

# Data Protection Policy

**Learning together for success and progression**

*Approved by Academy Trust Board: 6<sup>th</sup> July, 2020*

# Data Protection Policy

Trustee Committee Responsible:	Audit
Nominated Lead Member of Staff:	Joe Yeadon, Head of ILT Services
Status and Review Cycle:	Annual
Current Review:	June 2020
Next Review Date:	June 2021

**Contents**

Introduction.....	4
What is Personal Information?.....	4
The Principles of the General Data Protection Regulations.....	4
Data Protection Privacy Notice .....	6
Responsibilities: Students .....	7
Rights to Information being Correct.....	7
Right to Erasure .....	8
Subject Consent.....	8
Sensitive Information .....	8
Police and Local Authority Access to Personal Information.....	8
CCTV images .....	9
High risk activity – Data Protection Impact Assessments .....	9
Retention of Data .....	9
Compliance .....	9
Complaints.....	10
Appendix 1: Transitional Arrangements.....	10
Appendix 2: Data Protection Impact Assessment Form.....	11
Appendix 3: – Data Protection Privacy Notices .....	12
Appendix 4: – Data Retention Schedule (Summary) .....	21

## **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. 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. 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'.

## **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;*
- (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;*
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;*
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that any personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;*
- (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;*

*(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. <sup>1</sup>*

### **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)

### **Personal Information Processing by, and on behalf of the College**

The College uses personal information to assess the performance of individual students and staff, and statistical cohorts of students with various characteristics. This may include personal information to identify 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 member of the College community.

The College may, occasionally, 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.

In no case will the College process personal information in a way which is detrimental to the individual. Automated decision-making processes may be used where they innocuous, for example using a student's previous school or the distance from a home address to provide an order in which students are invited to enrol. No automated process will be used to decide whether an applicant is accepted for a place at College, nor 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.

---

<sup>1</sup> <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/> - 18/01/2018

## **Data Protection Privacy Notice**

The College will provide all students, staff, trustees and other stakeholders, via a data protection privacy notice, how their data will be held and processed according to this policy. These notices may change to reflect new processes or systems. Those affected will be informed of the change as appropriate.

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, 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.
- 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, known as the College Information System (CIS), which provides for a secure, encrypted system with appropriate access controls to ensure access is limited to that authorised for the individual accessing it.

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, and destroyed once its use is complete. In any case, the primary record must be maintained in the College's database.

In the case of information relating to Safeguarding, additional security measures such as two-factor-authentication are required.

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 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 with the Regulations.

The Data Protection Officer reports directly to the Principal for Data Protection matters. This role may be a function of the Head of ILT Services, 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.

### **Rights to Access Information**

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 exemptions identified by the Information Commissioner's office, however, the College shall seek to minimise the records withheld to those which contain the opinion of another person – such as references, the details of disciplinary investigations, homework feedback, or the contents of internal emails. Further details are included in Appendix 2.

A Data Subject may exercise the right of Subject Access by submitting a request which provides sufficient information to reasonably verify the identity them. 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. In many cases, the information being requested is available via an online portal.

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.

### **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**

The College is unable to exercise its legal duties unless personal information is retained, as set out in Appendix 1. The rights to erasure are set out in Data Protection Privacy Notices. Peripheral systems such as the College's mailing list, or Open Evening Registration, where there is no associated legal duty, provides the means for the recipient to remove themselves from the College's data system.

### **Subject Consent**

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 students, 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 or external publication.

Subscribers to the College digital media may withdraw consent by unsubscribing.

### **Sensitive Information**

The College may process sensitive 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 applicants about any particular health needs from staff and students, such as allergies to particular medication, or medical conditions which may be relevant where First Aid may be required. The College will only use this information to protect the health and safety of the individual, but may be reviewed by the Learning Support Manager in case of impact on the Teaching and Learning affecting the individual or others around them. 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 *Sensitive* 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.

### **CCTV images**

The College site has a CCTV system to prevent and detect behaviour which is in breach of the Staff or Student Contract, detect crime, and to safeguard young people.

The College does not use software to automatically identify individuals using biometric data. Therefore, images routinely captured and stored do not constitute personal information until this identification has taken place, but the data must be kept securely, and encrypted.

Direct access to live CCTV images is restricted only to Security staff. Images may be stored for up to 30 days, except where an incident has been detected where video clips or snapshots may be kept, and made available to appropriate staff, until the proceedings of any incident has been concluded.

Where an incident has been recorded, and the CCTV image has been captured in this way, it will form part of the personal information for those affected, and therefore is subject to Subject Access. Images will only be released where no other identifiable person is within the image.

