POLICY DOCUMENT

POLICY: **Data Protection**

DEPARTMENTS AFFECTED: **All**

ISSUED BY: **College Steward**

DATE: **April 2018**

Introduction

We hold personal data about our students (and potential students), Fellows, employees, clients, suppliers and other individuals for a variety of purposes.

This policy sets out how we seek to protect personal data and ensure 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 (sDPO) and/or the College Data Protection Lead (CDPL) 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

College purposes/ needs	The purposes for which personal data may be used by us: Academic, Development, human resource management, administrative, financial, regulatory, payroll and business development purposes. College purposes include the following: ○ Tutorial processes including students' enrolment, personal contact information, course information, tutorial routines, examination administration and results ○ Senior and Junior Members' and visitors' accommodation arrangements ○ Junior members' health, welfare and disciplinary matters ○ Stewardship/Alumni relations and fund-raising activities ○ Financial reasons, such as recording transactions, raising invoices, security vetting, credit scoring and checking ○ Business development and event booking processes for commercial conference and accommodation activity including marketing activity ○ Compliance with our legal, regulatory and governance obligations and good practice ○ Transacting the business of the College (such as through email and other forms of correspondence). ○ Employment of personnel, checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments ○ Monitoring staff attendance, conduct, disciplinary matters ○ Building and maintaining our historical archive records.
Personal data	Information relating to identifiable, living, individuals, such as student applicants, current and past students, alumni, "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 we gather 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.
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.
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.
Processing data	Capture/collection, storage, use, updating, copying, sharing, deletion of data are all ways of processing data. This list is not exhaustive.
Data Subject	An individual about whom personal data is held by the College.
Category of Data Subject	Groups of subjects – e.g. Students, Employees, Conference Organisers, Conference/B&B Guests, Suppliers.
Data Controller	The College is the Data Controller.
Data Owner	Any College employee who is responsible for the processing of data in their area – e.g. Head of Department, departmental/line manager. Data Owners are responsible for the implementation of the College policy and procedures within their area.
Data Processor	Any member of staff who processes personal data.
Data Subject Privacy Notice	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. Publishing is usually on the College website and may also be shared with data subjects directly.
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.
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.

Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms. This policy supplements our other policies relating to internet and email use (see Staff Handbook and Website http://www.robinson.cam.ac.uk/college-life/it/network-usage-rules). We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

College Council authorises this policy and reviews it every 5 years or more frequently if there is a significant change. The College Data Protection Lead (CDPL), currently the College Steward, has overall responsibility for the day-to-day implementation of this policy. The CDPL will liaise and seek support or guidance from the Statutory Data Protection Officer sDPO, this role is filled by the Office of Intercollegiate Services (OIS).

Responsibilities of the Statutory Data Protection Officer:

- To inform and advise the College and the employees who carry out processing of their obligations pursuant to the Regulation(s)
- To monitor compliance with this Regulation(s), 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 pursuant to Article 35
- To cooperate with the supervisory authority [the Information Commissioner's Office (ICO)]
- To act as the contact point for the supervisory authority [the ICO within 72 hours of the incident] on issues relating to processing [and particularly reportable personal data breaches], including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter
- To investigate and manage complaints from data subjects and to facilitate them in exercising their rights

Responsibilities of the College Data Protection Lead:

- Liaising with the sDPO as required – note the table below indicating how the sDPO and the CDPL work together
- Reviewing all data protection procedures and policies on a regular basis including conducting internal audits
- In liaison with the sDPO, arranging data protection training and advice for all staff members and those included in this policy
- Responding to individuals such as students and employees who wish to know which data is being held on them by Robinson College
- Checking and approving with third parties that handle the College's data, any contracts or agreement regarding data processing – this may be delegated to Heads of Department.

