Data Protection Policy

Introduction

The college holds personal data about its students (and potential students), Fellows, employees, alumni, supporters, clients, suppliers and other individuals for a variety of purposes.

This policy sets out how the college seeks to comply with data protection law in the UK by protecting personal data and ensuring that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the statutory Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed. The policy is drafted to meet the provisions of the Data Protection Act 1998 (DPA) and the General Data Protection Regulation (GDPR) 2016 that comes into effect on or before 25 May 2018.

Definitions

Category of Data Subject	Groups of subjects – e.g. students, alumni and supporters, senior members and staff, college visitors and guests, commercial customers and suppliers.
College purposes/ needs	The purposes for which personal data may be used by the college: Academic, Development, human resource management, administrative, financial, regulatory, payroll and business development purposes. College purposes include the following: o Tutorial processes including students' admission, personal contact information, course information, tutorial routines, examination administration and results o Senior and Junior Members' and visitors' accommodation arrangements o Junior members' health, welfare and disciplinary matters o Stewardship/Alumni relations and fund-raising activities o Financial reasons, such as recording transactions, raising invoices, security vetting, credit scoring and checking o Business development and event booking processes for commercial conference and accommodation activity including marketing activity o Compliance with the college's legal, regulatory and governance obligations and good practice o Transacting the business of the college (such as through email and other forms of correspondence). o Employment of personnel, checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments o Monitoring staff attendance, conduct, disciplinary matters o Building and maintaining the college's historical archive records.
Data	Information that is held electronically or manually – i.e. in a computer data base for example or as printed material in a file held in a filing cabinet.
Data Cleaning	The processing of data which results in it being changed (due to inaccuracies or disputes), or because it no longer needs to be retained, is over-written, deleted, or anonymised. In the case of paper hard-copy, the document may be destroyed.
Data Controller	The college is the Data Controller.
Data Protection Statement ("DPS")	A statement published by the college, specific and relevant to particular data subject(s) which sets out how the college handles and uses information it collects about them. The statement will set out how the information is used; how long the information is kept; how the college shares the information with others; the data subject's rights. Publication is usually on the college website and may also be shared with data subjects directly.
Data Subject	An individual about whom personal data is held by the college.
Member	Senior members (Fellows) and junior members (students and alumni) of the college when they are handling or processing personal information on behalf of the college, except when they are acting in a private or external capacity.
Personal data	Information relating to identifiable, living, individuals, such as student applicants, current and past students, alumni and friends of the college and other benefactors, job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. Personal data gathered may include: individuals' contact details, educational background, academic performance information, employment opportunities/outcomes, wealth data, donation history,

	financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV, events booking information and history. These lists are not exhaustive.
Processing data	Capture/collection, storage, use, updating, copying, sharing, deletion of data are all ways of processing data. This list is not exhaustive.
Records Retention Schedule	A control document that sets out the periods for which the college's records should be retained to meet its operational needs and to comply with legal and other requirements. It is written by the college's Archivist and approved by college council.
Sensitive personal data	Personal data about an individual that is medical, financial or performance related, for example physical or mental health or condition, biometric and genetic data; salary, fees, or other personal financial data; appraisal or results data; as well as criminal offences, or related proceedings. Any use of sensitive personal data should be strictly controlled in accordance with this policy.
Staff	Anyone working in any context for the college at any level or grade (whether permanent, fixed term or temporary) and including employees, retired but active members and staff, visiting Fellows, workers, trainees, interns, seconded staff, agency staff, agents, volunteers, and external members of college committees

Scope

This policy applies to all staff and members of the college, except when they are acting in a private or external capacity, and should be read in conjunction with:

- college statutes and regulations;
- staff employment contracts, staff handbook and comparable documents;
- policies, procedures and terms and conditions of the college and, where relevant, similar documents of the University of Cambridge with regard to:
    i. information security;
    ii. acceptable use of IT facilities (including use of personal devices);
    iii. records management and retention;
    iv. any other contractual obligations on the college or the individual which impose confidentiality or information management obligations (which may at times exceed those of college policies with respect to storage or security requirements – e.g. for funded research).

This policy is reviewed and approved by the college council and the Governing Body. It is reviewed at least once every three years. The Governing Body remains responsible for ensuring appropriate resources are in place to achieve compliance with data protection law in line with an appropriate overall risk profile.

Who is responsible for this policy?

The data controller for all personal information is Selwyn College, Grange Road, Cambridge CB3 9DQ and as such is subject to a range of legal obligations. The statutory Data Protection Officer for the college is the Office of Intercollegiate Services Ltd. (OIS) at 12B King's Parade, Cambridge; 01223 768745; college.dpo@ois.cam.ac.uk. OIS should be contacted if you have any concerns about how the college is managing your personal information, or if you require advice on how to exercise your rights as outlined in this statement. The College Data Protection Lead (CDPL)within the college is the Bursar, Nick Downer, who may be contacted at bursar@sel.cam.ac.uk .

Responsibilities of the college

The college upholds data protection law as part of everyday working practices, through:

- ensuring all personal data is managed appropriately through this policy;
- understanding, and applying as necessary, the data protection principles (see "General Principles" below) when processing personal information;

- understanding, and fulfilling as necessary, the rights given to data subjects (see "Rights of Data Subjects" below) under data protection law;
- ensuring all members and staff are aware of this policy and any associated procedures and notes of guidance relating to data protection compliance, provide training as appropriate, and reviewing regularly its procedures and processes to ensure they are fit for purpose.
- maintaining records of its information assets
- understanding, and implementing as necessary, the its accountability obligations under data protection law; and
- the publication of data protection statements outlining the details of its personal data processing in a clear and transparent manner.

