Chaucer College Data Protection Policy

This policy document sets out the expectations of staff for compliance with the GDPR. Any breach of the GDPR by staff may be a matter for disciplinary action and where a criminal offence is committed it will be reported to the appropriate authorities.

Legislation and Guidance

The General Data Protection Regulation (GDPR) replaces the UK Data Protection Act of 1998. Its purpose is to protect the rights and freedoms of living individuals and to ensure that personal data is only ever processed with their knowledge and, where possible, their agreement. This policy meets the requirements of the GDPR and is based on guidance published by the Information Commissioner's Office, the UK's supervisory body for data protection.

Definitions

The following terms are used throughout this and related policies.

Term	Definition
Personal Data	The definition of personal data is wide, it includes any information relating to an identified or identifiable individual. For example, the individual's: • Name or initials • ID number • Username • Location It may also include information specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special Categories of Personal Data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation This data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

Processing	The definition of processing is wide and applies to automated or manual processing, paper-based or electronic. It includes the collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, displaying, disseminating, erasing or destroying of personal data.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Profiling	Any form of automated processing of personal data intended to evaluate an individual. For example, automated grade prediction, lead scoring or employee performance.
Child	Under the GDPR, a child is an individual under the age of 16 years (note that some European countries may choose to adopt 13 years). The processing of the personal data of a child is only lawful if parental or guardian consent has been obtained.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Data Protection Principles

The GDPR is based on data protection principles that Chaucer College must comply with. The principles state 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

This policy sets out how Chaucer College aims to comply with these principles.

Roles and Responsibilities

Chaucer College as Data Controller

In order to ensure compliance, the Chaucer College Board of Directors will delegate responsibility to:

- The Data Protection Officer - to oversee data protection compliance for the company
- Principal - to act as the representative of the Data Controller for Chaucer College
- Senior Management Team - to support the implementation of this policy and continued GDPR compliance in schools
- Department Managers - to support the implementation of this policy and continued GDPR compliance throughout the organisation
- All staff – to comply with this policy in its entirety

The Chaucer College Board of Directors will also ensure that:

- Adequate funding is in place to support this policy
- This policy and all related policies are maintained and updated regularly

Data Protection Officer

The Data Protection Officer will be responsible for:

- Maintaining expert knowledge of data protection law and practices
- Informing the company of their obligations under the GDPR and other data protection laws
- Ensuring data management is strengthened and unified
- Monitoring compliance with the GDPR and other data protection laws
- Overseeing the management of internal data protection activities, ensuring:
    - All data is processed fairly and lawfully
    - Security measures and confidential systems are followed to protect personal data
    - Data is obtained for specific and lawful purposes
    - Data is adequate, relevant and not excessive
    - All personal data is accurate, and that inaccurate data is corrected or erased
    - Procedures are in place to deal with requests for access to personal data
    - Data is not kept longer than is necessary
    - Staff are aware of their rights
    - Staff are aware of their responsibilities
- Ensuring risk and impact assessments are conducted in accordance with ICO guidance
- Reporting data breaches within 72 hours
- Ensuring individuals have greater control over their personal data
- Ensuring procedures are in place to deal with requests for access to personal data
- Ensuring that prior to the processing of an individual's data that:
    - The process is in line with ICO guidance
    - The process is transparent
    - The individual will be notified
    - The notification is written in a form that is understandable to students (where necessary)

    - When sharing an individual's data to a third party that details for the sharing are clearly defined within the notifications
- Sharing an individual's data where it is a legal requirement to provide such information
- Processing all written subject access requests from individuals within 40 days of receiving them
- Having in place formal contracts or service level agreements with data processors, checking that they are GDPR compliant
- Ensuring the secure disposal of redundant data and IT hardware, in compliance with ICO guidance
- Training college personnel
- Conducting audits
- Being the first point of contact for supervisory authorities and for individuals whose data is processed
- Keeping up-to-date documentation
- Updating and maintaining Chaucer College's GDPR documentation
- Periodically reporting to the Senior Management Team and Board of Directors
- Annually reporting to the Board of Directors on the success and development of this policy

Principal

The principal will be responsible for:

- Ensuring the college complies with the GDPR and any related legislation
- Working closely with the Data Protection Officer
- Ensuring that Chaucer College GDPR policies are followed, including that:
    - All data is processed fairly and lawfully
    - Security measures and confidential systems are followed to protect personal data, staff, student and homestay records
    - Data is obtained for specific and lawful purposes
    - Data is adequate, relevant and not excessive
    - All personal data is accurate, and that inaccurate data is corrected or erased
    - Procedures are followed to deal with requests for access to personal data
    - Data is not kept longer than is necessary
    - College personnel are aware of their rights
    - College personnel are aware of their responsibilities
    - Data breaches are reported to the DPO as soon as they take place
    - The DPO is informed of any new agreements with partner organisations, in order to ensure ongoing GDPR compliance
- Ensuring that changes to this policy are identified to staff and followed
- Ensuring guidance, support and training are provided to all staff
- Monitoring the effectiveness of this policy
- Annually reporting to the Board of Directors on the success and development of this policy

