Data Protection Policy and Procedure

Introduction

The Sixth Form College is required to keep and process certain information about its staff students, parents and Governors in accordance with its legal obligations under UK Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18). The College may be required to share personal information about its staff or students with other organisations.

This policy is in place to ensure all employees, volunteers and governors (staff) are aware of their responsibilities and outlines how the College complies with the core principles of data protection legislation.

Organisational methods for keeping data secure are imperative, and The College believes that it is good practice to keep clear practical policies, backed up by written procedures.

Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (DPA 18)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2006
- The School Standards and Framework Act 1998

Applicable data

Personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. Data protection law applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

Sensitive personal data is referred to as ‘special categories of personal data’ and is afforded more protection. This is information relating to:

Race or ethnic origin
Political opinions
Religious or philosophical beliefs
Trade union membership

Genetic data
Biometric ID data
Health data
Sexual life/and or sexual orientation
Criminal data (convictions and offences

Principles

In accordance with legal requirements, personal data will be:

The College complies with data protection legislation guided by the six data protection principles. In summary these require that data is:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Used only for limited, specified stated purposes and not used in any way incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date.
- Not kept for longer than necessary
- Kept safe and secure

The data controllers shall be responsible for, and able to demonstrate, compliance with the principles

Accountability

The College will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.

The College will provide comprehensive, clear and transparent privacy policies.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

The College will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.

- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.
- Data protection impact assessments will be used, where appropriate.

Data protection officer (DPO)

The DPO is responsible for advising the College of its data protection obligations under the law, monitoring compliance and they will:

- Inform and advise the College and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the College's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to Colleges.

The DPO will report to the highest level of management at the College, (The Principal).

The DPO will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

Processing data Lawfully

In order to process personal information, the College must meet one of the legal bases contained within Article 6(1) of the UK GDPR. In order to process special category personal information, the College must also meet one of the legal bases contained within Article 9(2). The legal basis for processing must be determined before the processing commences. The legal basis must also be recorded, for example through a Data Protection Impact Assessment or within the College's suite of Privacy Notices.

The College must therefore determine under which legal basis the data is being processed.

There are six legal bases listed in Article 6(1) of the UK GDPR. These are:

a. Consent: the data subject has given clear consent to process their personal data for a specific purpose

b. Contract: the processing is necessary for a contract the College has with the data subject, or because they have asked the College to take specific steps before entering into a contract

c. Legal Obligation: the processing is necessary to comply with the law

d. Vital Interests: the processing is necessary to protect someone's life

e. Public Task: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the College

f. Legitimate Interests: processing is necessary for the purposes of the legitimate interests pursued by the College or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

Lawful basis for processing special category data

UK GDPR legislation provides additional grounds that need to be met in order to process
special category data (as defined by the UK GDPR). These are

a. Explicit Consent: the data subject has given explicit consent to the processing of special category data for one or more specified purposes

b. Employment, social security and social protection: processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the College or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by UK law
c. Vital Interests of the data subject or another person: processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

d. Not -for -profit bodies - processing is carried out in the course of its legitimate activities with appropriate safeguards.

e. Public Domain: processing relates to personal data which are manifestly made public by the data subject

f. Legal Claims: processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

g. Substantial Public Interest: processing is necessary for reasons of substantial public interest, with a basis in UK law which shall be proportionate to the aim pursued.

h. Health and Social Care: processing is necessary for the purpose of preventative or occupational medicine, for the assessment of the working capacity of an employee.

i. Public Health: processing is necessary for reasons of substantial public interest.

j. Archiving, research and statistics (with a basis in law)

Criminal convictions data

Where the College processes personal data relating to criminal convictions and offences or related security measures, it must do so in accordance with the law and provide appropriate safeguards for the rights and freedoms of data subjects. Schedule 1 of the Data Protection Act 2018 provides further information as to when special category and criminal convictions and offence data can be lawfully processed.

Fair Processing of Personal data

Processing of personal data must always be fair as well as lawful. In general, the College will only handle personal data in ways that people would reasonable expect and will be clear and transparent in its processes.

The College's Privacy notices and data retention policies describe how we will process and use personal data.

