KEW COLLEGE PREP

Data Protection Policy

This policy applies to the whole school including the EYFS

The policy is written with due regard to the following:
Data Protection Act 1998
UK General Data Protection Regulation (UK GDPR)
Freedom of Information Act 2000
Department for Education - Data Protection in Schools guidance Feb 2023
Independent Inquiry into Child Sexual Abuse (IICSA)
IRMS Records Management Toolkit for Schools - Feb 2016.
ISBA Guidelines for Independent Schools on the Storage and Retention of Records and Documents – Jun 2017
Guide to the General Data Protection Regulation – Information Commissioner's Office

See also the School's:
CCTV Policy, Privacy Notice, Taking, Storing and Using Images of Pupils Policy

Definitions or abbreviations used in this policy
CCTV: Closed circuit television
Data Controller: The legal entity that decides what data is processed and how
EYFS: Early Years Foundation Stage
UK GDPR: UK General Data Protection Regulation - the legal regulation governing the protection of personal data for all UK citizens (regardless of where the data is being processed)
ICO: Information Commissioner's Office
Personal Data: Personal data covers information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, pupils and their parents, suppliers and marketing and business contacts. It includes expressions of opinion about the individual, any indication of someone else's intentions towards the individual, information necessary for employment such as the worker's name and address and details for payment of salary
Special Category Data: personal data that's considered more sensitive and given greater protection in law: includes information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics (where used for identification purposes), physical or mental health, sex life or sexual orientation
Criminal Offence Data: is personal data that is treated in a similarly sensitive way to special category data. It records criminal convictions and offences or related security measures
The School: Kew College Prep

The School's data processing activities are registered with the ICO as required of a recognised Data Controller.

1. About this Policy

The School collects, stores and uses personal data about a variety of individuals. In this context these individuals are known as data subjects. The School's data subjects include: pupils and former pupils, parents and carers, current and former employees and non-employed staff, governors and trustees, local-authority personnel, volunteers, visitors and applicants.

Everyone has rights regarding the way in which their personal data is handled. During the course of the School's activities it collects, stores and processes personal data about staff, pupils, their parents, suppliers and other third parties, and it is recognised that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

The requirements of this Policy are mandatory for all staff employed by the School and any third party contracted to provide services within the School. Those who are involved in the processing of personal data are obliged to comply with this policy when doing so. Any breach of this policy may result in disciplinary action.

This policy sets out the basis on which the School will process any personal data we collect from data subjects, or which is provided to us by data subjects or other sources. It does not form part of any employee's contract of employment and may be amended at any time.

2. General Statement of the School's Duties

The School is required to process relevant personal data regarding individuals as part of its operation and shall take all reasonable steps to do so in accordance with this Policy. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data.

3. Data Protection Officers

The School does not have a Data Protection Officer, but has appointed two Privacy Officers who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 1998. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Bursar.

4. The Data Protection Principles

All data within the School's control shall be identified as personal, special category or criminal offence data to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

Anyone processing personal data must comply with the seven key principles good practice as documented in the Data Protection Act 1998. These provide that personal data must be: -

- Processed lawfully, fairly and in a transparent manner
- Processed for a specified, explicit and legitimate purpose
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and up to date
- Not kept for longer than necessary for the purposes for which it is processed

- Secure
- Processed with accountability, with measures and records in place to demonstrate compliance

5. Types of personal data processed by the School

Personal data covers both facts and opinions about an individual. The School may process a wide range of personal data about individuals including current, past and prospective pupils and their parents and staff as part of its operation, including, by way of example:

- Identity details
- Contact details
- Bank details and other financial information
- Information about pupil behaviour and attendance
- Assessment and exam results
- Where appropriate, information about individuals' health, and contact details for their next of kin;
- Images of pupils (and occasionally other individuals) engaging in School activities, and images captured by the School's CCTV system (in accordance with the School's CCTV Policy and Taking, Storing and Using Images of Pupils Policy).
- Staff recruitment information
- Staff contracts
- Staff development reviews
- Staff and pupil references

Generally, the School receives personal data from the individual directly (or, in the case of pupils, from parents). However in some cases personal data may be supplied by third parties (for example another School, or other professionals or authorities working with that individual), or collected from publicly available resources.