Responsibilities of the DPO, in conjunction with the College Data Protection Lead ("CDPL")

- to inform and advise the College and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
- to monitor compliance with data protection law, with other Union or Member State data protection provisions and with the policies of the College in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance;
- to cooperate with the Information Commissioner's Office (ICO);
- to act as the contact point for the ICO within 72 hours of any incident**,** on issues relating to processing and particularly reportable personal data breaches, and to consult, where appropriate, with regard to any other matter.

In addition, the DPO is:

- expected to investigate and manage complaints from data subjects and to facilitate them in exercising their rights;
- required to ensure that any other duties/responsibilities they hold are not in conflict with these roles;
- appointed on the basis of their "professional qualities and, in particular, expert knowledge of data protection law and practices…";
- to be in a position where they report to the "highest management level", without interference or instruction or risk of penalty or dismissal;
- provided with appropriate resources to carry out their duties, including their own professional development; and
- accessible to any data subject for the discussion of any issues or management of their rights.

Responsibilities of the CDPL

- Manage subject data access requests;
- Manage all data subject rights requests;
- Manage the impact of a data breach within the college, and implement any internal or external recommendation;
- Report all breaches to the DPO;
- Liaise with the police if there is a crime;
- Determine and implement risk measures to reduce likelihood of breaches occurring;

- Ensure that staff are appropriately and proportionally trained, depending on their roles;
- Advise the DPO on nature of any training gaps;
- Assist the DPO in the provision of information;
- Create, update and maintain appropriate records (including DPS, data register, risk register).
- Facilitate any audit visit by the DPO.

Responsibilities of the Compliance Manager

- Deputising for the CDPL as necessary
- Auditing policy compliance
- Maintaining GDPR training records

Responsibilities of the IT Manager

- checking and scanning college security hardware and software regularly to ensure it is functioning properly;
- providing an advisory/consultancy service on matters relating to hardware/software for college staff.
- Auditing college systems as necessary.

Responsibilities of Heads of Department

- conducting data audits as required by the DPO on personal data collection and processing and on personal data sharing and transmission;
- contributing to DPSs to be published;
- ensuring all systems, services, software and equipment meet acceptable security standards;
- researching third-parties that the college is considering working with or does work with to store or process data;
- checking and approving with third parties that handle the college's data, any contracts or agreement regarding data processing;
- ensuring that staff members are fully briefed in respect of data processing;
- coordinating with the DPO to ensure all initiatives adhere to data protection laws and this policy.

Responsibilities of all Employees

- completing relevant data protection training, as advised by the college;
- ensuring that you understand this policy and that you adhere to its terms;
- only accessing and using personal data as necessary for your contractual duties and/or other college roles and ensuring such data is not disclosed unnecessarily or inappropriately;
- ensuring that personal data is secure against loss or misuse;
- ensuring that you process personal data accurately. If you believe that information is inaccurate you should record the inaccuracy and inform your HOD and/or the DPO;
- taking reasonable steps to ensure that personal data we hold about you is accurate and updated as required. If your personal circumstances change, please inform the HR Officer so that your records can be updated;
- reporting personal data breaches, and co-operating with college authorities to address them;
- only deleting, copying or removing personal data as agreed with the college and as appropriate.

Non-observance of these responsibilities may result in disciplinary action against individual members or staff. The responsibilities outlined above do not waive any personal liability for individual criminal offences for the wilful misuse of personal data under data protection legislation.

General Principles

The general principles of data protection are set out below.

1. Fair and lawful processing

The college must process personal data fairly and lawfully. This generally means that it should not process personal data unless at least one of six conditions for processing exists.

1.1 Conditions for processing

The college will ensure that any processing of personal data is justified using at least one of the conditions for processing and that this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be stated on the relevant DPS

a. ***Consent:*** The data collected is subject to active consent by the data subject. This consent can be revoked at any time. The consent must have been given for one or more specific purposes e.g. to receive the alumni newsletter and or marketing mailings.

b. ***Performance of a contract:*** Data processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract e.g. to enrol as a student at the college or make a conference booking or become employed by the college.

c. ***Legal obligation*** Processing is necessary for compliance with a legal obligation to which the college is subject e.g. reporting accident information under RIDDOR.

d. ***Vital interests*** Processing is necessary to protect the vital interests of the data subject or of another natural person. This condition only applies in cases of life or death, e.g. where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.

e. ***Public interest*** Processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions or in the exercise of official authority vested in the college e.g. reporting student's residence status to the local council.

f. ***Legitimate interest*** Processing is necessary for the purposes of the legitimate interests pursued by the college or by a third party on whose behalf the college acts, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child, e.g. our development and alumni relations activity.

1.2 Sensitive personal data

In most cases where the college processes sensitive personal data it will require the data subject's explicit consent to do this unless exceptional circumstances apply or it is required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed. For clarification, please discuss this requirement with the DPO.

2. Data collected for specified and lawful purpose

The college will ensure that it is clear about why it processes personal data and what it intends to do with it. It will ensure that it provides details of the data processing to the data subjects through its DPSs. There may be a DPS for each category of data subject.

