Godalming College

Data Protection Policy

Learning together for success and progression

Approved by Academy Trust Board: 14th July 2025

Data Protection Policy

Trustee Committee Responsible:	Audit
Nominated Lead Member of Staff:	Joe Yeadon, Data Protection Officer
Status and Review Cycle:	Annual
Current Review:	June 2025
Next Review Date:	June 2026

(unless the Data (Use and Access) (DUA) Bill requires an earlier review)..

Contents

Introduction

The College collects and processes information about people in order to execute its public task of delivering education on behalf of the Government. This information is used to secure funding, assess the performance and safety of the College and its students and staff, recruit and employ staff and appoint Trustees, operate Safeguarding (including Child Protection) procedures, and administer the College as a whole.

The College is registered with the Information Commissioner's Office as a Data Controller. The registration notice outlines how personal data is collected and processed. The College is also subject to the Privacy and Electronic Communications (EC Directive) Regulations 2003, and consideration for this is included in this policy.

While the College is also subject to The Freedom of Information Act 2000, Data Protection is paramount. However, it also has a Duty of Care under the Children Act 2004 and must comply with the Counter-Terrorism and Security Act 2015 and Investigatory Powers Act 2016 and Health and Safety legislation, in relation to its recording and retention of personal information. Furthermore, regulatory documents such as 'Keeping Children Safe in Education' requires data collection about young people within the College, under Section 175 of the Education Act 2002.

The Data Protection Act (2018) controls how personal information is used by organisations. The General Data Protection Regulation (GDPR) requires everyone in the organisation to be responsible for using data in line with key 'principles'.

However, the Data (Use and Access) (DUA) Bill is likely to be passed imminently, which will enact greater protection for the Personal Information of Children. The College will revise this Policy once the Bill is enacted, using appropriate guidance provided by the Information Commissioner.

What is Personal Information?

Personal information is any information associated with an individual living person. For example, a person's date of birth, performance, image, contact or financial details would be considered personal information.

The Principles of the General Data Protection Regulations
Personal information should be:

> *(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');*
>
> *(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');*
>
> *(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data is accurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').[1]

Aims and Objectives

The aim of this Policy is to ensure that any processing of personal data complies with the Data Protection Act and GDPR regulations.

All students, staff and other users are entitled to:

- know what information the College holds about them and why
- know how to gain access to it
- know how to keep it accurate and up to date
- know what the College is doing to comply and demonstrate its obligations under the Data Protection Act (2018)

Furthermore, the College has responsibility to keep those who process personal data informed about Data Protection and their obligations, in the form of training and other guidance.

Personal Information Processing by, and on behalf of the College

The College uses personal information to operate the business of the College, assess the performance of individual students and staff, and statistical cohorts of students with various characteristics. This may include personal information to assure the quality of education of the cohort. In some cases, this analysis may be contracted to companies or organisations. The results of such analysis will be kept in accordance with this policy. Information about visitors may be used to assure the safety of members of the College community.

The College may, seek assistance from companies for specific purposes, such as tracking destinations of students, or providing training to staff. Only the minimum information needed for this purpose will be disclosed and appropriate agreements must be in place to ensure Data Protection.

Similarly, companies or contractors may be engaged to provide technical services or systems which are used for the processing of personal data. Agreements must be in place to ensure that the College's Data Protection polices are upheld.

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ retrieved 26th May 2022

In no case will the College process personal information in a way which is detrimental to the individual. Automated decision-making processes (including the use of Artificial Intelligence) may be used to support human decision making, where they are not unduly detrimental to any individual. No automated process will be used to decide whether an applicant is accepted for a place at College, nor decide their academic programme.

Personal information may not be sold or passed on to any other organisation for financial gain.

Personal information may be passed to the Police or other agencies which are members of the Surrey Crime and Disorder Information Sharing Protocol on receipt of a formal request, with the delegated authority of the Principal. Any request should have a clear purpose in relation to data protection and the remit of the Protocol

Data Protection Privacy Notices

The College will provide all students, staff, trustees and other stakeholders, via a data protection privacy notice, assurance of how their data will be held and processed according to this policy.

Applicants are provided with a data protection privacy notice describing how their information will be used in the course of the Application process, this provides consent for their data to be stored while their application is being completed, in order to facilitate the College assisting with that application.

Before Applicants submit their full and final application they must positively agree to the privacy notice that applies to all Godalming College students, otherwise the application cannot be processed.

The notices also remind staff and students to update the College (normally via Student Reception or the Personnel team), should their personal information change. The College's Personnel department will periodically invite staff to verify their details.