Tasks for sDPO (OIS)	Tasks for College CDPL
Provision of advice in complex cases of data protection.	Manage **subject data access requests**. Manage all **data subject rights** requests.
Assessing whether a **data breach** is reported to the ICO. Managing a breach with the ICO, including all communications and risk assessments. Maintaining records of all breaches for reporting to the individual College.	Managing the impact of a data breach within the College, and implementing any internal or external recommendation. Reporting all breaches to the sDPO.
Supporting a College in reporting a data breach crime to the police.	Liaising with the police if there is a crime.
Reviewing breaches across all Colleges to identify risks and trends.	Determining and implementing risk measures to reduce likelihood of breaches occurring.
Provide face-to-face data protection awareness **training to College staff**, supplementing on-line training available from the University and internal training by the College	Ensure that staff are appropriately and proportionally trained, depending on their roles.
Provide face-to-face data protection awareness **guidance to governing bodies**	
Annual development and review of training and awareness courses	Advise sDPO on nature of training gaps.
Undertake paper-based **audit** of College documentation and procedures, review governance risk rating and produce an appropriate report for the College	Assist sDPO in provision of information. Create, update and maintain appropriate records (including DP statements, asset registers, risk register).
Undertake an **audit visit** for Colleges with identified high-risks, involving attendance at the College, interviewing appropriate personnel and producing an appropriate report	Facilitating audit visit of sDPO.
Advising on **data protection impact assessments**	

Responsibilities of the IT Manager

- Checking and scanning Robinson security hardware and software regularly to ensure it is functioning properly
- To provide an advisory/consultancy service on matters relating to hardware/software and in respect of the College Website for College staff.

Responsibilities of Heads of Department

- Conducting data audits as required by the CDPL on personal data collection and processing and on personal data sharing and transmission
- Drafting departmental policy in respect of data subject types; the personal data collected; the lawful condition(s) for processing the data used in each case – see Conditions for processing below; storage and retention of data
- Approving data subject privacy notices to be published, attached to emails and other copy
- Ensure 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 process the College's data, any contracts or agreement regarding data processing and sharing

- Addressing data protection queries from departmental contacts, members, alumni, target audiences
- Ensuring that departmental staff members are fully briefed on the departmental policy in respect of data processing.
- Coordinating with the CDPL to ensure all initiatives adhere to data protection laws and the College's Data Protection Policy.

Responsibilities of all Employees

- Ensure that you understand this policy and that you adhere to its terms.
- You must keep personal data secure against loss or misuse.
- Ensure that you process personal data accurately. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform your HOD and/or the CDPL – see procedures below.
- You are a data subject as an employee. You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the HR Manager so that your records can be updated.

General Principles

There are 8 general principles as set out below.

1. Fair and lawful processing

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

1.1 Conditions for processing

We will ensure any processing of personal data is justified using at least one of the conditions for processing and 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 Data Subject Privacy Notice (DSPN).

a. ***Consent*** The data that we collect 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 conference 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 Robinson 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 we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are 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 CDPL.

2. Data collected for specified and lawful purpose

We will ensure that we are clear about why we process personal data and what we intend to do with it. We will ensure that we provide details of our data processing to the data subjects through our DSPNs. There may be a DSPN for each category of data subject.

We 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

We will ensure that any personal data we process is relevant, adequate not excessive, given the purpose for which it was obtained.

4. Accurate and up to date

We will ensure that any personal data we process is accurate. Individuals may ask that we correct inaccurate personal data relating to them.

5. Data retention

We 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 our data retention policies. We will set out our retention policies in our Records Retention Schedule and wherever possible we will also provide that detail in our DSPNs.

5.1 Data Retention Guidelines

Personal data will need to be retained for longer in some cases than in others. How long we retain 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 CDPL 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 in the *Fair and Lawful Processing* section above, then we 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, we should consider whether we need to keep the information once the relationship ends, e.g. a conference client.

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

In some cases, we may need to keep personal data so we can defend possible future legal claims. However, we 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 we keep 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.

6. Rights of Data Subjects

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

6.1 Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. We must provide individuals with information including: our purposes for processing their personal data, our retention periods for that personal data, and who it will be shared with. We must provide privacy information to individuals at the time we collect their personal data from them.
We do this through the publication of Privacy Notices for each category of data subject we deal with – see Data Subject Privacy Notices section below.

6.2 Right of access requests

All Data Subjects, including staff members who are data subjects, will on most occasions have the right to have copies of or a report on personal data (depending on the type and format of the original 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.
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.
If you receive a data subject access request, you should refer that request immediately to your HOD and the CDPL – see procedure below.

6.3 Right to rectify inaccurate information

An individual has a right to ensure that the information we hold is accurate and require us to correct any inaccuracies.
If you receive advice that information is inaccurate or a request to correct information, you should refer the matter immediately to your HOD and the CDPL – see procedure below.

6.4 Right to erasure/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 – see procedure below.

6.5 Right to restrict processing of data

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, we are still permitted to store the personal data, but not to use it.
If you receive such a request, you should refer that request immediately to your HOD and the CDPL – see procedure below.