The college will not process personal data obtained for one purpose, for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

3. Relevant, adequate and not excessive for the stated purpose

The college will ensure that any personal data it processes is relevant, adequate not excessive, given the purpose for which it was obtained.

4. Accurate and up to date

The college will ensure that any personal data it processes is accurate. Individuals may ask that the college corrects inaccurate personal data relating to them.

5. Data retention

The college must not retain personal data for any longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with the college's data retention policies. The college will set out its retention policies in its Records Retention Schedule and wherever possible will also provide that detail in its DPSs.

5.1 Data Retention Guidelines

Personal data will need to be retained for longer in some cases than in others. How long the college retains different categories of personal data should be based on individual college purposes. It is a legitimate interest of the college to retain data for archiving purposes. Therefore before deletion of any personal data, representation should be made to the college Archivist and the DPO to determine whether cause to retain the data exists. A judgement must be made about:

- the current and future value of the information;
- the costs, risks and liabilities associated with retaining the information; and
- the ease or difficulty of making sure it remains accurate and up to date.

The appropriate retention period is also likely to depend on the following.

a. What the information is used for

If it continues to be necessary to hold the data for one of the reasons set out above, then the college should retain it for as long as that reason applies. On the other hand, information with only a short-term value may have to be deleted within days.

Where personal data is held for more than one purpose, there is no need to delete the data while it is still needed for any of those purposes. However, personal data should not be kept indefinitely "just in case", or if there is only a small possibility that it will be used.

There may often be good grounds for keeping personal data for historical, statistical or research purposes. The Data Protection Act provides that personal data held for these purposes may be kept indefinitely as long as it is not used in connection with decisions affecting particular individuals, or in a way that is likely to cause damage or distress. This does not mean that the information may be kept forever – it should be deleted when it is no longer needed for historical, statistical or research purposes. See the section below on Archives.

b. The surrounding circumstances

If personal data has been recorded because of a relationship between the college and the individual, the college should consider whether it needs to keep the information once the relationship ends, e.g. a conference client.

The college may not need to delete all personal data when the relationship ends. It may need to keep some information so that it can confirm that the relationship existed – and that it has ended – as well as some of its details e.g. details of a past student's attendance and course dates.

In some cases, the college may need to keep personal data so it can defend possible future legal claims. However, it could still delete information that could not possibly be relevant to such a claim. Unless there is some other reason for keeping it, personal data should be deleted when such a claim could no longer arise.

c. Any legal or regulatory requirements

There are various legal requirements and professional guidelines about keeping certain kinds of records – such as information needed for income tax and audit purposes, or information on aspects of health and safety. If the college keeps personal data to comply with a requirement like this, it will not be considered to have kept the information for longer than necessary.

d. Agreed "industry" practices

How long certain kinds of personal data should be kept may also be governed by specific sector requirements and agreed practices. E.g. medical records may be kept for an agreed length of time based upon medical practice.

The College's Data Retention Schedule is attached as an Appendix.

6. Rights of Data Subjects

Data will be processed in accordance with the data subject's rights as outlined below.

6.1 Access requests

Under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a subject access request, you should refer that request immediately to the CDPL. The college may ask you to help comply with those requests.

Please contact the CDPL if you would like to correct or request information that we hold about you though please note that there are restrictions on the information to which you are entitled under applicable law.

6.2 Right to object to data processing

An individual may object to their data being processed if it is likely to cause or is causing damage or distress. Please report any such complaint to your HOD or the CDPL immediately. Further instruction will then be given.

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify your HOD or the CDPL about any such request.

Do not send direct promotional or marketing material to someone electronically (e.g. via email) unless you have an existing relationship with them, specific to purpose/subject of the promotional subject matter e.g. a potential applicant has already engaged with college with a view to making an application to study here.

HODs should contact the CDPL for advice on direct marketing before starting any new direct marketing activity.

6.3 Inaccurate information

An individual has a right to ensure that the information held is accurate and to require the college to correct any inaccuracies.

You should always record any requests made for inaccurate personal data to be rectified, blocked, erased or destroyed; report this to your HOD and the CDPL who will determine the appropriate course of action.

6.4 Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done free of charge.

You should always record any requests made for a copy of data to be made available and or ported; report this to your HOD and the CDPL who will determine the appropriate course of action.

6.5 Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

You should always record any requests made for data to be erased and the data subject "forgotten"; report such requests to your HOD and the CDPL who will determine the appropriate course of action.

7. Data security

The college must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on its behalf, the HOD or CDPL will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

7.1 Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed, subject to the requirement to archive relevant data – see the section below on Archives.
- Data stored on a computer should be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used.
- The IT Manager must approve any cloud used to store data.
- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up in line with the college's backup procedures.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- Laptops, tablets or smartphones that have on-line remote access to servers where data is stored must be securely retained at all times by its college owner.
- All servers containing sensitive data must be approved and protected by security software and a strong firewall.

8. Transferring data internationally

The law places restrictions on the transfer of personal data outside the European Economic Area (EEA) unless the country involved ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Therefore no data may be transferred outside of the EEA without first discussing it with the DPO.

Specific consent from the data subject must be obtained prior to transferring their data outside the EEA. If, after careful consideration, it is regarded as essential that the transfer of personal data outside the EEA should take place – and there is not adequate protection – the prior consent of the data subject must be sought.

Where data is transferred outside the EEA for the purposes of obtaining legal advice, consent of the data subject is not required.