Responsibilities: Staff

In the course of their work staff will often use information about students, colleagues, applicants, alumni, visitors or other data subjects and as such can be described as 'processing personal data' on behalf of the Data Controller.

In this capacity, staff must:

- Only collect or access information which is relevant and necessary to their role, and not attempt to access any information to which they are not entitled
- Ensure any personal data they hold is kept securely to prevent access by others
- Ensure that it is kept in a structured system in order that it can be retrieved if required – wherever possible this should be in the centrally-provided database systems (CIS/Markbook)
- Ensure that personal information is not disclosed, accidentally or otherwise, to any unauthorised third-party, including online services, and Artificial Intelligence tools other than as explicitly approved by the College
- Not create any online post which includes personal information (including images) without explicit written consent
- Destroy personal data once the purpose for which it was collected has passed
- If any suspected or actual breach of data security occurs, it is reported to the Data Protection Officer or Duty Manager

The College has a central database system, , which provides for a secure, encrypted system with appropriate access controls to ensure access is limited to those individuals authorised to access it. This should be used wherever possible, to provide a single, authoritative source of information about student performance and progression.

Information may need to be extracted from CIS for various reasons (such as Trip Contact Sheets, Value Added calculations, references or other records). This must be kept securely, wherever possible, using College online systems such as OneDrive, and destroyed once its use is complete. In any case, the primary record must be maintained in the College's database. Where staff personal devices (BYOD) are used to access College systems, personal information should not be saved to the personal device, and the device must be registered in line with the College's CyberSecurity procedures (CyberEssentials).

Technical controls must be used wherever they are available, such as two-factor authentication, to minimise the risk of data security breach.

Where information is passed to another body or agent of the College for further processing, it must be within the context of this policy.

Responsibilities: Students

Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of personal details are notified to Student Reception who will ensure that these are updated on the CIS system. Students can access their Personal Information via their online portals.[2]

Students are reminded of this policy in the Student Contract.

Responsibilities: The Data Controller

Godalming College is the Data Controller in relation to its activities under the General Data Protection Regulations and subsequent legislation. The Academy Trust is ultimately responsible for the College's compliance and implementation of the Regulations.

The Data Protection Officer reports directly to the Principal for Data Protection matters. This role may be undertaken by a suitable member of staff in the form of an additional duty, providing the line of report is distinct to avoid Conflict of Interest. The role of Data Protection Officer is described in the Data Protection Act 2018.

Responsibility for administering 'subject access' lies ultimately with the Principal, who may delegate that role as appropriate.

All reported suspected breaches of Data Protection will be investigated by the Data Protection Officer, and the Principal will be appropriately notified.

Rights to Access Information

[2] At 01 June 2025, via SELF

Students, staff and other users of the College have the right to access any personal data that is kept about them.

Some records held by the College are subject to the Education Records Section of the Data Protection Act. Therefore the College is likely to refuse the disclosure of information which meets this criteria.

A Data Subject may exercise the right of Subject Access by submitting a request which provides sufficient information to reasonably verify their identity. The Subject's personal information will normally be provided to them in an electronic format.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month, unless there is a good reason for the delay – in this case the Subject Access Controller will inform the data subject of the reason for the delay. Where possible, information will be made available via online portals.

If an individual makes a request which is deemed to be excessive or unfounded (Vexatious), the College reserves the right, in line with the Data Protection Act, to turn down such a request or charge a fee commensurate with the cost, or refuse to provide the information requested. Information may also be withheld if its disclosure is deemed to be detrimental to the Vital Interest of any individual (i.e. there is a risk of death or serious harm), and then only with the authority of the Principal.

Rights to Information being Correct

The College will amend its records as soon as practicable where it has been identified that information is incorrect. This can be done via the College's Administration team or Personnel office.

Right to Erasure

Where individuals have become students, staff or other members of the College, the College is unable to exercise its legal duties unless personal information is retained, as set out in Appendix 2. Clarification about the rights to erasure are set out in the Data Protection Privacy Notices. .
Where the individual has provided their information by consent, such as the College's mailing lists and alumni records, or Open Evening Registration, where there is no associated legal duty, the College will provide the means for the individual to remove themselves from the College's data system.

Subject Consent

All Data Subjects shall be provided with a relevant Data Protection Privacy Notice before they are admitted to the College. Where consent is required, such as the partial completion of an application form for a prospective student, no further processing shall take place until they confirm they have read the Notice. A completed application (for staff, students, Trustees etc) is not subject to consent because it is the public task of the College to process that information once provided.