6.6 Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
The right to data portability only applies to personal data an individual has provided to a controller;
where the processing is based on the individual's consent or for the performance of a contract; and
when processing is carried out by automated means.
If you receive such a request, you should refer that request immediately to your HOD and the CDPL – see procedure below.

6.7 Right to object to data processing/withdraw consent

Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.
Individuals must have an objection on "grounds relating to his or her particular situation". We must stop processing the personal data unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims.
We must inform individuals of their right to object "at the point of first communication" and in our privacy notice. This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".
If you receive such an objection, you should refer that request immediately to your HOD and the CDPL – see procedure below.

6.8 Right to not be subjected to automated decision-making

The GDPR has provisions on automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process. This may affect Development Department but probably not any other areas of College.

7. Data security

We must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our 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
- Data stored on CDs or memory sticks must be locked away securely when they are not

being used
- The CDPL 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 may be stored on mobile devices – see Hardware section below
- 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 – see Hardware section below.
- 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 CDPL. 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

These should be practical instructions and tools for HODs and staff to follow.

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
- 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. See Appendix A Form 1

HODs will conduct audits on Personal Data Collection and Processing and on Data Sharing and Transmission. See Appendix A Forms 2 and 3.

Any action that may be highlighted as a result of the audit will be noted and followed through to completion or resolution. See Appendix A Action Required.

HODs will use the audit data to inform their departmental DSPNs.

Data Subject Privacy Notice (DSPN) - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important. We publish a Data Subject Privacy Notice relevant to each element of our activity which:

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

Heads of Department will set out the specific DSPNs, for each data subject type, based upon the details collected in the data audits. DSPNs will be published on the College website and may also be referenced in emails or other mailed information as relevant.

DSPN for Children (under 16) and Young People - We do not currently have cause to collect data on children under the age of 16 apart from any dietary requirements they may have (possibly the student's name). Such children would only be expected in College as part of a school visit where such personal data would be shared with us by their school. We do collect data on Young People over 16 and this is detailed in the STUDENTS Data Register. In respect of the right to be informed, for Young People, we rely upon the general admissions DSPN for applicants as published by the University:
https://www.information-compliance.admin.cam.ac.uk/data-protection/applicant-data.

Collecting/Capturing Data

Before processing any personal data, we should consider the checklist set out below:

- What is the purpose of our collecting this data?
- What is our justification for collecting the data and which condition will apply?
- Do we really need to collect the information? Do we really need to collect all of it?
- Is the information 'ordinary' or is it 'sensitive'?
- Are we authorised to collect/store/process the data – by the College or by the data subject?
- If we need the data subject's consent, have we go it?
- Unless the data has been obtained from a reliable source, have we checked with the data subject that the data is accurate?
- Are we 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.

The HOD will need to determine in the department policy, which elements of data processing require *consent* and how that consent will be sought and recorded. The policy should also detail the duration of the consent and how it will be renewed.

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, Kinetics. These will in most cases be regarded as the master/authoritative data storage system or “source of truth”. Each relevant HOD is expected to determine 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 like Dot Mailer or MailChimp. 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. A Data Sharing Agreement will need to be in place with such providers – discuss with the CDPL.
- E-mail is also a form of data processing and by definition storage. See the section on E-mail below which defines the College policy in respect of email retention. Whilst live, HODs should consider how email storage 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 in the drafting of the department policy. Consider who has access and how access is controlled. Setting of strong passwords is important as is the control of keys to secure filing cabinets.

Hardware

It is acknowledged that data is stored on a variety of hardware and indeed a number of differing platforms. College issued hardware includes workstation PC’s, laptops, tablets and other mobile devices. However, data is also stored on apparatus that is neither owned by the College nor under College control.

College owned laptops will be encrypted to protect against unauthorized access to data should the hardware be lost. Where users have permission to store College data on personal or other hardware – e.g. emails on a personal smart phone – It is the responsibility of the user to ensure that:

- All College data is adequately secured (i.e. Password, passcode, fingerprint unlock, encryption) before the data can be accessed.

- The College's data is removed from the device when authority to hold the data is revoked - e.g. at the end of employment or before the device leaves the possession of the user e.g. is disposed of, or sold.
- The College is informed immediately of any loss or compromise of the device or data stored on it (i.e. Virus infection, or device is lost or stolen)

The College reserves the right to forcibly erase the device where possible to protect the data which may result in personal data also being erased.