Procedures and Processes

Data Register and Data Audits
The data register contains information on what data is held in respect of each category of data subject, specifically listing:

- What type of data is collected and stored
- What we do with that data/how it is used
- The legal condition we rely upon to process the data
- Where we get the data from
- Where it is stored
- How long we keep it for
- Any anticipated impact upon the privacy of the data subject as a result of our processing
- Who we share the data with
- What data we share
- When we share it and for what purpose
- Any written agreements that exist to cover the sharing of data.

The various sections of the register will also detail who is responsible for that element. Data audits will be carried out from time to time by the responsible HODs and the CDPL and these will inform the updating of the data register.

The IT Manager will conduct a system audit from time to time. HODs will conduct audits on Personal Data Collection and Processing and on Data Sharing and Transmission. Any action that may be highlighted as a result of the audit will be noted and followed through to completion or resolution. Audit data will be used to inform the relevant DPSs.

Data Protection Statements - transparency of data protection
Being transparent and providing accessible information to individuals about how the college will use their personal data is important. The college publishes a DPS relevant to each element of its activity which:

- Sets out the purposes for which it holds personal data and how it is used;
- What data is held by the college and the retention duration;
- Highlights that its work may require it to share data with third parties such as the University of Cambridge, contractors and/or other professional advisers who perform a service;
- Provides that data subjects have a right of access to the personal data that is held about them;
- Advises who in college is responsible for the data policy and provides relevant contact information.

The CDPL will set out the specific DPSs, for each data subject type, based upon the details collected in the data audits.

Children (under 16)
The college does not currently have cause to collect data on children under the age of 16. However, it is our policy that if this is necessary, any relevant DPS would be written in such a manner that they can understand it.

Collecting/Capturing Data
Before processing any personal data, we should consider the checklist set out below:

- What is the purpose of the college collecting this data?
- What is its justification for collecting the data and which condition will apply?
- Does the college really need to collect the information? Does it really need to collect all of it?
- Is the information 'ordinary' or is it 'sensitive'?
- Is the college authorised to collect/store/process the data – by the college or by the data subject?
- If the data subject's consent is needed, has it been obtained?
- Unless the data has been obtained from a reliable source, has the college checked with the data subject that the data is accurate?
- Is the college sure that the data is stored securely?
- How long should the data be retained?

Where ***consent*** to collect data is the condition in use, we will need to invite a data subject to give consent for his data to be collected and/or processed providing clear information on the specific purpose we intend. The consent must be:

- specific, informed and freely given;
- it cannot be implied;
- the data subject must specifically "opt in";
- the consent must be for a specified duration;
- when the duration has lapsed, consent must be renewed;
- if consent is not given or if it is withdrawn, data must be removed or anonymised.

Therefore in such circumstances, appropriate documentation will need to be drafted in order to obtain the subject's consent and the following factors should be taken into account:

- We do not need to have consent to carry out a direct marketing campaign by mail – i.e. hard copy dispatched through the post.
- Sending an email to ask for consent may of itself be an infringement of the subject's rights.

Recording Data
When we process data, we need to consider what data is recorded.

The law means that any recorded opinion about or intentions regarding a person, is personal data to which a data subject may gain access. This should be borne in mind when written or other records are made (and this includes e-mails and audio recordings, in addition to computer and manual files). The following is a useful test to apply to 'doubtful' comments:

- Is this comment fair, accurate and justifiable?
- If you were to show this to the data subject, would you still be confident that the comment is fair, accurate and justifiable?
- If the answer to the questions - and in particular the first question - is 'No', then the comment should go unrecorded.

Data Storage
Information that may be held electronically or in a 'relevant' manual filing system. There are definitive **databases**, which various departments use to store their data, e.g. Raisers Edge, Mercury, Accurate Solutions etc.. Each relevant HOD is expected to understand the departmental policy in respect of the use of its database and how the Data Protection Policy applies to its use.

Additionally, the department policy will need to consider other data storage methods and the routines to manage them.

- Informal databases, e.g. spreadsheets are not permitted for long term storage of data. They may be used for short term activity but should then be deleted. The main database should be updated as required so that future short-term data bleeds can draw on the most up to date information.
- Consideration should be given to the management of cloud based or on-line additional data storage tools. The HOD will need to ensure that such systems are recorded by the IT Manager on the system audit and that appropriate routines are in place to manage the data stored therein.
- Email is also a form of data processing and by definition storage. See the section on email below which defines the college policy in respect of email retention. Whilst live, HODs should consider how email traffic is managed so that data is protected.
- Hard copy storage. A 'relevant' manual filing system may have the following characteristics:
  - Grouping within a common criteria, even if not physically kept in the same file or drawer
  - Structuring by reference to the individual by name, number, or by criteria common to individuals, such as sickness, type of job, membership of pension scheme or department
  - Structuring that allows specific information about the individual to be readily accessible.

In practical terms it is prudent to assume that most, if not all, manual filing systems will fall under the provisions of the law and will therefore fall within this policy. Security routines for all data storage systems, should be considered by the HOD. Consider who has access and how access is controlled. Setting of strong passwords is important as is the control of keys to filing cabinets.

Internet and Email
The provisions of the DPA and GDPR apply as much to websites and to email as they do to data processing by any other means. Any personal data downloaded from the web, included within a web site, or contained within an email are subject to the same restrictions as information held in manual files or on databases. The type of data placed onto web pages should reflect the fact that information posted onto a web page is potentially accessible world-wide.