However, consent must be obtained before information is released to a third-party other than in connection to the College's core business, for example the publication of specific examination results in the media, or the use of a student's image on the College website, social media, or external publication.

Subscribers to the College digital media, or marketing mailing lists may withdraw consent by unsubscribing.

Special Category Information

The College may process Special Category Personal Information about a person's health, disabilities, criminal convictions, family details, race or gender in pursuit of the legitimate interests of the College.

This may include processing 'suitability checks' (such as with the Disclosure and Barring Service) where an individual will be working with young people or vulnerable adults.

The College asks staff and student applicants about their individual health needs, such as allergies to particular medication, or medical conditions which may be relevant where First Aid could be required, Educational Health and Care Plans, or to facilitate Access Arrangements for exams.

The College will only use this information to protect the health and safety of the individual, and support their Teaching and Learning via the Learning Support Manager or Human Resources Manager, as appropriate.

Trustees do not normally have access to personal information, except in relation to specific staffing or legal matters. In such cases, the personal information will be treated under the terms of reference for the relevant committee or remit in relation to a particular College policy.

Police and Local Authority Access to Personal Information

Personal information about an individual may be disclosed to the Police when an officer has formally requested particular information as part of the data sharing agreement. Normally this request will be made in writing – but it is at the College's discretion to assist the Police where a student's wellbeing is at risk. Any such request should be processed by the Head of Administration, a member of the Senior Management Team, or the Data Protection Officer.

No *Special Category* information (as defined by the Data Protection Act) may be disclosed unless there is a documented reason and only with the specific authority of the Principal.

The College has a legal duty under the Children Act (2004) to inform the Local Authority where a child's welfare is at risk. Where the Data Subject is under 18, the College does not require consent to inform the Local Authority where it has concerns. However, wherever possible, the Data Subject will be properly informed of the process, according to the College's Safeguarding Policy.

The Local Authority also has a legal duty under the Education and Skills Act 2008 to monitor the participation of young people in education – the College may provide personal information for this purpose.

Artificial Intelligence

Artificial Intelligence (AI) is becoming increasingly used to generate content and aid productivity. However, AI learns how to respond to inputs through learning from previous use, and the information to which is has access. This in turn means that exposing personal data to AI can constitute a Data Security Breach, as the personal information has become part of the pool of information available to the AI tool.

Similarly, an imperfectly trained AI tool could provide inaccurate results when performing a process using personal data. This inaccuracy would, in itself, constitute a breach of the Data Protection Act.

This makes the use of AI a high risk activity. Therefore any use of AI in College should be subject to a Data Protection Impact Assessment, and approved by the Principal.

Online Meetings and Online Chat

Online meetings have the capability to be automatically recorded and often this means they can be automatically transcribed. This also means that any personal data mentioned in the meeting becomes part of the record, and is subject to Subject Access Request, of the person being discussed. The same applies to online chat – it is retrievable and therefore subject to SAR. Participants should be mindful to only discuss personal data where it is necessary.

Consent should be obtained before recording any online meeting, or inform participants that meetings will be recorded so they can choose not to participate. Meeting hosts should inform participants to that any personal information discussed in the meeting may be recorded, and therefore should be avoided unless necessary.

College Archives

The College holds an archive of people and activities (such as publications, photographs etc) which are of historical value, in the Public Interest. These are kept in relation to the College's Public Task to document the history of the College and education in the local area, for historical research, and

academic study. No Special Category information is archived, unless that information is in the public domain. Requests to access the College Archive are assessed individually by the Data Protection Officer.

College archives shall be maintained following the School Archives and Records Association and British Library guidelines.[3]

CCTV Images and Monitoring

The College site has a CCTV system to prevent and detect behaviour which is in breach of the Staff or Student Contract, detect crime, to monitor the Health and Safety of people on the College campus, and to safeguard young people. Monitoring systems may be used to detect activities such as vaping, and this may be linked to CCTV systems.

The College may use software to automatically identify individuals using biometric data, for example to track an intruder on the campus. Where a person becomes identified using such software, the images shall become part of that person's record, but is otherwise unstructured data. CCTV images must be kept securely, and encrypted.

Direct access to live CCTV images is restricted only to Security staff[4] and the Director of Estates. The Security staff may release CCTV images to the Safeguarding Team in order to investigate alleged breaches of College policy. Images may not be further shared without the authority (delegated or otherwise) of the Principal. Images may be stored for up to 30 days, except where an incident has been detected where video clips or snapshots may be kept until the proceedings of any incident have been concluded.