The use of Removable USB for storing and transferring personal or sensitive data is highly discouraged, due to the increased risk of the data being lost, and the inability of the College to revoke and protect the data;, instead remote access solutions should be used where possible. Where USB storage must be used, any personal or sensitive data should be password protected before being transferred to the removable storage or the removable storage encrypted, and files deleted on completion.

World Wide Web and E-mail

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 mailbox will be automatically deleted when the email is 60 months old. Therefore users should save the email elsewhere if its retention is required beyond 5 years.

Sharing data

We do not share data generally either within the College (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 only 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 we would not disclose data outside the College to third-parties unless we have 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
- We are required by law to make a disclosure
- We believe that failure to disclose is likely to prejudice the prevention or detection of crime
- We need to take legal advice or to comply with legal obligations and disclosure of the data is necessary for that purpose
- We need to disclose the data for our 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 we do "routinely" share data with third parties, this should be noted in the relevant DSPN and a Data Sharing Agreement between the College and the third-party must be in place

In relation to former staff, data will be held in the Personnel Office; data may also be held in the Catering and Housekeeping Offices, in order that the College can deal accurately with any reference request and also as a way of maintaining a complete historical record.

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 (i.e. The Source of Truth) 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 Archives 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. HOD's 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 part of the data register where applicable.

Inter-departmental cross-referencing - 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 Payroll department.

Third-Parties that handle College data

HODs must ensure that, where a third-party processes data on the College's behalf (e.g. a mailing agency, for example), there is a Data Sharing Agreement in place 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 an agreement can be obtained from the CDPL. Such an arrangement should be disclosed in the relevant DSPN.

Data Cleaning

PRIOR TO ANY DATA CLEANING, HODs should give consideration to the historical value of the data. See the section below on Archives.

This may include the regular and habitual cleansing of data on a cycle – for example, cleaning all data relating to a particular student cohort or year group once the data retention period has been reached.

Data cleaning also 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.

Routine

HODs will need to determine the appropriate routine and timescale for checking through databases and all other data storage mediums. 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.

HODs will need to give consideration to the process to adopt by which other people who hold duplicate data, independent of the department, e.g. Tutors, are instructed to cleanse their copy of data. This may be a detailed instruction by email giving clear direction of the data, the year group/cohort that is to be cleansed.

Cleansing Process

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. Some data that may have current sensitivity but is nevertheless of significant archive value may be passed to the College Archive and be immediately sealed thus ensuring only controlled access under specified circumstances.

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 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 Archives Committee will make the final decision and where appropriate, arrange for the transfer of data to the Archive storage system. Such records will then be stored under seal from further processing for a period of time to be determined in each specific case.

Procedures to ensure Rights of Data Subjects

Request to view data we hold

- Any person (including staff members) who wishes to exercise this right should complete an **Data Subject Access/Change Request Form** (Appendix B) on the College website http://www.robinson.cam.ac.uk/about-robinson/data-protection and forward it to the CDPL. The College does not levy a charge (except where requests are manifestly unfounded or excessive).
- Once the request has been received, the CDPL will liaise with the relevant department(s) to be able to respond to the request.
- 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.
- The College can withhold data where the information identifies third parties who have not consented to the disclosure.
- The CDPL will make a record of such requests and produce an annual summary report.

Request to correct data we hold

- Any person (including staff members) may contact the relevant department if they would like to correct, complete or erase part of the information that we hold about them.
- An individual can make a request for rectification verbally or in writing. The requestor or the staff member receiving the request should complete details of the request on a Data Subject Access/Change Request Form (Appendix B) on the College website http://www.robinson.cam.ac.uk/about-robinson/data-protection and forward to their HOD and the CDPL.
- In certain circumstances the College can refuse a request for rectification. HODs will advise staff accordingly. There may be a requirement to evidence the identity of the requester to ensure that changes are made with due authority. As appropriate, advice may be sought from the CDPL.
- Once the correction has been made, ***under direction from HOD or CDPL***, the staff member should write to the data subject to confirm that the request has been responded to. We have one calendar month to respond to such a request.
- The HOD must notify all other parties within College and any third-parties who process this data of the correction and require them to duplicate the correction.
- The CDPL will make a record any requests made and produce an annual summary report.

