Data Protection Policy

Executive Summary

The General Data Protection Regulation "Data Protection Law" sets out the principles that should be followed when dealing with information about individuals. This policy reflects these data protection principles and regulates the use of such information.

Introduction

Eastbourne College Incorporated (ECi) operates as Data Controller for St Andrew's Prep and Eastbourne College. Instances of "the School" within this document refer to both schools.

The Eastbournian Society, The Androvian Society and Friends of St Andrew's groups within this document are referred to as "Societies".

The School is committed to protecting the personal data of all individuals with whom we interact, including students, staff, parents, and other members of the school community. We comply with all applicable data protection laws, including the UK General Data Protection Regulation (UK GDPR), which came into effect on May 25, 2018.

It is important that individuals read this policy to ensure they are aware of the nature of the information that the School holds about individuals and reasons why the School needs to process this information, and to ensure they understand their responsibilities when dealing with information about others. Any breach of this policy will be taken seriously and may result in disciplinary action.

This policy must be complied with not only by staff and pupils, but also by individuals working in the School in other capacities, such as consultants, contractors, etc.
The policy impacts on a variety of people and the types of information that the School may be required to handle includes details of (not an exhaustive list):

- current, past, and future pupils
- parents of these pupils
- individual contacts of Suppliers
- individual contacts of Customers
- individual contacts at Local Authorities and other agencies or government departments
- current, past, and prospective staff
- individual donors
- other individuals with whom we communicate

This policy is provided by way of guidance only and does not form part of an individual's contract with the School. The School may issue further guidance or amendments to this policy from time to time and / or in line with legal developments or policy change.

Please note that since the UK formally left the European Union on 1 January 2021, Eastbourne College (Eastbourne College Incorporated) will operate as Data Controller within UK domestic law via the UK Data Protection Act 2018 (the UK DPA). Further information on the UK DPA and UK Data Protection governance can be obtained online at https://ico.org.uk.

Data Collection and Processing

We collect and process personal data for the following purposes:

- enrolling and educating students
- managing and supporting staff
- communicating with parents and other members of the school community
- fulfilling legal and regulatory requirements
- improving our services and operations

We only collect and process the personal data that is necessary for these purposes, and we do so in a fair, transparent, and lawful manner.

Societies (and their constituents) also process data on behalf of Eastbourne College Incorporated (registered charity 307071) including, without limitation, for the following purposes:

- inviting members to social and other events
- putting members in contact with other Society members
- sharing contacts for career opportunities
- contacting members for fund-raising opportunities and donations
- contacting members for contributions to Society publications
- accessing databases to canvass for donations and inviting individuals to fundraising events
- publishing names of donors in Society publications

The School and any person or staff member who processes personal data on behalf of the School, or for the School on behalf of the Societies, shall:

- only process personal data fairly and lawfully
- only process personal data for limited purposes and in an appropriate way, always specifying one or more purposes
- when collecting personal data, then only use that data for the purposes specified
- only collect personal data that is adequate, relevant, and not excessive for the purposes specified
- keep personal data accurate and up to date
- keep personal data only as long as is necessary for the purpose
- process personal data in accordance with the rights of the people who are the subject of the data

- keep the personal data secure and adopt technical and organisational measures to prevent:
    - unauthorised or unlawful processing of personal data
    - accidental loss or destruction of, or damage to, personal data
- not transfer personal data to people or organisations situated in countries without adequate protection

Data Security

We take appropriate technical and organisational measures to protect personal data from unauthorised access, alteration, disclosure, or destruction. We also regularly review and update our security measures to ensure that they remain effective.

Data Retention

We retain personal data for as long as necessary to fulfil the purposes for which it was collected and processed, and as required by law. We have implemented a data retention policy that outlines the specific retention periods for different types of data.

Data Access and Rectification

Individuals have the right to request access to their personal data and to request that it be rectified if it is inaccurate or incomplete. We will respond to such requests within one month, unless the request is particularly complex or we receive a high number of requests, in which case we may take up to two months to respond.