Where an incident has been recorded, and individual people have been identified within the CCTV images, they will form part of the personal information of those identified, and therefore is subject to Subject Access. Images will only be released as part of a Subject Access Request, where no other identifiable person is within the image, or can be reasonably redacted to protect the rights of other people.

Where a crime has been alleged to have been committed, the College may release images to the Police as part of their investigation (see above).

High risk activity – Data Protection Impact Assessments

Any activity involving personal information, and either uses new technologies or presents a high risk to the rights and freedoms of individuals, is subject to a Data Protection Impact Assessment. This includes any new process where personal information is passed onto a 3rd party for further processing.

Any member of the College wishing to conduct such activity should consult the Data Protection Officer to determine whether a DPIA needs to be completed. Where a DPIA is completed, it shall be performed according to relevant guidance in place.

Retention of Data

[3] School Archives & Records Association | Home Page

[4] College IT staff have access for the purpose of administering the technical systems, but only when acting as a Systems Administrator.

The College keeps different types of information for differing lengths of time, depending on legal, academic and operational requirements in keeping with the purpose of the data when it was collected. The schedule of retention is available on request from the College, or shown in Appendix 3.

Compliance

All staff, students, trustees, visiting or associate staff, contractors and other members of the College are required to comply with this Policy, and Data Protection will be included in new policies and systems by design.

Any breach of the Data Protection Policy may lead to disciplinary, and where appropriate, legal proceedings. Any questions or concerns about the interpretation or operation of this policy should be addressed to the Data Protection Officer, in the first instance.

Any *suspected* Data Security Breach should be reported immediately to the Data Protection Officer who will evaluate whether a Breach has taken place. In the case of a Breach, it will be reported to the Information Commissioner in line with the relevant regulations in place. This currently requires reporting any breach to the ICO within 72 hours of notification, thus investigations should take place in advance of this deadline. In the absence of the Data Protection Officer, the College Duty Manager shall take the appropriate action.

Appendix 1: Data Protection Impact Assessment Form

<table>
<tr><td>Name of proposer</td><td></td></tr>
<tr><td>Title of project or proposal</td><td></td></tr>
<tr><td>Summary of proposed Data Process.</td><td></td></tr>
<tr><td>Who is affected by this process, and how will their information be used? Include details of any transfer to any 3rd party, and how long the information will be retained</td><td></td></tr>
<tr><td>Explain the steps taken to identify the risks to data security and privacy. Include details of any consultation.</td><td></td></tr>
<tr><td>List the risks identified above</td><td><table><tr><td>Risk</td><td>Impact</td><td>Likelihood</td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></table></td></tr>
<tr><td>List the actions which will be taken to reduce the risks (mitigation).</td><td><table><tr><td>Risk</td><td>Solution</td><td>Result</td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></table></td></tr>
<tr><td>Describe the approval process for this project. Include relevant committees if appropriate</td><td></td></tr>
<tr><td>Data Protection Impact Assessment accepted:</td><td><table><tr><td></td><td>Name</td><td>Signature and date</td></tr><tr><td>Project proposer</td><td></td><td></td></tr><tr><td>Project Sponsor (SLT)</td><td></td><td></td></tr><tr><td>Data Protection Officer</td><td></td><td></td></tr></table></td></tr>
</table>

Appendix 2: – Data Protection Privacy Notices

Data Protection Privacy Notice – Staff (including Applicants and Volunteers) and Trustees

Godalming College is a 16-19 Academy Trust, specialising in Sixth Form education. The purposes for which the College collects and processes personal data is notified and registered with the Information Commissioner's Office (ICO), under the Data Protection Act 2018.

Your data and privacy is of upmost importance to us. We are committed to keeping your personal data safe. We will prompt you, at least once a year, to ensure that the personal data we have is up to date.

How we use your personal information

The College will collect, store and process your personal data only for the Legitimate Interest of administering the College, and the execution of the College's Public Task of providing education on behalf of the Government. This includes what you disclose on your application, at interview and what is learnt about you afterwards as a staff member, trustee or volunteer.

The College requires certain information about you in order to administer your position as a member of staff, or application to be a member of staff, trustee or volunteer at the College.

In particular the College will collect and process:

- Your contact details, any information you provide on your application including previous employer details, and the results of any reference request in order to administer the appointment process
- Certain classes of special category personal information only for the purposes of statistical monitoring of Equality and Diversity of the workforce
- Information relevant to 'Keeping Children Safe in Education', School Staffing Regulations (2013), or 'Section 128' checks relevant to your role

This information will only be kept for 6 months after the interview date for applicants who are not appointed.