It is important that the composure (and forwarding) of emails is given careful consideration as what goes into an email, is effectively recorded data – see Recording Data section above. Therefore email senders need to ensure that no inadvertent unauthorised sharing of data occurs or that sensitive data or data that a data subject may not feel is fair, accurate and justifiable, is sent or forwarded. Once the data has left the sender in an email, it is no longer within the college's control and that may be a problem.

Generally speaking, email may be retained by staff as a reference source. However, where data is specific to a particular data subject, there should be a formal retention policy in place in respect of where that email trail is stored. Ideally, this should be in a sub-directory or sub-folder that can be easily identified and can therefore be managed. Specific policies should be in place for the deletion of relevant emails relating to a particular subject at a pre-defined point in time – for example 12 months after a conference booking.

It is the college's general policy that emails in a user's in-box should be automatically deleted when the email is 24 months old. Therefore users should save the email elsewhere if its retention is required beyond 2 years.

Data Cleaning
Prior to any data cleaning, HODs should give consideration to the historical value of the data. See the section below on Archives.

HODs will need to determine the appropriate routine and timescale for checking through databases and all other data storage media. Regularity and reasonable frequency is important and a consistent approach is vital. The timescales will vary from department to department and from process to process. However, having determined and set the retention period for specified data, the HOD must ensure that the policy is adhered to.

Data cleaning includes correcting inaccuracies found in data that is to be retained as it is still within the data retention period. If in processing data you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform your HOD. Action should then be taken to resolve the dispute or correct the inaccuracy.

The process of cleansing data that is no longer to be retained will vary from department to department. Some data may be simply over-written, others deleted and others anonymised. The HOD must determine which is appropriate and devise a system and process within the department policy to carry this out.

It should be noted that similar routines must be carried out in respect of **hardcopy/printed paper records** – also considered to be data cleaning. In this process records may need to be destroyed at the end of their retention period. However, it may be that the documents should be transferred to a master file initially rather than be destroyed at this time – see *Inter-departmental cross-referencing – Manual storage systems* below.

Anonymising data
Database systems may limit the ability to remove data because of the effect of creating incomplete records. It may therefore be necessary to anonymise field data rather than delete it. The HOD should agree with the IT Manager the best way to effect this cleaning process and then add the agreed procedure to the departmental policy.

Archives
The Data Protection Act provides that personal data held for historical, statistical or research purposes may be kept indefinitely as long as it is not used in connection with decisions affecting particular individuals, or in a way that is likely to cause damage or distress. This does not mean that the information may be kept forever – it should be deleted when it is no longer needed for historical, statistical or research purposes.

It is the college's position that its current records and data may well form the basis of valuable historical, statistical or research activity in years to come and that therefore before any deletion decision is reached, consideration should be given to determining whether there is value in indefinite retention.
The Library and Archives Committee will give guidance on the kind of data that might qualify and in accordance with that advice, HODs will submit samples of data from time to time for consideration and decision. The Library and Archives Committee will make the final decision and where appropriate, arrange for the transfer of data to the Archive. Such records will then be stored under seal from further processing for a period of time to be determined in each specific case.

Inter-departmental cross-referencing

Software systems - All systems used within the college should be considered with a view to minimising the amount of data duplicated in other systems. Consideration should also be given to which system is authoritative for any given piece of information and the life cycle it is authoritative for. For example: CAMSIS would be considered to be authoritative for most student data until the student finishes their studies at which point the Raisers Edge alumni database may then be considered authoritative, and after a certain period the Archive may then take over being the authoritative source. The IT Department will give guidance on which systems might already exist and which system should be considered authoritative for the data to be stored within the system.

An authoritative system should be one into which data is captured. Thus this is where data changes will be effected. HODs will need to determine in their policy how any such data changes (being in the authoritative system), are communicated to other departments/systems to ensure that all data is consistently accurate.

Where new systems are implemented consideration should be given to their suitability to interoperate with the college's existing systems, so that the transfer of data between systems may be automated, and so that data can be easily exported in machine-readable form in order to comply with data access requests in a timely manner.

Existing systems should be reviewed periodically by each department to make sure that the duplication of data is minimised or automated between systems where practical, and that any new data being stored is recorded on the relevant data register where applicable.

Manual storage systems – As with software systems there should be departmental review on primacy over hardcopy records and files. It is undesirable for there to be duplicate records held in multiple places. For example, the HR department should hold the master personnel file for staff members and this should not be duplicated elsewhere. There may be elements of data that are pertinent to specific functions – e.g. payroll documents – which may therefore be retained in the Bursary.

Sharing data

The college does not share data generally either internally between departments or with third parties without consideration being given to why the sharing is required and whether the data being shared is relevant. Irrelevant data should not be shared – you should just share what is required. That may mean that the process is a little harder while irrelevant data is separated but that is better than inadvertently sharing sensitive data.

Generally the college would not disclose data outside the college to third parties unless it has the data subject's consent unless:

- The sharing is within the frame of the condition for processing – i.e. sharing student data with the University in fulfilment of the student contract
- It is required by law to make a disclosure
- It believes that failure to disclose is likely to prejudice the prevention or detection of crime
- It needs to take legal advice or to comply with legal obligations and disclosure of the data is necessary for that purpose
- It needs to disclose the data for its legitimate business interests (where no harm will result to the data subject).