Senior Management Team

The College Senior Management Team will be responsible for:

- Assisting in ensuring the school complies with the GDPR and any related legislation
- Working closely with Principal and the Data Protection Officer
- Working closely with their teams to monitor compliance with Chaucer College GDPR policies and procedures to ensure that:
    - All data is processed fairly and lawfully
    - Security measures and confidential systems are used to protect personal data, staff, student and homestay records
    - Data is obtained for specific and lawful purposes
    - Data is adequate, relevant and not excessive
    - All personal data is accurate, and that inaccurate data is corrected or erased
    - Procedures are followed to deal with requests for access to personal data
    - Data is not kept longer than is necessary
    - College personnel are aware of their rights
    - College personnel are aware of their responsibilities
    - Data breaches are reported to the DPO as soon as they take place
    - The DPO is informed of any new agreements with partner organisations, in order to ensure ongoing GDPR compliance

Department Managers

Group senior managers undertake to:

- Assist in ensuring the company complies with the GDPR and any related legislation
- Work closely with the Data Protection Officer
- Work closely with their teams to monitor compliance with Chaucer College GDPR policies and procedures to ensure that:
    - All data is processed fairly and lawfully
    - Security measures and confidential systems are used to protect personal data, staff and student records
    - Data is obtained for specific and lawful purposes
    - Data is adequate, relevant and not excessive
    - All personal data is accurate, and that inaccurate data is corrected or erased
    - Procedures are followed to deal with requests for access to personal data
    - Data is not kept longer than is necessary
    - Company personnel are aware of their rights
    - Company personnel are aware of their responsibilities
    - Data breaches are reported to the DPO as soon as they take place
    - The DPO is informed of any new agreements with partner organisations, in order to ensure ongoing GDPR compliance

Partners

Partners includes, but is not limited to: Universities, Educational Agents, Parents, Homestay Providers, Transfer Companies (i.e. Taxi and Coach services), Security Services, Cleaning Services, Catering Services, Guardian Services, etc.

Chaucer College partners are expected to:

- Be aware of and comply with the GDPR
- Comply with the terms of contracts or service agreements in place with Chaucer College that relate to data protection
- Inform the company or school of any changes to their policies or procedures which may affect the handling or use of personal data
- Inform the company or school of any changes to personal data that Chaucer College holds or processes on their behalf
- Inform the DPO of any data breaches involving data held or processed on Chaucer College's behalf

General Responsibilities

All Staff are responsible for:

- Processing personal data in accordance with this policy
- Informing the school of any changes to their own personal data, such as a change of address
- Contacting the DPO 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 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 planning a new activity that may affect the privacy rights of individuals
- If they enter into a new contract or begin sharing personal data with third parties

The Collection of Personal Data

Chaucer College needs to process the personal data of staff, students and partners. In some cases, there is a legal obligation to process this data. For example, HMRC requires organisations to process staff tax data and the immigration laws require the processing of student attendance data. These are examples of a **legal basis** (or reason) for processing personal data. The GDPR has six legal bases for processing personal data:

1. **Consent** freely given by a data subject to process their data for a specific purpose
2. For the fulfilment of a **contract** between an organisation and a data subject, or because the data subject has asked for specific steps to be taken before entering into a contract
3. In fulfilment of a **legal obligation** (excluding contractual obligations)
4. Because of shared l**egitimate interests**

5. Because it is in the **vital interests** of the data subject, for example in a life-threatening emergency
6. To carry out a **public task** or a task in the **public interest**

Chaucer College will only process personal data where one or more of these legal bases applies. For special categories of personal data, Chaucer College will also ensure that at least one condition for processing is met from Article 9 of the GDPR. Where consent is used as the legal basis and the student is under 16, parental consent will be sought.

Whenever personal data is first collected, the data subject will be informed about its use, specifically they will be informed about:

- What personal information is being collected and processed
- Why the data is being collected
- What the lawful basis for collecting and holding the data is (where applicable)
- Who/which organisations data is shared with and why
- How the data is stored, how long for, and how security is ensured
- How to exercise their right of access to the data
- How to exercise their other rights, such as restricting certain types of processing (for example biometric data) or to rectify data
- Who to contact for queries

Personal data will only be collected for specified, explicit and legitimate reasons and will only be used for those reasons. Details on what data is processed, the reasons for its processing and the legal bases on which that processing is based, are in the privacy notices published alongside this policy document.

