Ruskin College
Oxford

DATA PROTECTION POLICY

Created: May 2012
Approved: Governing Executive
Last Reviewed: May 2018
Responsibility for Review: Governing Executive
Date of Next Review: July 2021

1.0 Data Protection Policy

1.1 Related controlled and advisory documents

- General Data Protection Regulation (GDPR) and related acts of parliament.
- Data Breach Policy and Procedure
- Requirements of Validating and Professional Bodies.
- Admissions Policy
- IT Policy
    - o IT Rules and Regulations
- Social Media Policy
- CCTV Policy
- Appeals and Complaints Policy (emerging complaints and compliments policy)
- GDPR Data Map
- Ethics consent form

2.0 Introduction

2.1 This policy relates to anyone who process personal information including staff, students and contractors. In addition the GDPR introduces an 'accountability' principle, this ensures that Data Controllers (Ruskin College) are responsible for, and can demonstrate and verify their compliance with personal data legislation.

2.2 If in any doubt as to the applicability or meaning of this policy or of the regulation, contact the relevant data co-ordinator or the Data Protection Officer (dataprotection@ruskin.ac.uk)

2.3 Principles. The College adheres to the principles of both the superseded UK Data Protection Act and the European General Data Protection Regulation. In accordance with these principles personal data shall be:

Data Protection Act 1998	General Data Protection Regulation 2016 The GDPR becomes enforceable on the 25th May 2018 - http://ec.europa.eu/justice/dataprotection/reform/index_en.htm
Processed fairly and lawfully	Processed lawfully, fairly and in a transparent manner in relation to individuals
Processed for specified purposes only	Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
Adequate, relevant and not excessive	Adequate, relevant and limited to what is

	necessary in relation to the purposes for which they are processed
Accurate and up to date	Accurate and, where necessary, kept up to date; whilst having regard to the purposes for which data is processed, every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay
Not kept longer than necessary	Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
Processed in accordance with data subjects' rights	GDPR does not contain a specific principle relating to individuals' rights - these are specifically addressed in separate articles (see GDPR Chapter III - https://gdprinfo.eu/chapter- 3/)
Processed and held securely	Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Not transferred outside the countries of the European Economic Area with adequate protection	GDPR does not contain a specific principle relating to overseas transfers of personal data - these are specifically addressed in separate articles (see GDPR Chapter V - https://gdpr-info.eu/chapter-5/)

3.0 Scope

3.1 The scope of this policy covers all personal data that is processed, stored, sent or recorded, in any way, throughout Ruskin College or to any third party. As a data controller, Ruskin College needs to collect and process information, including personal data, about the people that it deals with in order to operate effectively and efficiently.

3.2 The policy has been written to ensure that all members of the College comply with data protection legislation Ruskin College processes information to allow the College to meet its legal requirements to:

- funding bodies
- validating and awarding bodies
- provide education and support services to its students, professional learners, staff and alumni
- manage our accounts and records
- provide commercial activities to our clients
- undertake research
- advertise and promote the College and the services we offer
- publish College and alumni materials
- and to undertake fundraising.

3.3 The information processed may relate to past, present and prospective data subjects. The College also processes personal information through CCTV systems, detail of which may be found in the CCTV policy.

This policy applies regardless of where the personal data is held or whether it is held in hard copy or electronically.

4.0 Definitions

GDPR – Stands for the General Data Protection Regulations. These are an EU wide Regulation governing personal data. The full legislation can be found here.

Data Controller – Means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (Article 4 (7)). In this case the controller is Ruskin College.

In this instance the College is the Data controller who is registered with the Information Commissioners Office (ICO).

Data Protection Officer (DPO) – Is a designated person within the College and is the contact point for enquiries/enacting your rights under the legislation. They advise the College on compliance with the legislation. The role of the DPO can be seen here.