You should only share data with third parties if you have checked with your HOD and been instructed to do so. Where the college "routinely" shares data with third parties, this should be noted in the

relevant DPS. In relation to former staff, data will be held in the HR; data may also be elsewhere, in order that the college can deal accurately with any reference request and also as a way of maintaining a complete historical record.

Third Parties that handle college data
HODs must ensure that, where a data processor processes data on the college's behalf (e.g. a mailing agency, for example), there is a written contract between the parties which specifies that the processor agrees to act on the college's instructions and to abide by the provisions of the DPA and the GDPR in connection with data security. Further guidance on appropriate terms for such a contract can be obtained from the CDPL. Such an arrangement should be disclosed in the DPS.

Request to view data we hold
All Data Subjects, including staff members who are data subjects, will on most occasions have the right to have copies of or a report (depending on the type and format of the original data) on personal data that is being kept about them either on computer or in 'relevant' manual filing systems. Confidential references given by the college cannot be accessed in this way.

Any person who wishes to exercise this right should complete an access request form and forward it to the CDPL. The college may levy a charge (currently up to £10), which will be revised and published from time to time on each occasion that access is requested.

Where required to do so under the law, the college will aim to comply with requests for access to personal information from data subjects as quickly as possible but will do its best to ensure that it is provided within 40 days from the date of the request. The college does not have to comply with repeated requests unless the requests are at reasonable intervals.

Note: The college can withhold information where the information identifies third parties who have not consented to the disclosure.

Access rights also mean that the confidentiality of references provided either internally or for external bodies can no longer be assumed (even though we do not have to disclose them). This should be borne in mind when references are drawn up.

Marketing and Development Processes

Sending electronic marketing messages
If the college wishes to send electronic marketing messages (by phone, fax, email or text), use cookies, or provide electronic communication services to the public or to companies/organisations, it needs to be aware of the Privacy and Electronic Communications Regulations (PECR), which sit alongside the Data Protection Act. They give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

Departments that undertake such activity will need to be specifically briefed on the provisions of PECR to ensure that the rules are not infringed. Prior to undertaking any such marketing activity, the CDPL should be consulted so that appropriate processes can be put in place.
For more information, HODs should consult the Direct Marketing Guide issued by the Information Commissioner's Office: https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf.

Policy Support and Management

Training
All staff who, as part of the job, process personal data, will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar on a regular basis. It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of training is compulsory

Reporting breaches
All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Information Commissioner's Office (the supervisory authority) of any compliance failures that are material either in their own right or as part of a pattern of failures

Please report any instances (even if you are not sure) to the CDPL.

Monitoring
Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply
The college takes compliance with this policy very seriously. Failure to comply puts both you and the college at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the CDPL. However, as an aide-memoire, the following list of staff obligations should serve to help you keep within the policy parameters:

If you process data:

- Ensure that any personal data which you hold is kept securely, particularly sensitive data
- Ensure that any personal data is not disclosed either orally or in writing, intentionally or otherwise to any unauthorised third party

- Take particular care when removing personal data from college premises, for example to work on at home. You should be aware that this policy and your responsibilities under it apply when data is processed under such circumstances. Off-site use of personal data presents a potentially greater risk of loss, theft or damage to personal data

All staff (even those who do not process data):

- Ensure that any personal data that you provide to the college in connection with your employment is accurate and up-to-date
- Inform the college of any changes to your personal data for which they are responsible, for example, changes of address. (The college cannot be held accountable for errors arising from changes about which it has not been informed.)

Types of Data Subject

a) Pre-applicants and applicants (pre-offer) to be done in conjunction with the University
b) Applicants (post offer)
c) Students
d) Alumni and supporters
e) Senior members and staff
f) College visitors and guests (includes conference, chapel, archives, library)
g) Commercial customers and suppliers (includes tenants and contractors)

Selwyn College Cambridge

Current Retention Schedule (subject to completion and amendment)

1. Pre-applicants and Applicants

Type of Record	Retention Period	Reason for Period
Unsuccessful student applications and interview reports	This information will be retained by the College for as long as it remains relevant. In the case of unsuccessful applications this normally means that files will be destroyed on the 15th October in the year following application.	Provision of feedback and answering queries. Consistent with University policy

2. Students

Type of Record	Retention Period	Reason for Period
Student records, including academic achievements and conduct and financial records, contact details, bank details, dietary requirements and access requirements. (Camsis)	At least 6 years from the date the student leaves the College, in case of litigation for negligence.	Limitation period for negligence Accounting and Audit rules
Student records: Application form, references received, Formal Interview records, References provided, Supervision records, Academic achievement records	Permanent	Historical
Student records: Information about disabilities, allergies and other medical conditions requiring special arrangements	3 years after student leaving date	Limitation Act 1980
Student records: All minor disciplinary records, mitigating circumstances documentation, routine correspondence and permissions, routine correspondence relating to exams	3 years after student leaving date	

Student records: Medical consultation and treatment records		Limitation Act 1980
Personal and academic references	8 years after leaving	NHS Guidance
Residence lists and room records	A minimum of 10 years	Permits the College to provide references for a reasonable length of time.
		Limitation Act 1980
	6 years	While personal and academic references may become 'stale', some data e.g. transcripts of student marks may be required throughout the student's future career. Upon the death of the data subject, data relating him/her ceases to be personal data.
	Certain personal data may be held in perpetuity	
		Fundraising requests (e.g. campaigns, gifts) and recording donations (e.g. gifts, pledges, legacies)
	In perpetuity	Sending event invitations and hosting events (e.g. dinners, talks, concerts, reunions)
		Sending out publications (e.g. newsletters, Annual Report, Selwyn Calendar)
	In perpetuity	Careers advice
	In perpetuity	