All staff should constantly consider not only whether they can but whether they should be using personal data. When sharing data, especially special categories of data staff should ensure the use of the data is appropriate and should consult with the DPO for advice and guidance where necessary

Data Rights

Staff and students have rights protected by UK GDPR legislation as follows:

- to be informed
- of access
- to rectification
- to erasure
- to restrict processing
- to data portability
- to object

(For further information regarding these rights, and how to action them please see Appendix A).

Automated decision making and profiling

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

The College will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

Privacy by design and data protection impact assessments

The College will adopt a privacy by design approach and implement technical and organisational measures which demonstrate how the College has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the College's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the College to identify and minimise the data protection risks involved in projects, processes and activities and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the College's reputation which might otherwise occur.

A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Principal will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the College becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the College will notify those concerned directly.

A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the College, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required to do so may result in a disciplinary procedure.

Data security

The personal data that the College and its staff collect and process must be secured by appropriate technical and organisational measures against accidental loss, destruction or damage and against unauthorised or unlawful processing.

Staff are responsible for ensuring the security of the personal data they process in the performance of their duties and tasks and they must follow procedures and practices that the College has put in place to maintain the security of personal data from collection to destruction. Staff must also take particular care and use practical measures to ensure that data is used and shared appropriately and to relevant organisations/people.

The College has stringent security protocols for both paper and electronic systems i.e. use of two step authentication processes to ensure access to data is secure and all staff are expected to comply with security procedures in place.

The College takes its duties under data protection legislation seriously and any unauthorised disclosure may result in disciplinary action.

The Director of Information Systems is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Publication of information

A publication scheme is available on the college website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

The College will not publish any personal information, including photos, on its website without ensuring that the correct privacy notices are in place.

When uploading information to the College website, staff are considerate of any metadata or deletions, which could be accessed in documents and images on the site.

CCTV and photography

The College understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The College notifies all students, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for six months for security purposes; an Assistant Principal is responsible for keeping the records secure and allowing access.

Data Retention

Data will not be kept for longer than is necessary. Data will be retained in line with data retention schedules.

Some educational records relating to former students or employees of the College may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed if possible, once the data should no longer be retained.

Additional College Policies

This policy will be implemented in conjunction with the following other College policies:

- Freedom of Information Policy
- Internet Acceptable Use policy
- Confidentiality Policy and Protocol
- Electronic Communications policy
- MIS usage Policy
- Social Media policy
- CCTV Policy
- College Code of Conduct

Appendix A

Data Rights

Staff and students have rights protected by UK GDPR legislation as follows:

The right to be informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent and easily accessible.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.

The existence of the data subject's rights, including the right to:

- Withdraw consent at any time.
- Lodge a complaint with a supervisory authority.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

The right of access

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

The College will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the College may impose a ‘reasonable fee’ to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.
In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the College holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the College will ask the individual to specify the information the request is in relation to.

The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the College will inform them of the rectification where possible.

Where appropriate, the College will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the College will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent and consent was the basis for processing
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The College has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the College will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

The right to restrict processing

Individuals have the right to block or suppress the College's processing of personal data in some circumstances.

In the event that processing is restricted, the College will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.
The College will restrict the processing of personal data in the following circumstances:

- Where an individual contest the accuracy of the personal data, processing will be restricted until the College has verified the accuracy of the data.
- Where an individual has objected to the processing and the College is considering whether their legitimate grounds override those of the individual.
- Where processing is unlawful and the individual opposes erasure and requests restriction instead.
- Where the College no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If the personal data in question has been disclosed to third parties, the College will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The College will inform individuals when a restriction on processing has been lifted.

The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means
- Personal data will be provided in a structured, commonly used and machine-readable form.
- The College will provide the information free of charge.
- Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The College is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the College will consider whether providing the information would prejudice the rights of any other individual.

The College will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the College will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to object

The College will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:
An individual's grounds for objecting must relate to his or her particular situation.

The College will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the College can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The College will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The College cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.

Where the processing of personal data is necessary for the performance of a public interest task, the College is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the College will offer a method for individuals to object online.