Data – In the terms of the Act data is information relating to an individual where the structure (e.g. its encryption status, format or contents) of the data allows information about the individual to be readily accessed. The information may be held in hard copy (e.g. as written notes relating to a person or as part of a manual filing system structured by name, address or other identifier) or in a form capable of being processed electronically.

Data Subjects – Refers to a natural person (individual) who is the subject of personal data. Therefore the data subject is the person whom the personal data is about, (this could include students, staff, Alumni, Customers and suppliers). The GDPR does not cover deceased individuals or data that cannot be identified or distinguished from others.

Data Co-ordinators – The College has designated data co-ordinators who manage various areas of the College. These are mainly heads of departments who will have an overview of the process and data within their department; in liaison with the Data Protection Officer they keep the use of data within their departments within legal guidelines.

Data Processing - 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; (Article 4(2)).

Anything that the College does with personal data could therefore come under the definition of data processing.

Personal Data – means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (Article 4 (1)). It covers any data relating to a living person.

Sensitive Personal Data – This is a subset of personal data that relates to a living person, recording such things as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, criminal convictions, sex and genetic and biometric come under sensitive personal data and require additional criteria for processing.

5.0 Procedure

5.1 All

The College expects all its members to comply fully with its Data Protection Policy, the law and all other related processes (as outlined in the data map) and policies.

To ensure the lawful processing of personal information, anyone processing personal data must comply with the enforceable principles of good practice, which state that personal data shall be (taken from article 5 of the General Data Protection Regulations):

- Obtained and processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy)

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (storage limitation)
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised and unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality)
- The data controller shall be accountable for and be able to demonstrate compliance (accountability)

5.2 Staff

5.2.1 All Ruskin Staff are responsible for:

- Ensuring that all the personal data the College holds about them in relation to their employment is accurate and up to date;
- Informing the College of any changes or errors to information which they have provided immediately, e.g. change of address
- Ensuring, where they process personal data in connection with their employment and are permitted to do so under the law, that any personal data processed is kept securely and is not disclosed either orally or in writing to any unauthorised third party;
- Informing the Data Protection Officer if they process personal data for a new purpose, transfer personal data to a new data processor or undertake any significant changes to the management or handling of personal data.
- Ensuring that all data collection forms are up to date and legal under current legislation.
- Do not take any personal data off site and to make sure that all College based communication goes through the College systems (i.e. not personal email)
- To immediately inform the Data Protection Officer if any breach of data has occurred or has possibly occurred.
- To never leave an office (or personal data) unattended and unlocked and to always lock a computer when moving away from the terminal.
- Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party.

5.2.2 Personal information should be: -

- Kept in a locked filing cabinet or draw
- If it is computerised be password protected and on the College system (do not take personal data off site)
- **Under no circumstances should personal data be taken off site**

5.2.3 If there are any significant changes to the way that data is processed, obtained or stored a Privacy Impact Assessment (PIA) must be carried out before implementation. This is a legal requirement under the GDPR.

5.2.4 As part of the PIA staff need to provide full details of the type of personal data to be processed (i.e. financial details, contact details), who the subject of the data is (e.g. students, staff, the public), why the data is being processed (e.g. marketing, staff administration) and whether the intention is at any time to transfer the data to a third party external to the College who is not the subject of the data, including whether this is an international partner and why the College is changing from the current methodology to a new one.

5.3 Students

Students need to make sure that all data supplied to the College is accurate and up to date. If a student (i.e. head of the RSU) is in a position to hold or process personal data then they will need to abide by this policy. All students who handle or process personal data must be aware of the processing principles and how to apply them. Student research may involve data collection/processing, in that case the student would need to follow this policy as well as the ethics approval form and implementing ethics documentation. There are certain exemptions in the act for research purposes; this should be relayed to the students via Ruskin Tutors. If a student is unsure please seek the advice of your tutor/department.