For members of staff and trustees, the information that we may collect are as follows:

- **Basic personal details** such as your name, initial, date of birth, position held and ID image
- **Personnel information** such as your contact details, gender, nationality, attendance records, proof of ID and qualifications, training and professional review records, education and employment history, information needed to perform your DBS check, and medical records where they relate to your attendance at College, and to monitor the College's performance on equality
- **Financial information** such as salary records, bank details, income tax and NI records and pension records, Insurance and other details needed to operate the Payroll service
- Your image, and car registration details, in order to operate the College ID Card system, and enable members of the College to identify you or your vehicle as a member of staff
- Information about your use of the **Cashless Catering** system
- Information about your performance in relation to your employment in your role.
- **Health and Safety records** relating to the COSHH regulations (use of chemicals)
- **Marketing Information** including photos of you and information about your time at the College, your consent will be sought separately

- If you take part in **Trips and Visits** we may collect information such as your passport details, additional medical information and details of your travel insurance
- CCTV footage will be captured of you when you are on the College campus, which may be linked to other monitoring systems (such as vape detection). The College is equipped with a CCTV system for the purpose of the security, **monitoring Health and Safety,** safeguarding of College members and visitors, and the detection of crime. The CCTV images will not be used for any other purpose.

We may share your information with the following third parties:

- The College's appointed Payroll provider, and Pension services
- Disclosure and Barring service and other regulatory agencies
- Organisations that provide and administer the pension schemes
- The S7 Consortium and other training providers where you may be asked to participate
- Occupational Health Provider
- Credit Reference Agencies who have made an enquiry on your behalf
- Future employers in respect of references where you have given consent

Third parties acting on our behalf include:

- IT services – Microsoft, online teaching services and companies that provide online resources
- Auditors, acting on behalf of the Board of Trustees or ESFA
- Courts, law enforcement agencies and other emergency services as necessary to comply with a legal requirement, for the administration of justice, to protect Vital Interest (to prevent death or serious harm), to protect the security or integrity of College operations, and to detect, investigate or prevent crime
- Travel agents, airlines and other companies with which you have engaged with to organise a College Trip

Access to your information

You have a right to request the information we hold about you. The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month, unless there is a good reason for the delay – in this case you will be informed about the reason for the delay.

If an individual makes a request which is deemed to be excessive or unfounded, the College may charge a fee commensurate with the cost, or refuse to provide the information requested. Information may be withheld, with the authorisation of the Principal, where it is detrimental to the Vital Interest (i.e. there is a risk of death or serious harm) of any individual.

Transferring your data

Any data that is shared will be subject to the Data Protection Act (2018).

We may provide your information to the police, medical personnel or any other official where we believe it is in your Vital Interest (i.e. to prevent death or serious harm), or in that of others, and that to withhold it would be detrimental.

Correcting mistakes

You have the right to request we update any information we hold about you if you think it is incorrect, incomplete or out of date. If we believe the information we hold about you is correct we may refuse to update our records but we will note your objection.

Objecting to how we process your data
We have a Legitimate Interest in processing your personal information in relation to the Public Task of the College business. You have the right to object, on grounds relating to your particular situation, to us processing your personal data where you feel the processing has a disproportionate impact on your rights and is in excess of this legal basis.

Automated processing
We may use automated processing (including AI) to assist human decision-making. Any automated processing will be subject to a Data Protection Impact Assessment.

The right to be forgotten
You can ask us to erase your personal data in the following situations:

- The data is no longer necessary in relation to the purpose for which it was originally collected
- You have objected to us processing the data and there is no overriding legitimate interest for us to continue the processing
- Your personal data was unlawfully processed
- Your personal data has to be erased in order to comply with a legal obligation

We may in some circumstances refuse to erase your personal data. If we do this we will explain why and the legal reason for doing so.

Your rights
If you have any questions or queries about the information we hold about you, and how we use it, you can either speak to your Line Manager, Clerk of the Academy Trust, or Personnel. Or you can address your concerns to the College's Data Protection Officer. They can be contacted via email: dpo@godalming.ac.uk

If you feel your question or complaint has not been addressed to your satisfaction, you can contact the Information Commissioner's office:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF
https://ico.org.uk/

This statement will be subject to regular review and will be updated accordingly.

Data Protection Privacy Notice – Students

How will we use your personal information?
Godalming College is a 16-19 Academy Trust which delivers education on behalf of the Government (called a Public Task). The College is registered with the Information Commissioner's Office (ICO). Your data and privacy is of upmost importance to us and we are committed to keep your personal data safe. This notice will help you to understand how we collect, use and process your personal data. You may wish to show this to your parents/carers to help you fully understand it. You must seek their permission before providing their details to us, to be added to your records.