	In perpetuity	
Student awards and bursaries	Current students + 6 years	Limitation Act 1980
Student Loans Company	Current students + 6 years	Limitation Act 1980
Student bills and financial information	Current students + 6 years	Limitation Act 1980
Student paper files	Permanent	Historical
Tenancy agreement and tenants' details	End of tennancy + 6 years	Limitation Act 1980

3. Alumni and Supporters

Type of Record	**Retention Period**	**Reason for Period**
Alumni and other supporter records, including contact details, bank details, dietary requirements and access requirements (Raisers' Edge Database)	In perpetuity	Fundraising requests (e.g. campaigns, gifts) and recording donations (e.g. gifts, pledges, legacies) Sending event invitations and hosting events (e.g. dinners, talks, concerts, reunions) Sending out publications (e.g. newsletters, Annual Report, Selwyn Calendar) Updating contact detail changes Enabling fellows to keep in contact with alumni/supporters
	.	

4. Senior Members and Staff

Type of Record	**Retention Period**	**Reason for Period**
Applications for academic posts (including Research Fellowships)	6 months from the date of successful appointment. Data for unsuccessful applicants will be destroyed at this time.	Time limit on litigation
Personnel and appraisal files Employee personal files	7 years from the end of the employment by the College. Duration of employment + 6 years	References and potential litigation Limitation Act 1980
Facts relating to redundancies where less than 20 redundancies	7 years from the date of redundancy	Time limit on litigation
Income tax and NI returns	At least 7 years after the end of the financial year to which the records relate.	Income Tax (Employment) Regulations 1986

Statutory maternity pay records and calculations	At least 7 years after the end of the financial year to which the records relate	Statutory Maternity Pay (general) Regulations 1986
Statutory sick pay records and calculations	At least 7 years after the end of the financial year to which the records relate	Statutory Sick Pay (general) Regulations 1986
Wages, and salary and tax records	7 years	Taxes Management Act 1970
Accident report forms	3 years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979 RIDDOR 1985
RIDDOR	3 years after the date of the last entry	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995
RIDDOR investigations	3 years after the date of the last entry	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995
Health records	During Employment	Management of Health and Safety at Work Regulations
Health records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances hazardous to Health regulations	40 years	Control of Substances Hazardous to Health Regulations 1985
Employee records, including contact details, bank details, dietary requirements and access requirements	In perpetuity	Fundraising requests (e.g. campaigns, gifts) and recording donations (e.g. gifts, pledges, legacies) Sending event invitations and hosting events (e.g. dinners, talks, concerts, reunions) Sending out publications (e.g. newsletters, Annual Report, Selwyn Calendar)
Fellow records, including contact details, bank details, dietary requirements and access requirements	In perpetuity	Fundraising requests (e.g. campaigns, gifts) and recording donations (e.g. gifts, pledges, legacies) Sending event invitations and hosting events (e.g. dinners, talks, concerts, reunions) Sending out publications (e.g. newsletters, Annual Report, Selwyn Calendar) Enabling alumni to keep in contact with fellows

Fellows' correspondence (held by the Master's Assistant)	Current academic year + 6 years	Limitation Act 1980
Fellows' bills	Current financial year + 6 years	Limitation Act 1980
Pension records	Retirement age + 6 years OR 5 years after last action/death if pension has been paid	Data Protection Act 1998 / Scheme rules
Staff lists (names, dates of service, job titles)	Permanent	Historical

5. College visitors and Guests

Type of Record	**Retention Period**	**Reason for Period**
Guest registration forms (accommodation)	12 months	Immigration (Hotel Records) Order 1972 (and subsequent amendments)
Booking forms (all conference organisers, both internal and external)	3 years	Look back at history for repeat bookings
Email query information from guests	2 years	To compare repeat booking information
Client information on Pro-forma invoices	3 years	Look back at history for repeat bookings
Contractor and visitor sign in sheets (Porters' Lodge)	6 months	Only need to hold for a limited period if there are short term issues, such as keys not returned
Contractors and suppliers information	This information will be retained by the College for as long as it remains relevant.	Current suppliers are kept whilst working with the College. Ex-suppliers, contact information held for possible reinstatement

6. Commercial customers and Suppliers

Type of Record	**Retention Period**	**Reason for Period**
CCTV footage DUPLICATED	28 days	To allow sufficient time for a crime or serious event to be discovered and investigated.
Library Management System DUPLICATED	Records of former students are retained for 2 years	In case a student returns for further studies later
Professional advisers' files	Current calendar year + 6 years	Limitation Act 1980
Purchase invoices (Bursary masters)	Current financial year + 6 years	Limitation Act 1980

Purchase invoices (department copies)	Current financial year + 1 year	Operational
Purchase invoices (department copies, high value items)	Current financial year + 6 years	Operational