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 3<sup>rd</sup> 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**

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.

### **Compliance**

All staff, students, trustees, visiting or associate staff, contractors and other members of the College are required to comply with this Policy. 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 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: deleted**
**Appendix 2: Data Protection Impact Assessment Form**

Name of proposer																		
Title of project or proposal																		
Summary of proposed Data Process.																		
Who is affected by this process, and how will their information be used? Include details of any transfer to any 3 <sup>rd</sup> party, and how long the information will be retained																		
Explain the steps taken to identify the risks to data security and privacy. Include details of any consultation.																		
List the risks identified above	<table border="1"> <thead> <tr> <th>Risk</th> <th>Impact</th> <th>Likelihood</th> </tr> </thead> <tbody> <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> </tbody> </table>			Risk	Impact	Likelihood												
Risk	Impact	Likelihood																
List the actions which will be taken to reduce the risks (mitigation).	<table border="1"> <thead> <tr> <th>Risk</th> <th>Solution</th> <th>Result</th> </tr> </thead> <tbody> <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> </tbody> </table>			Risk	Solution	Result												
Risk	Solution	Result																
Describe the approval process for this project. Include relevant committees if appropriate																		
Data Protection Impact Assessment accepted:	<table border="1"> <thead> <tr> <th></th> <th>Name</th> <th>Signature and date</th> </tr> </thead> <tbody> <tr> <td>Project proposer</td> <td></td> <td></td> </tr> <tr> <td>Project Sponsor (SMT)</td> <td></td> <td></td> </tr> <tr> <td>Data Protection Officer</td> <td></td> <td></td> </tr> </tbody> </table>				Name	Signature and date	Project proposer			Project Sponsor (SMT)			Data Protection Officer					
	Name	Signature and date																
Project proposer																		
Project Sponsor (SMT)																		
Data Protection Officer																		

### **Appendix 3: – Data Protection Privacy Notices**

#### **Data Protection Privacy Notice – Staff (including Applicants) 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 keep 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 sensitive 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
- **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 performance in relation to your employment in your role, such as Professional Reviews, lesson observations, exam results of the students you have taught.

- **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. The College is equipped with a CCTV system for the purpose of the security and safeguarding of College members and visitors, and the detection of crime. The CCTV images will not be used for any other purpose.

**Who we share your information with the following third parties:**

- Surrey County Council Payroll 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 our behalf such as:**

- IT services – Microsoft, online teaching services and companies that provide online resources
- Auditors, acting on behalf of the Board of Trustees or ESFA funding terms and conditions
- 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 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.

**Transferring your data**

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

**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 do not carry out any automated processing.

#### **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](mailto: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 utmost 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.

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, 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 SELF (Student Electronic Learning File), 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.

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.

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.

You school is required to provide us with any safeguarding information 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 18<sup>th</sup> birthday.

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

We 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 interests, 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.

### **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 SELF (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](http://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](mailto: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 – 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.

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 the Student Receptionist.

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 son or daughter'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](http://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](mailto: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 your 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](mailto:dpo@godalming.ac.uk). A copy of the College Data Protection Policy can be found here: <http://www.godalming.ac.uk/docs/default-source/Publications/policy-docs-2019/data-protection-policy.pdf>

**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. A signature is requested to confirm the visitor has seen 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, for the purpose 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 three months, 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 of breach of College policies.

**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 detection of breach of College policies.

**Appendix 4: – Data Retention Schedule (Summary)**

Type of Record	Retention Period	Reason
<b>Staff Records</b>		
Personnel records inc. wages/salary records.	7 years from the end of employment (unless redundancy is involved, see below)	Provision of references and limitation period for litigation. Taxes Management Act 1970
Staff record of an investigation that has a significant element of allegation or abuse	50 years following last action on file	Safeguarding
Staff personal network areas which may include personal information	1 Year from leaving date. Not retained	Access for member of staff to their work on the network
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	12 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 kept in relation to the Control of Substances Hazardous to Health	40 years	COSHH regulations
Trustee Records, including contract details, register of interest etc	7 years	Provision of limitation and litigation
<b>Student Records</b>		
Student Files, Performance Data, References etc	6 years from the end of the Academic Year to which the records relate	Subject Access, Job/Education references. Audit evidence for funding and performance data.
Virtual Learning Environment records	Within the current academic year only	Operation of online learning environment
Computer usage logs/internet history	One year	To ensure the College can comply with Prevent legislation
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 25 <sup>th</sup> 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