In order to administer your place at Godalming College, we collect information from you and about you in various ways, including via your original application as well as from your school, references, enrolment and interviews, attendance data, financial transactions (such as trip payments), the CCTV system, University and College Admissions Service (UCAS), exam boards, and interaction with your teachers, parents, and tutors at College. The College has strict policies on what information we hold, how it can be used, and when it must be destroyed. You can see your own personal information via College online systems, or by speaking to your Senior Tutor.

The information we hold about you may include 'Special Category' information, such as learning needs in order to provide support for your learning and administer special exam arrangements, or ethnicity, gender or health for the purpose of monitoring the Equality and Diversity of the College as a whole. This information will be kept especially carefully and accessible only to those specifically authorised.

If you use the College Cashless Catering system, we will record details about how you use it in order to administer the catering service.

We will use your information to communicate with you and your parents to inform about your progress and attendance. This is the normal operation of College systems designed to ensure you perform to your potential. If you have concerns about this, you should contact your Senior Tutor.

Your information will be passed to various Government and other agencies including the Department for Education and its related agencies, Learner Records Service, Examination Boards, UCAS, as well as organisations such as those which provide results and performance analysis for the College. It is the legal duty of the College to communicate with these agencies in the execution of its Public Task.

In some specific circumstances, it may be necessary to perform a criminal records check with the Disclosure and Barring Service, such as where you apply to perform work experience that involves working with children.
The school you attended before enrolling at the College, along with your Local Authority, has a duty to monitor the progression of its pupils after Year 11; we may inform them that you have applied and the progress of your application – up to and including your final exam results and your destination after College (e.g. university). This information will not be released to the public without your consent.

Your school is required to provide us with any safeguarding, or information held under The Prevent Duty, they hold about you, and similarly we are required to pass on any safeguarding information to any institution you attend should you leave the College before your 18th birthday.

All these organisations have their own Data Protection policies, and are all regulated and monitored by the Information Commissioner's office.

We will treat your personal information with respect: it will only be available to authorised people and organisations, not used for commercial gain and will be destroyed when it is no longer needed. Unauthorised access (or attempts to access) of personal data contravene the College's Data Protection Policy. For more information about Data Protection and how long we keep your data, please consult the College Data Protection Policy, which is available on the website.

We may provide your information to the police, medical personnel or any other official where we believe it is in your Vital Interest (i.e. there is a risk of death or serious harm), or in that of others, and that to withhold it would be detrimental.

Publicity
We will not disclose your personal information for publicity purposes without your express permission (consent).

Alumni
Separately from your official 'Destination' (which is required to perform the College's Legal Duty), when you leave College, you may be invited to join the College Alumni programme, which is intended to keep you abreast of developments at College, track your progress, and invite you to participate in helping future students.

Joining the Alumni programme is with your consent, your information will not be shared outside the College or used for publicity without your express permission. You may remove your consent and ask for your information to be corrected, or erased.

Correcting mistakes
You have the right to request we update any information we hold about you if you think it is incorrect, incomplete or out of date, and we ask you to inform us if any of your personal information changes. If we believe the information we hold about you is correct we may refuse to update our records but we will note your objection.

You can see the information we hold about you via the relevant online portal or by speaking to your Personal Tutor in the first instance.

Objecting to how we process your data
The College performs a Public Task on behalf of the Government, and therefore has a Legal Obligation to process your information and therefore retain it in accordance with our policies. You have the right to object, on grounds relating to your particular situation, to us processing your personal data where you feel the processing has a disproportionate impact on your rights.

Further information can be found:

- Information Commissioner's Office - www.ico.gov.uk

Complaints
If you have any questions or queries about the information we hold about you, and how we use it, you can speak to your Personal Tutor the first instance. If you still have concerns please address them to the College's Data Protection Officer. They can be contacted via email: dpo@godalming.ac.uk

If you feel your question or complaint has not been addressed to your satisfaction, you can contact the Information Commissioner's office:
Information Commissioner's Office
Wycliffe House
Water Lane

Wilmslow
SK9 5AF

https://ico.org.uk/

This statement will be subject to regular review and will be updated accordingly.

Data Protection Privacy Notice – Discovery Course Students

The College runs 'Discovery Courses' for students in Year 10, in order to provide an experience learning about topics not normally included in the 11-16 school curriculum.

When you provide us with your personal information, you consent for us to use it to enable us to provide you with a place on your chosen course.