Data Subject Rights

Individuals have the right to:

- request access to their personal data
- request rectification of their personal data
- request erasure of their personal data
- request restriction of processing of their personal data
- object to processing of their personal data
- request the transfer of their personal data (data portability)
- withdraw their consent to the processing of their personal data at any time

Privacy Officer

ECi has appointed a Privacy Officer to oversee our compliance with data protection laws and to act as a point of contact for individuals who have any questions or concerns about their personal data. If you have any questions or concerns about this Data Protection Policy or about the personal data we hold about you, please contact Joseph Burge at jcburge@eastbourne-college.co.uk or +44 (0) 1323 452228

While the Privacy Officer has overall responsibility for ensuring compliance, it is important to note that it is the responsibility of every member of staff / consultant / contractor who processes personal data on behalf of the School, or for the School on behalf of Societies, to comply with the UK GDPR and Data Protection Act 2018 and this policy.

Given the nature of the personal data being processed, the School stresses the importance of compliance by every member of staff / consultant / contractor.

Personal Data

Personal data covers both facts and opinions about an individual. It includes any information which relates to or can identify an individual. It relates to data held on computers or held manually in files.

The School may process a wide range of personal data of pupils, their parents or guardians, staff and others, as part of its operation. This personal data may include (but is not limited to): names and addresses; email addresses; telephone numbers; bank details; donations; academic, discipline, admissions and attendance records; references; photographs; examination scripts and marks; and general employee information.

Processing of Personal Data

The day-to-day working of the School necessarily involves the processing of personal data. The School also needs to collect and use personal data about individuals for a variety of personnel, pupil administration and School management purposes.

These purposes include payment of salary and operation of the payroll system, collection of fees, the provision and administration of staff and pupils, carrying out appraisals, performance reviews, salary reviews and promotion assessments, etc.

Processing of personal data is also required to fulfil our contractual regard to the Parents' Contract and other legal obligations.

The UK GDPR and Data Protection Act 2018 seeks to ensure that the processing of personal data is done fairly and without adversely affecting the rights of the individuals who are the subject of the data. The individuals whose personal information the School processes must be told who the data controller is (in this case Eastbourne College Incorporated), who the data controller's representative is (in this case the Officer), the purpose for which the data is to be processed by the School, and the identities of anyone to whom the data may be disclosed or transferred. This information will generally be provided in the Parents' Contract documentation for personal data of pupils and parents collected on the admission of a pupil and will be provided to staff in their employment contracts and related documentation. However, staff / consultants / contractors need to bear these points of principle in mind for:

- the processing of other personal data
- the provision of new personal data in relation to pupils / parents and staff

- where there is a change to the use of personal data from the purpose(s) indicated when it was first collected by the School
- where the entities with whom it is necessary to share personal data change from when it was first collected by the School

Any information which falls under the definition of personal data, and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with the consent of the appropriate individual or other terms of this policy.

Sensitive Personal Data

The School may, from time to time, be required to process sensitive personal data regarding an individual. Sensitive personal data includes medical information and data relating to sexuality, religion, race, or criminal records and proceedings.

Where sensitive personal data is processed by the School, the explicit consent of the appropriate individual will generally be required in writing.

The School holds information relating to individuals' health such as records of sickness absence and medical certificates (including the School's self-certified Sickness Form and any doctor's certificates). The School may ask an individual to complete a medical questionnaire or undertake a medical examination and will therefore hold and use the resulting medical report. One of the purposes of finding out and keeping this sort of information is to administer and pay benefits related to ill-health such as the School and statutory sick pay, private medical insurance, long term disability schemes and life assurance. This information is needed to monitor and manage sickness absence and to ensure compliance with our obligations under the Disability Discrimination Act 1995 and health and safety legislation.

To enable the School to monitor the effectiveness of its Equal Opportunities Policy, individuals may be asked to complete a form which contains sensitive personal data relating to ethnic origin, age, gender, etc. The responses are analysed on an anonymous basis and are not used for any other purpose.

The School may also record details of union membership (for purposes of deducting fees from salary and for collective consultation), DBS specific information and criminal records.

CCTV

Another form of personal data that the School holds is images recorded on the various CCTV cameras. All CCTV cameras are clearly labelled and are in place for the purpose of crime detection, for the security and welfare of staff and pupils, and for the protection of our working environment. Images are kept for no longer than is necessary to meet this purpose. Further details can be found in the School's CCTV policy document.

Storage of Personal Data

Personnel Files

Most of the types of employee information described above are kept in our personnel files. These files are located in the HR Department and access to the files is limited to staff in the HR Department. The HR Department will only allow other staff to view or copy information in the personnel file if it is essential for them to carry out their duties of employment.

