Godalming College

Data Protection Policy

Updated for publication: 16 June 2011
Updated: 15 September 2011
Updated Autumn 2014

Data Protection Policy

Updated October 2014

Contents

Introduction
The College needs to keep certain personal information about past, present and future students, potential students, staff, governors and other members of the College Community in order to administer its operation, secure funding, and assess the performance of the College, recruit and employ staff, and administer the College as a whole. This means the College must adhere to the Data Protection Act (1998).

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.

In order for this collection and use of personal information to be lawful, the College must follow the *Principles* of the Data Protection Act, which state that personal information should:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Every member of the College who collects, or uses any personal information is responsible for following these principles. This Policy sets out how the College manages information in accordance with these principles.

Key Personnel
The key College personnel in relation to Data Protection are (at October 2014):

Name	Title	Role
David Adelman	Principal	Overall responsibility for Data Protection
Martin McCarthy	Director of Services	Overall responsibility for Administration and ILT including DPA compliance
Joe Yeadon	Head of ILT Services (Data Protection Officer)	Responsibility for information systems Advisor for Data Protection matters, and point of liaison for the Information Commissioner's Office
Carol Horlock	Assistant Principal	Responsible for ensuring all staff are trained appropriately in relation to Data Protection. Responsible for Senior Tutors and Learning Support team – who are key points of disclosure for *sensitive information*

Status of the Policy
The College is committed to the protection of personal information, and as so it is a condition of employment that employees comply with the Data Protection Policy. Students are required to comply with this Policy under the terms of the Student Contract. Any breach of this policy will be considered a disciplinary matter

What is Personal Information?
Personal information is anything which can be identified with an individual and is personal to them. For example, a person's date of birth, performance, image, contact or financial details would be considererd Personal Information. Indeed, summary information or statistics which might enable someone to identify an individual could also be considered Personal Information.

Some specific types of information are defined in the Data Protection Act as *Sensitive Information*, and must be treated with a greater degree of care. These are:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade Union membership
- Physical or mental health
- Sexual life
- Commission or alleged commission of offences
- Proceedings for any offence, disposal of or sentence of the court in such proceedings

Information about how to treat these types of information are described elsewhere in this document.

Notification
Data subjects are informed, via a statement on the Job Application Form for staff, or College Online Application Form for students, that their data will be held and processed according to this policy.

Students are presented with a notification statement, informing them about how their Personal Information may be used, at the final stage of completing an Online Application, applicants must positively agree to the notice before their application can be submitted. This notice is reviewed annually.

The notices also remind Staff and Students that it is their responsibility to update the College should their Personal Information change. Any member of the College may be directed to participate in any data-checking exercise.

The College is registered with the Information Commissioner's Office, the registration notice outlines how personal data is collected and processed.

Responsibilities of Staff
In the course of their work staff will often use information about students, colleagues, 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 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 (either on paper or electronically) in order that it can be retrieved if required.
- 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.

This means that personal data should:

- Be kept in a locked filing cabinet or locked drawer
    - This applies to paper files, reports, references etc
    - Staff should remember that their room may be accessed by other staff (e.g. cleaning or site staff) who do not have authority to access the data
- Not be copied to a USB memory stick, removable disc drive or copied to CD, except to secure the data in a secure environment (for example computer backup) – and that storage is suitably encrypted or protected in a manner which would prevent unauthorised access should the device be lost or stolen, and
- Not be removed from the College site except where the purpose for the removal is absolutely necessary (e.g. NVQ assessment). ,
    - Where staff are authorised to access personal data to complete their professional duties, they should access the information using online systems.

Some staff (such as Counsellors or Senior Tutors) may have additional *Sensitive Information* disclosed to them. This should be kept separately from the main student file to prevent general access by other staff, kept securely, and only disclosed in accordance with the Data Subject's wishes.

Occasionally, staff may supervise students doing work which involves the processing of personal information (e.g research, event organisation) – staff should ensure that those students are aware of the Data Protection Principles, in particular the requirement to obtain the data subject's consent, data security and keeping the data secure against disclosure.

Where information is provided to students, for example as part of a research project, all data which identifies individuals should be removed prior to it being made available to the student.