7. College IT Systems

Type of Record	**Retention Period**	**Reason for Period**
CCTV footage	28 days	To allow sufficient time for a crime or serious event to be discovered and investigated.
Network Access Logs (firewall)	45 days	For diagnostic purposes, and to allow the College to comply with University CERT requests
RADIUS (eduroam) Logs	45 days	For diagnostic purposes, and to allow the College to comply with University CERT requests
Website Analytics	26 months	To provide performance and usage statistics for continual improvement of website content.
IT Helpdesk Request System	Indefinitely	For reference knowledge base of previous incidents
Maintenance Request System	Indefinitely	For reference knowledge base of previous incidents
IT Purchase Order System	10 years	For budgeting and asset tracking purposes
'My Documents' file store	Within 1 year of users account being cancelled	For HOD to access files from previous employee.
Shared Drive file store	As per departmental policy	Defined by department or otherwise stated in retention scheduled. Managed by department.
CCTV footage	28 days	To allow sufficient time for a crime or serious event to be discovered and investigated.
Library Management System	Records of former students are retained for 2 years	In case a student returns for further studies later

8. College Administration

Type of Record	**Retention Period**	**Reason for Period**
Annual Report	1 copy to Archives	Historical

Buildings O&M Manuals	File kept for life of the building. Updated as required	Active document
Buildings contracts and projects files (major projects)	File kept for the life of the buildings	Historical
Buildings routine maintenance	6 years	Limitation Act 1980
Building plans (as built)	Permanent	Historical
Building plans (draft)	12 years after end of project	Limitation Act 1980
Car park permits	Current	Data Protection Act 1998
Chapel term cards and service sheets	1 copy to Archives	Historical
Chapel service sheets for special events	1 copy to Archives	Historical
Chapel service registers	Permanent	Historical
Chapel marriage registers	Permanent	Historical
Choir members' files	Duration of membership of Choir	Safeguarding policy/Limitation Act 1980
Choir members' basic details	Permanent	Safeguarding policy/Limitation Act 1980
Friends of the Choir scheme	Permanent	See Raisers' Edge
College policies (each final version)	Permanent	Historical
Committee minutes	Permanent	Historical
Committee papers	Permanent ? 1 copy to Archives	Historical
COSHH datasheets	Current + 6 years	Limitation Act 1980
Council minutes	Permanent	Historical
Council papers	Permanent	Historical
Conservation records	Permanent	Historical
Electrical testing records (PAT testing)	Current year ?	Electricity at Work Regulations 1989
Email general Inbox/Sent messages	3 months maximum (items that need to be retained for a longer period should be moved to structured files)	Operational
Event planning	Current + 2 years	Operational
Event photographs		Operational
Fire alarm testing	1 year	Regulatory Reform (Fire Safety) Order 2005
Fire drills		Regulatory Reform (Fire Safety) Order 2005
Fire risk assessments	Current	Regulatory Reform (Fire Safety) Order 2005

FOI enquiries	2 years	
Fuel records	Current + 6 years	Dangerous Substances and Explosive Atmospheres Regulations 2002
Function sheets	Current	Operational
Gas appliance safety checks	2 years	Gas Safety (Installation & Use Regulations) 1998
Health & Safety audits	Current + 6 years	Health & Safety at Work Act 1979
Health & Safety policies	Permanent	Health & Safety at Work Act 1979
Health & Safety risk assessments	Current + 6 years	Health & Safety at Work Act 1979
Insurance policies	40 years	Limitation Act 1980
Insurance claims	6 years after settlement or withdrawal of claim	Limitation Act 1980
Investment files	6 years	Historical
Job descriptions	1 copy to Archives	Historical
Leaflets	1 copy to Archives	Historical
Legacies (unconditional)	12 years after last action	Limitation Act 1980
Legacies (conditional)	Permanent	Operational/Historical
Legionella testing, risk assessments etc.	Current year + 6 years	Health & Safety at Work Act 1979 + HSE Guidance L27
Library stock records	Current + 1 year	Operational
Master's correspondence files	6 years	Operational
Menus	1 copy to Archives	Historical
Newsletters	1 copy to Archives	Historical
Photographs	Permanent	Historical
Pesticide records	Current	Operational
Pesticides, controlling and monitoring exposure	5 years	Limitation Act 1980
Plans (as built)	Permanent	Historical
Plans (draft)	12 years after end of project	Limitation Act 1980
Policies (each final version)	Permanent	Historical/Legal
Portraits	Permanent	Historical
Property files	Permanent	Historical
Publications, leaflets, brochures and other printed material	Permanent	Historical
Service records for equipment and vehicles	Permanent	Health & Safety at Work Act 1979

Statutes	Permanent	Historical
Statutory Accounts	Permanent	Historical
Title Deeds	Permanent	Historical
Trusts	Permanent	Historical
Unsolicited applications for employment	1 year	Limitation Act 1980
Waste disposal certificates (non hazardous)	2 years	The Environmental Protection (Duty of Care) Regulations 1991
Waste disposal certificates (hazardous)	3 years	The Environmental Protection (Duty of Care) Regulations 1991

Notes:

The two main sources of legislation that affect general records retention are:

The Limitation Act 1980 – which sets out the times after which claims against the College will be extinguished. For most transactions, the time limit is 6 years, except for some contracts and property transactions, personal injury claims and defamation.

The time limit for personal injury claims is 3 years from the time of the incident, except when the damage (for example from exposure to asbestos) does not become known until later. Thus, the time limit for health surveillance is much longer. For minors, the time limit does not start to run until they are 18.

The GDPR 2018 – which requires the College to not to keep personal data for longer than is necessary. What is "necessary" is defined as the period required to protect the College's interests, which is usually related to the Limitation Act 1980.

Where there is a duty to keep a record and no specific and clear retention period in legislation, a limit has been set according to the purpose that the record is kept for.