investigating crime, ensuring safety, and monitoring site security. The school retains footage no longer than reasonable. Although individuals' consent is not required for CCTV use, the school informs them of its presence and clearly displays signs indicating its use. Concerns regarding the CCTV system can be addressed to the Data Protection Lead.

9. Photographs and videos

The school may take photographs and record images of individuals during school activities, obtaining written consent from parents/guardians or pupils aged 18 and over. Possible uses of photographs and videos include the school's website, notice boards, school magazines, brochures, and social media. Consent may be refused or withdrawn, with the deletion of the photograph or video. The school makes reasonable efforts to protect the privacy of individuals attending public events. The annual yearbook, available for purchase internally, contains class and staff photographs and this is considered within the school's legitimate interests.

10. Data protection by design and default

The school incorporates data protection into all processing operations, including making sure the DPL has the required tools. Processing of personal data is done in compliance with applicable data protection law standards. The school keeps track of all processing activities, and through privacy notices, it provides data subjects with its contact information as well as explanations on how it utilises their personal information.

11. Data security and storage of records

The school endeavours to protect personal data from accidental or unlawful loss, destruction, or damage as well as unauthorized access, alteration, processing, or disclosure. When not in use, paper-based documents and portable electronic devices containing personal data are stored behind locked doors, and papers containing confidential personal data should not be left in public places. To safeguard portable devices and removable media storing personal data, encryption software is used. When sharing personal information with third parties, the school takes all necessary precautions and reasonable measures to ensure that it is stored securely and safeguarded.

12. Obsolete Data

The school requires staff to shred personal data documents on school premises if they are no longer needed. Staff should consult with DPL if unsure. Personal data documents must not be disposed of in recycling or rubbish bins. The school may use a third party to dispose of records and will ensure that the third party complies with data protection law.

13. Duration

An individual's consent to the storage of relevant data by the school is valid until the individual withdraws their consent in writing to DPL.

14. Staff Records

The school keeps personal data of its employees and may share it with linked organizations. If possible, that shall be communicated to the staff. Staff will be informed beforehand if any data is transferred outside the UK and European Economic Area. Members of staff will have the chance to object by getting in touch with the DPL.

15. Enforcement

The school's data, practices, and data protection policy are all subject to inspection by the ICO. The school could face legal repercussions or criminal charges if it does not follow the data protection laws. All personal data breaches should be reported to the DPL so that an internal log can be kept and any patterns identified and acted upon. The DPL will seek legal advice regarding any necessary to inform the ICO and affected data subjects.

16. Personal data breaches

The school shall make all reasonable endeavours to guard against breaches of personal data. The DPL will be informed of any suspected breaches and will notify the ICO as needed within 72 hours. Examples of data breaches may include non-anonymized datasets published on the school website, unauthorized access to safeguarding information, and theft of non-encrypted personal data on school devices.

17. Training

All employees and governors receive data protection training as part of their induction process. In addition, training will be offered as part of ongoing professional development as needed.

18. Monitoring arrangements

This policy will be monitored and reviewed by the DPL, and it will be updated as needed to reflect any modifications to data protection legislation that have an impact on the school's operations. Otherwise, it will be reviewed every 2-3 years.

19. Exclusions

The school's data protection practices for staff recruitment and selection are not covered by this policy.

20. Distribution

This Data Protection Policy is available to all employees, parents, guardians, students, and others whose data is retained. The Data Protection Lead will keep a copy of the policy and it will be posted on the school's website.