Guidelines for staff are provided in Appendix 3 (page 10).

Responsibilities of Students

In the course of their College life, students may occasionally come into contact with personal information about others, for example:

- Being told about medical details, or contact details of a student in their group while on a College trip (in case of emergency)
- Taking photographs of other students
- The information resulting from a research project which involves personal data

Students should adhere to the Data Protection Principles, and in particular seek permission from the data subject to collect, store and process that information, keep it securely, not disclose the information to a third-party, and destroy the data once it has been used. Additional help about how to comply with the Data Protection Act can be provided by their teacher or personal tutor in the first instance. Students should be particularly mindful of their use of social media, and in particular the need to seek permission of the data subject in order to prevent breach of the Child Protection Policy.

The College has specific policies in relation to Social Media, and Child Protection.

Rights to Access Information

Any Data Subject has the right to access any personal data that is kept about them. In practice, both students and staff can view the key Personal Information held about them using the College Information System (CIS) at any time.

However, a Data Subject may formally exercise the right of Subject Access by submitting a request in writing to the Subject Access Controller (see below).

The College reserves the right to make a charge of £10 for each official Subject Access Request made under the Data Protection Act.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 20 days, unless there is a good reason for the delay – in this case the designated data controller will inform the data subject of the reason for the delay.

All Subject Access Requests must be approved by the Subject Access Controller prior to the provision of information.

Subject Consent
For the most-part, Data Subjects will have consented to their Personal Information being processed as part of the general administration of the College, as described to them in the Data Protection Notice.

However, specific consent may be required before information is released to a third-party, 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.

Sensitive Information
The College may also process sensitive information about a person's health, disabilities, criminal convictions or alleged criminal activity, sexual orientation, ethnic origin or trade union membership in pursuit of the legitimate interests of the College. For example, some jobs or courses will bring the applicants into contact with children, including young people between 16 and 19, and the College has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the proposed role and students for their courses. The College may also require such information for the administration of sick pay, absence policy, or equal opportunities policy, or academic assessment.

The College will only seek to collect or process information which is relevant and not excessive for the purpose for which it is collected.

The College does ask for information about particular health needs, such as allergies to particular medication, or conditions such as asthma or diabetes. The College will only use such information to protect the health and safety of the individual, for example in the event of medical emergency. In the course of collecting this information, the College will ask for the express consent to the collection and processing of this sensitive information. Where this consent is withheld, the information will not be collected.

Police Access to Personal Information
Personal information about an individual may be disclosed to the Police where there is a suspicion of that person being involved in criminal activity, with the specific authority of the Principal. 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 Data Controller
Godalming College is the Data Controller under the Data Protection Act 1998, and the Principal is ultimately responsible for the College's registration and compliance with the Act. The Principal may delegate the authority to make decisions about data protection matters.

Responsibility for administering Subject Access is managed by the Director of Services, who may delegate tasks relating to this matter, where appropriate. This role is designated the Subject Access Controller.

Each Head of Department, Head of Service or Assistant Principal will be responsible for the activities within their area of responsibility, and that they comply with this policy and the Data Protection Act.

Responsibility for liaison with the Information Commissioner's Office, and advising the Principal on Data Protection matters lies with the Head of ILT Services. This role is designated the Data Protection Officer.

Information and advice about the collection, storage and processing of personal information can be obtained from the Data Protection Officer.

Retention of Data

The College will keep 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 shown in Appendix 1.

Compliance

All staff, students, visiting or associate staff, contractors and other members of the College are required to comply with the Data Protection Act. 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.

Any individual who considers that the policy has not been followed in respect of personal data should raise the matter with the Designated Data Controller concerned in the first instance. If the matter is not resolved it should be pursued via the staff grievance or student complaints procedure.

Appendix 1: Data Retention Schedule

Note that this table applies to electronic and paper records, unless specified.