5.4 General

Any other stakeholders, contractors, visitors, etc. who provide personal data to the College or process personal data on behalf of the College (e.g. Council Members, External Examiners,) must also comply with this policy and the law. Any third parties used for any reason regarding personal data should be fully contracted and GDPR compliant, a Privacy Impact assessment must be done for all third parties before deciding on whether to use them.

5.5 Individuals Rights

Under the General Data Protection Regulations the rights of the individual include: -

- **The Right to be Informed** – Individuals have the right to be informed about the collection and use of their personal data
- **The right of Access** - Individuals have the right to access their personal data (i.e. A Subject Access Request)
- **The right of Rectification** - A right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.
- **The right to Erasure -** The GDPR introduces a right for individuals to have personal data erased. (This is not an absolute right)
- **The right to restrict processing -** Individuals have the right to request the restriction or suppression of their personal data. (This is not an absolute right)
- **The 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. (This only applies to information that the individual has given to the College)
- **The right to object -** The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
- **Rights in relation to automated profiling and decision making**

For more information on the individuals rights please see the ICO website, linked here.

If an individual enacts any of these rights the College will do all it can to act quickly and efficiently, however there is certain information that the College legally has to hold, this will be made clear to the individual at the time of data collection. If anyone wishes to enact any of these requests they must contact the Data Protection Officer.

The College would appreciate any individual bringing any issues to the College in the first instance. Most difficulties can be resolved quickly and easily by doing this. However if anyone believe that the College has acted unlawfully in the processing of personal data they can complain directly to the Information Commissioners Office. Their contact details are linked here. This can become very serious and once this has occurred the complaint is out of the controller's hands and the investigation will be taken over by the Information Commissioners Office. This process can be found here. Once this occurs the liability and consequences will be decided by the Information commissioners Office, this could be against either the Controller or an Individual

5.6 Data Co-ordinators

Ruskin College as a body is the Data Controller under the Act, and the Governing Executive is therefore ultimately responsible for implementation. However the College has data co-ordinators and a Data Protection Officer. The Data Co-ordinators hold the overview of their department's use of personal data, dealing with day to day matters. Working with the Data Protection Officer and Data Controller they ensure that the data collection and processing within their departments are within the law and adherent to this policy. The current data co-ordinators are: -

- The Head of Student Services
- The Head of Finance
- The Facilities Co-Ordinator
- The Assistant Principal
- The Human Resources Manager
- The Data, Quality and Performance Manager
- The Business Development Manager

5.7 FOI and Subject Access Requests

Any freedom of Information or Subject access requests that come into the College should be sent to the Data Protection Officer. If any staff member receives these requests they should forward them to the Data Protection Officer immediately given the strict and defined timescale for responding to such requests. The Data Protection Officer will work with relevant staff and senior management were necessary to ensure that responses are answered fully and correctly. A member of the Senior Leadership Team will view these requests before they are sent out to make sure that information is accurate and complete.

5.8 Breaches

In the case of a data breach or suspected breach the Data Protection Officer must be informed immediately. The College has a legal responsibility to report any breaches to the Information Commissioners Office within the ICO defined time scales when a breach occurs. As named contact with the ICO these breaches will be reported by the Data Protection Officer, not an individual member of staff. For information regarding a data breach please see the Colleges data breach policy. It is important to note that any potential data breach will be treated in a similar way to an actual breach by the Information Commissioners Office.

5.9 Privacy Notices

Where personal data is being initially collected or used for a further purpose(s) then data subjects need to be informed through a Privacy (also known as a Fair Processing) Notice, how their personal data will be used by the College.

5.10 Non-Written Personal Data

The General data Protection Regulations also consider non-written information. This includes CCTV (see CCTV Policy), recording of student presentations, photographs of natural persons, recordings of speakers and presentations. Therefore all collection of these data mediums must adhere to this policy.

5.11 Disposing of personal data

All paper based personal details should be disposed of in confidential waste bags which should be kept securely until they are destroyed. For electronic data this needs to be permanently deleted and there be no unnecessary duplication of data. The data co-ordinators will take the lead on all data destruction in adherence to this policy and the law.