The Sharing of Personal Data

Personal data belonging to staff, students and partners is shared routinely for a number of reasons, some of which have been covered in the section on The Collection of Personal Data. Other reasons include, but are not limited to the following scenarios:

- Where there is an issue that puts the safety of a student or member of staff at risk
- Where data is required by third parties in order to provide services to staff and students (e.g. security companies, exam boards)
- When law enforcement agencies require personal data to fulfil their duties under the law
- Where disclosure is required to satisfy safeguarding obligations
- When sharing personal data with the emergency services or local authorities would help them to respond to an emergency situation that affects any staff or students

Full details of who data is shared with are in the privacy notices published alongside this policy document.

Where personal data is shared with third parties, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- 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

Where personal data is transferred outside the UK, it will be done in accordance with the GDPR.

Safeguarding

It is important to note that GDPR does not prevent or limit the sharing of information for the purposes of safeguarding. Fears about sharing information must not be allowed to stand in the way of safeguarding. Information can be shared without consent if to gain consent would create a safeguarding risk.

Rights of the Data Subject

In addition to the right to receive information when we are collecting their data about how we use and process it, individuals may also have the right to:

- Submit a Subject Access Request
- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Full details about how Chaucer College satisfies Data Subjects' rights are available in the associated 'Rights of Data Subjects' policy and procedure documents.

Marketing

Student personal data is used by Chaucer College for marketing purposes. This includes images, videos, testimonials and academic results. Explicit consent is required for this use and it is requested for this specified purpose, usually as part of the induction or onboarding process when students first arrive at school. Where parental consent is required, this will be sought during the application process.

Images may be used in the following ways:

- On college notice boards and in school magazines, newsletters, etc.
- Outside of college by external agencies such as the college photographer, newspapers, campaigns
- Online on the college website or social media pages
- In printed marketing materials, such as brochures and prospectuses

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. If an image is already in circulation in printed format, we will not be able to recall it, but we will ensure that the image will not be included in any future materials. Online images will be withdrawn from use within the time specified in the procedure for responding to objections.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified, unless we have confirmed with the student, parent or carer that they are happy for us to do so, such as in testimonials.

CCTV

We use CCTV in various locations around our college and residential sites to ensure the safety of students, college personnel, equipment, visitors, the school grounds and premises. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the College Principal, who may choose to consult with the DPO, dependent on the nature of the enquiry.

Under no circumstances will Closed Circuit Television (CCTV) be installed in students' toilets, bedrooms or in areas which may be considered intrusive on personal privacy.

Information Security

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records must be kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Laptops, external hard drives and memory sticks that contain personal data must be protected by passwords and encryption
- Where personal information needs to be taken off site, staff must sign it in and out with their line manager
- Passwords that satisfy complexity requirements will be enforced
- Staff, students or partners who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment

Full details about the measures taken to secure personal data are provided in the Information Security Policy.

Retention and 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.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic

files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Full details about the retention and disposal of data, including how long different types of data are kept for, can be found in the Data Retention Policy.

Privacy by Design

Privacy by Design is an approach to developing new processes and systems that promotes privacy and data protection compliance from the start rather than bolting it on after the rest of the system or process has been developed. It is an approach taken in the early stages of initiatives such as:

- Implementing new IT systems that process personal data
- Developing strategies that have privacy implications
- Implementing a new data-sharing arrangement
- Using data for new purposes

By addressing data protection and privacy needs early on, the initiative is more likely to provide a high level of data security for staff, students and partners, with the minimum intrusiveness. Privacy by Design aims to prevent privacy problems from arising and addresses the processing of personal data from initial collection through to secure destruction.

One tool of Privacy by Design is the Privacy Impact Assessment which must be used whenever a new process is introduced that may present a high risk to individuals' interests. PIAs will be triggered and carried out in line with the ICO's recommendations and making use of their approved templates.

Training

GDPR training will be provided for:

- The Data Protection Officer
- College Staff – including Principals and Senior Managers
- Central Marketing, Admissions and Regional Management/ Marketing staff
- Homestay providers
- Interns or volunteers

Contractors or agency staff who have access to personal data are required to demonstrate that they have undergone sufficient training prior to working with the company. If necessary, Chaucer College may provide training to those who cannot demonstrate sufficient training.

It is the responsibility of the DPO to ensure that all training is relevant to those undertaking it and covers the function and role that they fulfil. This should include:

- Chaucer College GDPR Policy and Procedures
- Basic understanding of Data Protection
- Staff rights and responsibilities
- Security measures
- Data handling procedures specific to job role or function
- What to do in the event of a data breach
- Subject Access Requests
- Dealing with complaints

Training will be completed on induction, with regular updates thereafter. It is the responsibility of the DPO to ensure that training updates are provided when necessary, taking into account any updates or changes to legislation or government guidance.

Records of training will be held by the HR Administrator in schools and by line managers for central marketing, admissions and regional managers/ marketing staff.

Monitoring

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated as necessary, and in any case, reviewed annually in line with the Chaucer College annual policy review.