Type of Record	Retention Period	Reason
Personnel files, training records, notes of grievance and disciplinary hearings Wages and Salary Records	10 years from the end of employment	Provision of references and limitation period for litigation Taxes Management Act 1970
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	3 years from date of redundancies (<20 employees) or 12 years (>=20)	Limitation period for litigation
Income Tax, Maternity Pay and Statutory Sick Pay records	7 years after the tax and financial year to which the records relate	Income Tax (Employment) Regulations 1993, Statutory Maternity Pay (General) Regulations 1986, Statutory Sick Pay (General) Regulations 1982
Accident records	3 years after Academic year to which the records relate	Management of Health and Safety
Health records	3 years from the end of employment	Subject Access, limitation period for personal injury claims
Records kept in relation to the Control of Substances Hazardous to Health	40 years	COSHH regulations
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.
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.
CCTV images	7 days unless a specific incident has occurred, and 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
Staff personal network areas which may include personal information	1 year from date of leaving	Access to materials created by Staff member

Appendix 2: Definitions

Data subject: an individual who is the subject of personal data.

Data controller: a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data processor: in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Recipient: in relation to personal data, means any person to whom the data is disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

Third party: in relation to personal data, means any person other than the data subject, the data controller, or any data processor or other person authorised to process data for the data controller or processor.

Appendix 3: Guidelines for Staff

For All Staff

The College uses lots of personal information in its day-to-day operations, from administering timetables and enrolment, through to exam entries and results, helping students with Learning Support needs, and performing staff reviews. We must all respect the privacy of this information, maintain it, and ensure that it is handled correctly.

Applying the Data Protection Policy can be summarised:

- Do not leave paper files without physical security – lock files away when you're not using them.
- Never leave a computer workstation unlocked when unattended – even for a moment, and don't print sensitive information to a printer where it can be picked up by someone else.
- **NEVER** allow another person to use your computer account.
    - If you have a visitor who needs to use a computer, please contact the ILT team who will assist you.
- Never take personal information off-site. USB sticks and laptops are easily lost or stolen and paper files can be accidentally seen by others or damaged.
    - It is fine to save files on the Staff Portal, or write reports using online College systems where they are secured.
    - Remote systems, such as eApps, are encrypted, and file data is stored on the College site.
- Never disclose information to anyone who is not specifically authorised. If in doubt, consult either the Data Protection Officer or a member of SMT.
- Only collect information that you really need, keep it securely, and destroy it when you don't need it anymore. (See Appendix 1)
- Remember that if you record information about someone, they have a right to inspect it.
- If in doubt – ASK!

Communication with External Bodies

It is inevitable that we need to transfer information to other staff, Universities/employers, or indeed the data subject themselves. You should consider the best method and chose the most appropriate:

- Letter – has the advantage that the addressee is apparent, but is slow and open to abuse if the addressee is not present when the letter is delivered. You should check the address is correct, where possible using the MIS system to generate the letter to avoid human error.
- Fax – has the advantage of immediacy, but is prone to an incorrect number being typed, and there is no way of knowing who has access at the 'other end'. Avoid faxing any personal information. In any case, the fax has largely disappeard from daily life.
- Email – within the College - is generally considered secure because a password is needed to access it and the College email system is encrypted, but you should double-check the address before clicking 'send'. While it is immediate, information which has been sent cannot be maintained, so use online systems where possible, and alert the addressee that it is there.
    - If you need to send sensitive information externally, you should include it was a password-secured attachment, and inform the recipient separately of the password.
    - Email to addresses outside the College is generally considered *not* secure unless it is encrypted. You should seek assistance before sending personal information to an address outside the College.
- Memo/paper notes – while easy and useful where the information needs little processing, also carries a risk of unauthorised access, for example a memo in a pigeon-hole is not secure.
- Telephone/face-to-face – for disclosing information, this is secure providing the identification of the person you're talking to can be verified, but should be used appropriately and only by authorised staff, and you are sure you cannot be overheard.

Messages containing personal information should not be left on voicemail systems as you cannot guarantee that others will not hear them.

Teaching and Learning

It is normal for teachers to process personal information about students. This could include date of birth, name and addresses, attendance, parental circumstances/custody information, disciplinary records, and marks, reviews and references etc. In general, staff are authorised to access information about students, but should not disclose it to an unauthorised third-party.