6. Processing of Personal Data

The School's policy is to process personal data in accordance with the applicable data protection laws as set out above. All staff have a personal responsibility for the practical application of this policy.

Staff should generally not process personal data unless:

- The individual whose details are being processed has consented to this;
- The processing is necessary to perform the School's legal obligations or exercise legal rights, or
- The processing is otherwise in the School's legitimate interests and does not unduly prejudice the individual's privacy.

The School will only process personal data when at least one lawful basis for processing applies. The lawful bases are:

1. Consent - where the individual (or their parent/carer when appropriate) has freely given clear consent
2. Contract - necessary for a contract the school has or will have with the individual concerned

3. Legal obligation - necessary to permit the School to comply with the law
4. Vital interests - necessary to protect an individual's life
5. Public interest - necessary to permit the school to carry out a task in the public interest or its official functions, and that task or function has a clear basis in law
6. Legitimate interest - necessary for the school's or a third party's legitimate interests (provided the individual's rights and freedoms are not overridden)

For special category data there are ten additional conditions. The School will ensure that at least one lawful basis and one condition (which does not have to be linked to the lawful basis) applies. The conditions are:

1. explicit consent – the accessing or processing of this personal data has the written explicit consent of the individual (or their parent/carer, where appropriate)
2. employment, social security or social protection – it is necessary for one of these 3 stated purposes and authorised by law
3. vital interests – it is necessary to protect an individual's life
4. not-for-profit body – it is necessary for the legitimate internal-only purposes of a membership body with a political, philosophical, religious or trade-union aim
5. manifestly made public – it relates to personal data the individual has themselves deliberately made public
6. legal claims or judicial acts – it is necessary for a legal case or required by a court of law
7. substantial public interest – there is a relevant basis in UK law and one of 23 specific public interest conditions has been met
8. health or social care – it is necessary for the provision of healthcare or treatment, or of social care (eg for the assessment of the working capacity of the employee)
9. public health – it is necessary for reasons of public interest
10. archiving, research and statistics – it is necessary for reasons of public interest

When gathering personal data or establishing new data protection activities, staff should, where applicable, ensure that individuals whose data is being processed receive appropriate data protection notices to inform them how the data will be used. There are limited exceptions to this notice requirement. In any case of uncertainty as to whether a notification should be given, staff should contact the Bursar.

7. Special Category Data

The School may, from time to time, be required to process special category data regarding individuals. Special category data is entitled to special protection under the Act, and will only be processed by the School with the explicit consent of the appropriate individual, or as otherwise permitted by the Act.

The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact the Bursar for more information on obtaining consent to process special category data.

Special category data includes: information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics (where used for identification purposes), physical or mental health, sex life or sexual orientation.

The following items are also treated as Special Category Data by the School: safeguarding matters, pupils in receipt of pupil premium, pupils with special educational needs and disability, children in need, children looked after by a local authority.

8. Criminal offence data

Criminal offence data is treated in a similarly sensitive way to special category data. It records criminal convictions and offences or related security matters.

Criminal offence data includes:

- The alleged committing of an offence
- The legal proceedings for an offence that was committed or alleged to have been committed, including sentencing

The School processes criminal offence data in storing the outcome of a DBS check and/or overseas police check on their employees, non-employed staff and volunteers. This data relates to criminal convictions.

9. Accuracy, adequacy, relevance and proportionality

Staff should make sure data processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

Individuals may ask the School to correct personal data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the Bursar.

Staff must ensure that personal data held by the School relating to them is accurate and updated as required. If staff personal details or circumstances change they should update Schoolbase to reflect the change inform the HR manager so that the School's records can be updated.

10. Data Access Requests (Subject Access Requests)

All individuals whose data is held by the School, have a legal right to request access to such data or information. The request should be reasonable and not excessive. The School shall respond to such requests **within one month.** Any individual wishing to access their personal data should put their request in writing to the Head. No charge will be applied to process a reasonable request.