Your information will be processed to administer your participation in the programme, in coordination with your school. Both your school, and the College, may link your participation to your records in order to track the success of the programme, and shape the provision for future students. We will retain the information that you have attended for Safeguarding purposes.

Your participation in the 'Discovery Course' programme will not be used as part of the applications process in any way, should you choose to apply for a place in the College for year Y12.

Complaints
If you have any questions or queries about the information we hold about you, and how we use it, you can speak to your College teacher or Schools Liaison Coordinator in the first instance. If you still have concerns please address them to the College's Data Protection Officer. They can be contacted via email: dpo@godalming.ac.uk

If you feel your question or complaint has not been addressed to your satisfaction, you can contact the Information Commissioner's office:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

Data Protection Privacy Notice – Parents/Carers

How will we use your personal information?
Godalming College is a 16-19 Academy Trust and is registered with the Information Commissioner's Office (ICO). Your data and privacy is of upmost importance to us and we are committed to keep your personal data safe.

We have been provided your details by a student or applicant in relation to their application to study at Godalming College. They have given your details as their nominated parent or carer, with whom we will communicate to support their studies. The student has been provided with a separate statement that you might wish to discuss with them. This includes information relating to how we will share their information with you. The student may amend their authorised contacts, subject to a safeguarding review.

In the course of the students' studies, we will collect information about you through the application and enrolment process, the Parents' Portal, correspondence, and the record of payments you have made to the College. This will be used to support the student's academic progress. We do not retain credit/debit card details.

We will keep you informed of the students' progress, and of activities at the College which may be relevant to their current or future studies, such as extra-curricular activities, trips, useful resources etc. We will provide access for you to the 'Parents' Portal', via which you can monitor attendance, timetables, and performance information provided by teachers.

You have the right to confirm what data we hold about you, but parents and carers are not entitled to make a subject access request for data on behalf a student.

Correcting mistakes
You have the right to request we update any information we hold about you if you think it is incorrect, incomplete or out of date. If we believe the information we hold about you is correct we may refuse to update our records but we will note your objection.

Objecting to how we process your data
The College performs a Public Task in providing education on behalf of the Government, it is in performing this role that we collect and process your information. We are required to maintain emergency contact details provided by the student.

If you wish to be removed from our database, we will delete your contact information and cease communication with you. Should you subsequently wish to resume contact with the College in relation to a particular student, the student should make this request via Student Reception.

We are unable to provide information about any student unless the student has provided your details as their parent or carer. For more information about Data Protection and how long we keep your data, please consult the College Data Protection Policy, which is available on the website.

Withdrawing consent
We do not rely on consent as a lawful basis for processing any of your information. If you choose not to give us your personal information, it may delay or prevent us from providing information relating to your student's education.

We may in some circumstances refuse to erase your personal data. If we do this we will explain why and the legal reason for doing so.

Further information can be found:

- Information Commissioner's Office - www.ico.gov.uk

Questions and Complaints
If you have any questions or queries about the information we hold about you, and how we use it, the please contact the College's Data Protection Officer. They can be contacted via email: dpo@godalming.ac.uk

If you feel your question or complaint has not been addressed to your satisfaction, you can contact the Information Commissioner's office:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

https://ico.org.uk/

This statement will be subject to regular review and will be updated accordingly.

Online Applications: Privacy Statement
Information you enter into the Godalming College Online Application system will be stored securely in order to facilitate the completion of your application. You should obtain the permission of your parents to provide us with their contact details before entering them on the online form. Prior to submitting your application your information will be used only for the purposes of monitoring statistics and assisting you should you ask for help, and for you to retrieve you application details.

We may contact you to offer assistance, but will not use the information for marketing.

The Online Application information will be kept for 2 years before it is deleted from our database, you can view your information at any time before this by logging into the system. If you wish for your information to be deleted before this time, please contact the College Admissions Officer.

When you have completed the form, but before you submit your application, you will be asked to read the full 'Privacy Statement for Students' and confirm that you understand it. This notice explains how we will manage your personal data once you have applied, including our legal duties to other organisations. We will not be able to process your application unless you confirm that you have read and understood this.

If you have any questions about this, or how we will use any information you provide to us, you can contact the College's Data Protection Officer dpo@godalming.ac.uk. A copy of the College Data Protection Policy can be found on the College website.

Data Protection Privacy Notice – Visitors
All visitors to the College are required to sign-in, providing the name of their host, and their vehicle registration number. Visitors will be signposted to the notice posted in the signing-in area regarding the purpose of this data collection. This information is only available to the Administration Team and site security staff, unless a concern has been raised where it may be used in the course of investigation.