Information may be disclosed to the student's parent; each student is notified of this at Enrolment, and consent to this disclosure is a condition of entry to the College. Occasionally students will withdraw this consent for personal reasons – this will be recorded on the College MIS system and must be respected. In any event, you should verify the identity of the parent using CIS before giving any information about the student.

Administering Students

In the course of administering enrolment, trips, work experience etc it is normal that information will be collected, processed, and passed-on to others within the College, or external bodies who need the information for the normal processing in relation to the College's activities. The student is notified of this when they enrol at the College and it is a condition of entry to the College that information can be used in this way. You may reasonably, for example, pass on a student's telephone number to a work-experience employer or to UCAS as consent is implied, but you must only do so with the condition that the recipient will treat the information as confidential. The organisations with which we do most transactions (UCAS, exam boards etc) have their own Data Protection policies which are compatible with ours.

Basic timetable information and whether a student is present at College can be requested by telephone by their parent via the Administration team. If you are asked to provide this information, you must verify the identity of the parent.

To do this, you can:

- Ask them information which only they would know, such as the student's date of birth and home telephone number, and check this against the CIS record (including parent's name!).
- Ask them where they are, and call them back using the telephone number stored on CIS.
- Ask them to consult the student directly rather than giving information over the phone – particularly where information is available to the student via Godalming Online.

You should never normally give any performance information (e.g. exam results) over the telephone, as the student is able to access this directly by using College systems.

You should not disclose information to anyone unless it is authorised, if in doubt speak to the Data Protection Officer.

Medical or Personal Circumstances

Staff, and sometimes students, have sensitive information disclosed to them, normally about medical conditions or personal circumstances. This is part of the normal pastoral care offered by the College.

You should never pass on this information without the express permission of the person who has disclosed the information, noting Safeguarding regulations which may require you to disclose matters of suspected abuse to the relevant Safeguarding Authority, regardless of that consent. All staff receive training on Safeguarding – if in doubt contact the College's Safeguarding Officer.

It is normal to ask, in the course of the disclosure, how the Subject wants the information to be treated – The Senior Tutor team and Learning Support team have guidelines about how this should be done, as this is the normal route for such disclosure.

References for Employers

Potential employers and their agents often ask for confirmation about ex-students or staff and their performance. You should only disclose this information if the data subject has given written permission for this purpose (i.e. authorising that employer or agent). You must only disclose reasonable information within the data retention periods – which means that after a period, you cannot provide a reference.

Staff who have left their employment at College

When staff leave their employment at College, their access to College systems and data is terminated with immediate effect on their last day of employment unless there are exceptional circumstances which have been agreed by the Principal or in his absence one of the other 'key personnel' detailed on page 3 of this Policy.

Staffthey are invited to continue their membership of the 'Staff Association'. In order to do this, some information (e.g. contact information) will be retained.
The Personnel team will ensure that only those records necessary for this membership will be kept – and will be passed to the Staff Committee. This organisation is entirely voluntary and is outside the auspices of Godalming College as a Data Controller.

System Administrators

By the nature of the work that IT Administrators do, they need to use computer accounts which permit an enhanced level of access to computer file and data systems which could potentially give them access to personal information. As a connected institution, the College subscribes to the JANET Administrators Charter. With relevance to Data Protection:

- Administrators should only access systems in order to administer them. They should not view files, folders or any other system for any other reason, e.g. reading a file or viewing a system to which they would not otherwise have access. It is good practice to separate administrative functions by using separate personal and administration accounts.
- Administrators will come into contact with sensitive information. They should not disclose this information to any other person, body or organisation.
- Administrators should, when implementing systems, consider the security requirements to prevent accidental or deliberate disclosure, whether in giving appropriate access to users, or securing them against intrusion.

Appendix 4: Data Security

Most breaches of data occur when a person makes an error – for example, leaving a laptop on a train, losing a USB stick, or dumping paper records into a skip. As a College, we have a duty to protect personal information, and so you should use the systems provided to secure data where ever possible. Individual circumstances may dictate that personal information needs to be removed from the College site (such as at an external hearing) – but this should be regarded as exceptional, and appropriate security should be in place.