11. Right to be Forgotten

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the School including any data held by contracted processors.

12. Disclosure of Personal data to Third Parties

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent.

- **Other schools:** If a pupil transfers from the School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.
- **Examination authorities**: This may be for registration purposes, to allow the pupils at our School to sit examinations set by external exam bodies.
- **Health authorities**: As obliged under health legislation, the School may pass on information regarding the health of children in the School to monitor and avoid the spread of contagious diseases in the interest of public health.
- **Police and courts**: If a situation arises where a criminal investigation is being carried out the School may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.
- **Social workers and support agencies**: In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.
- **Educational division**: The School may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

13. Use of external providers

As a School some of our processing activity is carried out on our behalf by third parties, such as IT systems, web developers or cloud storage providers. We use several external providers to monitor pupil progress and inform our teaching. This work is always subject to contractual assurances that personal data will be kept securely and only in accordance with the School's specific direction Further details on sharing data with external providers is outlined in the School's Privacy Notice.

14. Photographs and Video

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in the School only.

Images for publication or communication to external sources would not normally include the pupil's name without permission, and the School will seek specific consent from the parent/ guardian, depending on the nature of the image or the use.

It is the School's policy that external parties may not capture images of staff or pupils during such activities without prior consent from the Head.

Parents may capture images of their own children as long as they are taken for personal use only. Parents are asked not to take photographs of other children, except incidentally as part of a group shot, without the prior agreement of that pupil's parents. See ***Taking, Storing and Using Images of Pupils Policy***

Kew College Prep uses CCTV images to reduce crime and monitor the School buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to School property. The School's CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 1998. Recorded CCTV footage will not be retained for longer than is necessary and all retained data will be stored securely.

15. Data Security

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. This is in relation to data belonging to both staff and pupils. As such, no member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Head or Bursar. Where a worker is permitted to take data offsite it will need to be encrypted.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances;
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name;
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers;
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers;
- It is not permitted for staff to use USB sticks or hard drives. Staff can log into the School network from home. Data should not be transferred onto any home or public computers.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

16. Data loss or security breaches

A data breach is a security incident that results in personal data that the School holds being lost or stolen, destroyed without consent, changed without consent, accessed by someone without permission. Data breaches can be deliberate or accidental.

All employees processing data have a duty of care to ensure that it is processed in accordance with this guidance. The School has an obligation to report any major data loss or information security breach to the ICO within 72 hours, where feasible. Therefore **all staff have an obligation to notify the Head without undue delay, and within 72 hours of becoming aware of a major data loss or information security breach**. In addition, staff should notify the Head or Bursar and the Privacy Officers if they suspect a loss of data (electronic or paper) or a security breach as a result of their on-line (internet or email) usage.

One of the Privacy Officers, Bursar or in their absence the Head, will liaise with the Information Commissioner's Office if an information security breach needs to be reported. If an incident is serious enough to justify notification, the Information Commissioner's Office must be informed as soon as is reasonably possible.. It is better to have notified the Information Commissioner before someone makes a complaint to them. A record will be kept of any personal data breaches, regardless of whether they are notified to the ICO.

17. Data Disposal

The Records Manager, who is the person responsible for records management in the School will give guidance for good records management practice so that information will be retrieved easily, appropriately and in a timely way. The Record Management Guidelines, together with the accompanying Record Retention Schedule, will be reviewed on a regular basis. If records are to be kept for longer or shorter periods than laid out in this document the reasons for this need to be documented.

The School will not keep personal data longer than is necessary for the purpose or purposes for which they were collected and will take all reasonable steps to destroy, or erase from its systems, all data which is no longer required.

The School recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data containing personal, special category or criminal offence information held in any form of media (paper or electronic), should be rendered unreadable or unreconstructable. Where a third party disposal expert is used the organisation must provide a Certificate of Destruction.

Disposal of IT assets holding data shall be in compliance with ICO guidance

	Approved by:	**Updated by:**
	Name: Jane Bond	Name: Kim El-baz

	Title:	Head	Title:	Compliance Officer
	Date:	2 Oct 2023	Date:	2 Oct 2023