This information is required in order to fulfil the College's Legal Duty with regard to the Safeguarding of Young People, and the duty of care to the individual, and will be kept for a maximum of one year, unless an incident is reported under these regulations.

The College has a campus-wide CCTV system, the image of visitors will be recorded for the purpose of the detection security and safeguarding of College members and visitors, and the detection of crime.

Data Protection Privacy Notice – Lettings
Personal Information provided in relation to the letting of any College facility outside of its normal operating hours will be stored by the Estates Manager, and only used in relation to the operation of the booking.

These details will serve as the point-of-contact for the purpose of Safeguarding of Young People and the Duty of Care in relation to the use of the facility and will be retained for one year after the last booking using these details.

Financial records pertaining to external bookings will be retained in accordance with current tax guidance, which is normally 7 years after the end of the relevant financial year.

The College has a campus-wide CCTV system, the image of visitors will be recorded for the purpose of the security and safeguarding of College members and visitors, and the detection of crime.

Data Protection Privacy Notice – Open Evening Visitors

All visitors to College Open Evenings are asked to register in advance, including the name of the potential student, subject interest, and your contact details. We require registration in order to manage the number of people on the College campus throughout the evening. When you arrive, we will record that you have arrived. We will retain this information for three years, in order to measure the success of the Open Evening.

Should you apply to be a student at the College, we will link that you attended Open Evening in order to monitor the success of the Open Evening and identify that you have visited the College and whether we have catered for your interests, but the information as to your attendance will not be used in any way to influence the application process.

The College has a campus-wide CCTV system, the image of visitors will be recorded for the purpose of the detection security and safeguarding of College members and visitors, and the detection of crime.

If you have any questions about this, or how we will use any information you provide to us, you can contact the College's Data Protection Officer dpo@godalming.ac.uk. A copy of the College Data Protection Policy can be found on the College website.

Godalming College

Appendix 3: – Data Retention Schedule (Summary)

Type of Record	Retention Period	Reason
Staff Records		
Personnel records inc. wages/salary records. Staff record of an investigation where concerns were raised about their behaviour around children (even if proven unfounded) and is not malicious	7 years from the end of employment (unless redundancy is involved, see below), or until required for the purpose of administering the College pension provision (whichever is later) Until the retirement age of the individual, or 10 years, whichever is longest.	Provision of references and limitation period for litigation. Taxes Management Act 1970 Management of the College's pension provision Safeguarding[5]
Staff record of an investigation where the allegation is malicious	Not retained	
Staff application form and interview notes	6 months from date of interview date for unsuccessful candidates. Application form retained with Personnel file for successful application.	Limitation period for litigation
Facts relating to redundancies	7 years from date of redundancies	Limitation period for litigation
Accident records	3 years after Academic year to which the records relate	Management of Health and Safety
Records arising from health surveillance (HSE), or where a member of staff is suspected of exposure to a regulated substance	40 years in the case of exposure to carcinogens or other defined substances, otherwise 7 years after the end of employment.	COSHH regulations[6]
Trustee Records, including contract details, register of interest etc	7 years after the end of the engagement	Provision of limitation and litigation
Student Records		
Student Files, Performance Data, References etc Virtual Learning Environment records Computer usage logs/internet history Catering records	6 years from the end of the Academic Year to which the records relate Within the current academic year only One year 3 months after leaving College	Subject Access, Job/Education references. Audit evidence for funding and performance data. Operation of online learning environment To ensure the College can comply with Prevent legislation To manage the catering service
Records of counselling records held on the College site	These records are not retained	Not relevant
Basic student information sufficient only to confirm whether a student attended the College.	10 years from the end of the Academic Year to which the records relate – in electronic form only.	Provision of limited references for ex-students.
Personal Information relating to a student where a Safeguarding concern has been raised	Until the academic year following the individual's 25th Birthday or 6 years after the latest contact with the student, whichever is the latest	Sector guidelines, based on Children Act 2004.
CCTV images	30 days unless a specific incident has occurred or the images have been identified as evidence for police intervention.	Investigation of alleged or suspected criminal activity or investigation of behaviour by students which contravenes policies relating to student behaviour

[5] Child protection records retention and storage guidance | NSPCC Learning – retrieved 07 June 2021

[6] Control of substances hazardous to health (COSHH). The Control of Substances Hazardous to Health Regulations 2002 (as amended). Approved Code of Practice and guidance L5 (hse.gov.uk) – retrieved 07 June 2021