Any human efforts to secure personal information are only as secure as the facilities to secure them allow. Personal data should be stored in such a way that:

- Only authorised people can access it
- Is secure to intrusion
- It can be maintained so that it is accurate.

A secure storage could reasonably expected to be:

- Somewhere only authorised people can get to, for example:
    - A locked filing cabinet or drawer in a staff workroom to which only authorised people have keys.
    - A safe or other secure environment
    - In a centrally-backed-up electronic storage system where authorised access is controlled, e.g. CIS or Staff Portal

.. and isn't:

- In a pile on a desk in an unlocked office
- On a USB stick or shared network drive to which unauthorised people might have access
- Left in a car (on paper or electronically).

Paper records should be kept in an organised way – this is both so that information can be retrieved for updating or be found for destruction when its use if finished. When paper records need to be destroyed, they should be disposed of in a method appropriate to the information contained:

- *Sensitive* information should be shredded immediately by the authorised person (i.e. the person who held the records).
- Other information can be disposed of via a central shredding service, providing it is stored securely while in the process of being shredded.

Electronic records can be destroyed using several methods:

- The deletion of records using 'delete' facilities,
- The overwriting of backup tapes where the personal data may be archived (note that backup tapes need to be stored securely as they may contain personal data),
- In equipment which is taken out of service, hard-disk drives can be erased using magnetic destruction, specialist data destruction services etc.

A good test would be for you to imagine yourself as the Data Subject – what would you want to happen to your records?

Appendix 5: Additional Information

In addition to the Data Protection Act, the College must comply with a number of other Acts of Parliament. Practices in these areas are covered by other College Polices, which are available via the College website.

The other principal Act which relates to information is in the Freedom of Information Act – but relates to information about the College which is in the public interest and not personal information about individuals. This entitles a member of the public to request information about the College; the main categories of information are listed in a Publication Scheme. Details of how Godalming College manages its Freedom of Information requests are shown on the College website.

It is important to remember that the principles of Data Protection override any request for information under the banner of 'Freedom of Information'. Personal information should never be disclosed to a Third Party. If you are in doubt as to what can be disclosed and in what form, you should consult the Data Protection Officer, or the Director of Services.

Appendix 6: Mobile devices

The College has several systems which enable members to connect their mobile device (e.g. iPhone,Blackberry, Android etc) to view email, calendar and contact information via a remote connection, or via the College wifi. There are three methods available:

1. Web-based email – this uses the same security policies as from a laptop/home computer, or
2. With a Partnership between the device and the College systems which synchronises email and calendar information which are then stored on the device, and can be accessed without re-connecting to the internet.
3. eApps – remote applications, running over an encrypted internet connection.

'eApps' and webmail give access to email and calendars, as well as files and folders without storing data on the device. This is therefore the most secure method of access.

A partnership involves the storage of information away from the College site (i.e. on the device) and therefore it is important that the College obtains assurance that the information will be kept securely. Therefore, for those who wish to create a partnership, before the facility is enabled, they must agree:

- to keep their device safe, and that **only they** will use it (this may be of particular concern to those whose device may be shared with their family, such as with an iPad or tablet). Staff who share their device with others must not create a partnership.
- that the device is managed by the College's automatic security policies, which will enforce a number of settings, including:
    - That a complex password be used to access the device, and that it will need to be changed every 90 days
    - That a number of incorrect attempts to input the password will result in the device being wiped – in most cases to its factory state (dependant on the individual device). This will delete all information from the device – this is to minimise the risk of information stored in emails or calendar items being seen by someone other than that user.
    - That the device's memory will be encrypted. The user will be responsible for any consequence of this, depending on what else they use their device for.
    - That the device 'lock' is automatically applied after a few minutes of inactivity.
- The user must also immediately report to the ILT Services team if their device is lost or stolen – a remote wipe can be carried-out. If the user has access to the internet, they can also perform this themselves via the College's web-based email system (particularly if the device is lost out-of-hours.

The User is responsible for all access to their network account, and should protect their device and its password. Deliberately allowing another person to access a College computer account may result in disciplinary action.

Any suspected or actual compromise to an individual's account must be reported to the Principal without delay.