Pupil Files

Parents' and pupils' information is held by data managers in the Headmaster's Office. Prospective parents' and pupils' data is administered by the Registrar.

Some personal data described above may be kept in managers', individual teachers', or Heads of Departments' own filing systems either in addition to, or instead of, being kept in the main personnel files. It is the duty of each manager, teacher or Head of Department to ensure that any personal information is held securely, and that this data protection policy is complied with.

Some personal data of present and past pupils, parents and donors may also be kept in paper filing systems held by the Eastbournian Society or the School Archive. In addition, such personal data may be held in the Eastbournian Society's computer database for its processing of such data on behalf of the School, the Society and its constituents.

Computer Databases and Management Information Systems

Some or all of the types of personal information described above may be kept on a database, in order to facilitate the more efficient keeping and processing of the information.

Access to any such database is limited, and the School puts in place security measures to ensure the confidentiality of the information held on these systems. All security measures are regularly reviewed in line with legal and / or technological developments.

Other Means of Storage

Personal data is also held in other means of storage such as contact details in business cards, mobile telephones, diaries, and paper filing systems.

Accurate and Up-to-Date Information

The School takes steps to keep the personal data it holds accurate and up-to-date. Employees must ensure they inform the relevant data manager if there are any changes to personal details. Managers must also ensure that any personal data held about others is accurate and only stored for as long as is necessary.

Personnel files, pupil and parent records and other personal data relating to staff, pupils and other individuals are kept for a reasonable time after they have left the School employment

or have stopped dealing with the School, as outlined in the Data Retention Policy. The School needs to do this in order to ensure benefits have been properly administered, to give references if requested to do so, to ensure that the School's tax and regulatory obligations have been satisfied and to deal with any tribunal or other court proceedings.

The School will also retain personal information sufficient for fundraising and other charitable purposes. These records may be archived and stored by an external service provider.

The school reviews the periods for which it holds personal data, which are consistent with the principles laid out in the UK GDPR and Data Protection Act 2018.

Transferring Personal Data to Others

The School may make some personal data available to others such as lawyers, accountants, to those providing products or services to the School (such as ICT and other outsourcing providers) and to government and / or regulatory authorities.

Use of Personal Information by the School

With explicit consent, the School will from time to time make use of personal data relating to staff, pupils, and parents / guardians in the following ways:

- to make use of photographic images in School publications and on the School website. However, the School will not publish photographs of individual pupils with their names on the School website.
- for fundraising, marketing or promotional purposes, and to maintain relationships with pupils and parents of the School, including transferring information to any association, society or club set up for the purpose of establishing or maintaining contact with pupils or for fundraising, marketing or promotional purposes. As an example, personal data is transferred by the School to the Eastbournian Society and Androvian Society for the purposes outlined above.

Security

The School will take reasonable steps to ensure that members of staff will only have access to personal data relating to staff, pupils, their parents or guardians or others where it is necessary for them to do so. All staff / consultants / contractors will be made aware of this policy and their duties under the UK GDPR and Data Protection Act 2018. The School will ensure that all personal information is held securely and is not accessible to unauthorised persons.

Security procedures include:

- entry controls. Any stranger seen in entry-controlled areas should be reported.

- secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential).
- methods of disposal. Paper documents should be shredded. Floppy disks, digital storage devices, optical discs etc should be physically destroyed when they are no longer required.

Equipment

Data users should ensure that individual monitors do not show confidential information to passers-by and that they lock their PCs when left unattended. Passwords for PCs should not be shared or transferred to other members of staff.
Any personal data stored digitally must be encrypted or password protected.

Providing Information

Any member of staff dealing with enquiries should be careful about disclosing any personal information held by the School. In particular, they will:

- check the requestor's identity to make sure that information is only given to a person who is entitled to it. Where necessary, they will take the required details of the requestor and return contact once checks are completed; this includes calls from outside agencies such as Children's Services, the police.
- suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
- refer to the Privacy Officer for assistance in difficult situations. No-one should be bullied into disclosing personal information.

Enforcement

If an individual believes that the School has not complied with this policy or acted otherwise than in accordance with the GDPR, they should utilise the School complaints procedure and should also notify the Privacy Officer.

Date of this policy: February 2023
Policy drawn up by: JCB
Date of next policy review: November 2023
Date for publication of revised policy: February 2024