Request to be forgotten/have our data records erased

- Any person may make a request for their data to be erased. They may request this either verbally or in writing. The requestor or the staff member receiving the request should complete details of the objection on a Data Subject Access/Change Request Form (Appendix B) on the College website
  http://www.robinson.cam.ac.uk/about-robinson/data-protection
  and forward to their HOD and the CDPL. Further instruction will then be given.
- The right is not absolute and only applies in certain circumstances. Complete erasure may also not be possible within a computerised software record – i.e. anonymization may be adopted instead alongside permissions to process data being removed.
- Once the erasure has been carried out, ***under direction from HOD or CDPL***, the staff member should write to the data subject to confirm that the request has been responded to. We have one calendar month to respond to such a request.
- The HOD must notify all other parties within College and any third-parties who process this data of the erasure/anonymization and require them to duplicate the change.
- The CDPL will make a record any requests made and produce an annual summary report.

Request to restrict data processing

- Any person (including staff members) may make a request for restriction of their data verbally or in writing. The requestor or the staff member receiving the request should complete details of the objection on a Data Subject Access/Change Request Form (Appendix B) on the College website
  http://www.robinson.cam.ac.uk/about-robinson/data-protection
  and forward to their HOD and the CDPL. Further instruction will then be given.
- The restriction will normally be noted within the computerised software record – i.e. permissions will be removed to process data.
- Once the restriction has been made, ***under direction from HOD or CDPL***, the staff member should write to the data subject to confirm that the request has been responded to. We have one calendar month to respond to such a request.
- The HOD must notify all other parties within College and any third-parties who process this data of the restriction and require them to apply the same controls.
- The CDPL will make a record any requests made and produce an annual summary report.

Request for data to be ported

- When requested, and where possible, we must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.
- The HOD and CDPL should be informed immediately and may take advice from the IT Manager as appropriate.
- We must respond without undue delay, and within one month though this can be extended by two months where the request is complex or we receive a number of requests.
- The HOD will be responsible for ensuring this request is carried out and must ***under direction from CDPL***, inform the individual within one month of the receipt of the request or explain why the extension is necessary.
- The CDPL will make a record any requests made and produce an annual summary report.

Withdrawal of Consent/Objection to data processing

- As soon as you receive such an objection or a withdrawal of consent, you must immediately stop processing the individual's personal data for direct "marketing" purposes and notify your HOD or the CDPL about the request.
- The requester or the member of staff will record the request on a Data Subject Access/Change Request Form (Appendix B) on the College website http://www.robinson.cam.ac.uk/about-robinson/data-protection and pass this to their HOD who will review the grounds of the objection. Advice will be sought from the CDPL and/or sDPO as required.
- If the review results in acceptance of the individual's objection, permissions will be withdrawn from the computerised system in order to prevent any further data processing of this nature.
- The HOD must notify all other parties within College and any third-parties who process this data of the restriction and require them to apply the same controls.
- The HOD must make a record of the objection/withdrawal of consent which should be retained for future reference. This record will be created in conjunction with the CDPL.

Policy Support and Management

Training

There has been significant training opportunities in the lead up to the implementation of GDPR in May 2018. A number of staff have already benefited from attending such externally provided briefings. Formal internal training will take place in College, to be delivered by the College Steward and IT Manager. Additionally, the University provides an on-line training course which all data owners and data processors will be required to "attend"

Training for Heads of Department and other Data Owners

It is recognised that some data owners will have significantly more involvement than others and may therefore need more in-depth training. All data owners will be briefed on the basis of the following content and this will be supplemented as required. Training will be compulsory.

Content of training will include:

Outline briefing of the law - Principles and Conditions for processing data
College Policy - Definitions, Responsibilities, Procedures
Data Register/audits - Privacy Notices, Retention periods, Action Plans
Managing data - Culling, Future operations
Individuals Rights - Managing requests
CU On-line Training

Training for Data Processors

All staff who, as part of their 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/or procedures. Training will be compulsory.

Content of training will include:

Outline briefing of the law - Principles, Conditions for processing data adopted in College
College Policy - Definitions, Responsibilities, Procedures - Accuracy/Security
Privacy Notices - Individual Rights and managing requests
CU On-line Training

Briefing for All Staff

All Staff will have the opportunity to be briefed on the policy and how it affects them as employees and data subjects. The briefings will be held from time to time and will include:

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

Data Protection Compliance

Reporting breaches of data security

All members of staff have an obligation to report actual or potential data protection compliance failures AS SOON AS POSSIBLE. 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 (ICO - 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 immediately. The CDPL/SDPO is required to report the matter to the ICO within 72 hours.

What is a breach?

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Monitoring

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

Consequences of failing to comply

We take 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 aid 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.)

Approved by College Council April 2018

Appendix A Personal data register [Department/Function]

Data audit form 1 - DATA SYSTEMS OVERVIEW

Add as namy rows as you need to in order to compile a complete record. (This information will be used to create appropriate data protection statements and data retention schedules.)

#	System Name	System Owner	Department Users	System Overview / Use	Personal Data / Sensitive Personal Data	Data subject types *[see below for types]*	Host location	Format (e.g. software platform)	Notes
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									

a) pre-applicants

b) applicants

c) students (a College may want to separate undergraduate students and postgraduate students)

d) alumni and supporters (a College may want to separate these)

e) Fellows, employees and workers (a College may want to separate these)

f) conference organisers and guests (a College may want to separate these)

g) general visitors

h) commercial tenants

i) College companies

j) chapel attendees or users

Appendix A Personal data register [Department/Function]

Data audit form 2 – <u>PERSONAL DATA COLLECTION AND PROCESSING</u> Data subject type

_____

In the following table, please try to collate <u>all</u> data and information you collect and use for the "data subject type" specified above.
Add as many rows as you need to in order to compile a complete record. (This information will be used to create appropriate data protection statements and data retention schedules.)

#	**Condition**	**What do you do with personal data?** (record all purposes)	**What type of data do you collect/store?**	**Where do you get the data from?**	**Where do you store it?** (record all places HARDCOPY AND ELECTRONIC)	**How long do you keep it for?**	**Cross-reference to other purposes (#) & PRIVACY IMPACT**
		Example: *Create a new student file/student College ID*	*Full name, age and date of birth*	*The student (application form)*	*CamSIS, tutorial file, payroll system… … …*	*For the lifetime of the College (i.e. permanently)*	*all other purposes*

Appendix A Personal data register [Department/Function]

Data audit form 3 – <u>PERSONAL DATA SHARING AND TRANSMISSION</u> Data subject type

_____

In the following table, please try to collate <u>all</u> data and information you share with third parties (including the University) for the "data subject type" specified above.
Add as many rows as you need to in order to compile a complete record. (This information will be used to create appropriate data protection statements and data sharing agreements.)

#	Who do you share personal data with (third parties)?	What personal data do you give them?	When do you share it and for what purpose(s)?	What written agreement(s) exist to cover the sharing of the data?
	Example: *Local city council*	*Full name, age and date of birth*	*Annually provided for the purposes of council tax exemption eligibility*	*Data sharing agreement, dated 1 October 2015*

#	Who do you share personal data with (third parties)?	What personal data do you give them?	When do you share it and for what purpose(s)?	What written agreement(s) exist to cover the sharing of the data?

Appendix A Personal data register [Department/Function]

ACTION REQUIRED

#	ACTION	BY WHOM

Appendix B Data Subject Access/Change Request Form

The following information is needed to help us give a quick and accurate response to your enquiry. Please complete the information below and return the form by post or email to the Data Protection Officer (contact details are provided below).

Part A. Your request

Title:	
Surname:	
Forename(s):	
Address:	
Telephone number:	
Email address:	
Other name by which you have been known, if applicable:	
Relationship to the College:	

Please provide a description of your request, and any further information which will enable us to locate your personal data (continue overleaf if necessary).

Part B. Proof of identity

Data Protection legislation requires the College to satisfy itself as to the identity of the person making the request. Please send a photocopy of one form of identification containing a photograph (e.g. University Card, Passport, Photocard Driving Licence) to the Data Protection Officer. If the supply of this documentation is problematic please contact us to discuss alternative proof of identity arrangements. If the College is unable to satisfy itself as to your identity from the documentation you send us, we will contact you as soon as possible.

Part C. Declaration

I am the Data Subject named in Part A of this document, and hereby request, under the provisions of Data Protection legislation, that Robinson College provides me with copies of my personal data as described in Part A.

I have provided my proof of identity.
Signature: …… Date: ……

Please return this request to:

Data Protection Officer

Robinson College, Grange Road, Cambridge CB3 9AN

Tel: 01223 339100

data.protection@robinson.cam.ac.uk