6.0 Outcomes

6.1 Grievance

For internal grievances the College will follow its grievance policies as outlined in the defined policies, available on the college website. If anyone has a grievance that is data protection related please contact the Data Protection Officer or Data Co-ordinator in the first instance.

6.2 Complaints

Please refer to the colleges published policy, available on the website.

6.3 Liability – Individual and collective

Everyone (including staff, students, external contractors) has responsibility to abide by this policy and the law under the General Data Protection Regulations. In most instances the Data Controller holds ultimate responsibility under the regulation however individuals could be held personally liable for data protection breaches by the Information Commissioners Office. As stated, internal issues will be dealt with through the grievance and complaints procedures.

7.0 Conclusion

Compliance with the General Data Protection Regulations and related acts is the responsibility of all members of Ruskin College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to Ruskin College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up, in the first instance, with the designated data co-ordinator and referred to the data controller if necessary.

8.0 Appendices

8.1 Staff Guidelines for Data Protection

1. All academic, academic-related and academic support staff will process data about students on a regular basis, when marking registers or Ruskin College work, writing reports or references, as part of a pastoral or academic supervisory role or in supporting any of the above functions. Ruskin College will ensure through registration procedures that all students give their consent (or relevant GDPR principal) to this sort of processing and are notified of the categories of processing, as required by the Act (see section 5.1 and the GDPR map). The information that staff deals with on a day-to-day basis will be standard and will cover categories such as:

- General personal details such as name and address;
- Details about class attendance, course work marks and grades and associated comments;
- Notes of personal supervision, including matters about conduct and discipline.

2. Information about a student's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity is sensitive and can only be collected and processed with the student's consent. If staff need to record this information, they should use a Ruskin College standard form, e.g. when recording information about dietary needs for religious or health reasons prior to taking students on a field trip or recording information that a student is pregnant as part of pastoral duties.

3. All staff have a duty to make sure that they comply with the data protection principles, which are set out in Ruskin College Data Protection Policy. In particular, staff must ensure that records are:

- Accurate;
- Up-to-date;
- Fair;
- Kept and disposed of safely, and in accordance with Ruskin College policy.

4. Ruskin College will designate staff in each area as 'authorised staff'. These members of staff are the only staff authorised to hold or process data that is:

- Not standard data; or
- Sensitive data.

The only exception to this will be:

- If a non-authorised staff member is satisfied that the processing of the data is necessary in the best interests of the student or staff member or a third person, or Ruskin College; and

- He or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.

This should only happen in very limited circumstances, e.g. if a student is injured and unconscious but in need of medical attention, and a tutor tells the hospital that the student is pregnant or a Jehovah's Witness.

5. Authorised staff (i.e. data co-ordinators) will be responsible for ensuring that all data is kept securely.

6. Staff must not disclose data to any student, unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller, or in line with Ruskin College policy.

7. Staff shall not disclose data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with Ruskin College policy.

8. Before processing any personal data, all staff should consider the checklist set out below.

Staff Checklist for Recording Data (see also 8.2/8.3)

- ♦ Do you really need to record the information?
- ♦ Is this information already recorded somewhere i.e. the MIS system?
- ♦ Have you specified the time limits in which you will hold the data to the data subject?
- ♦ Have you explained the data subjects rights to them?
- ♦ Is the information 'standard' or is it 'sensitive'?
- ♦ If it is sensitive, do you have the data subject's express consent?
- ♦ Has the student been told that this type of data will be processed and how it will be processed?
- ♦ Are you authorised to collect/store/process this data?
- ♦ If yes, have you checked with the data subject that the data is accurate?
- ♦ Are you sure that the data is secure?
- ♦ If you do not have the data subject's consent to process, are you satisfied that it is in the best interest of the student or the staff member to collect and retain the data?
- ♦ Have you reported that fact of data collection to the authorised person

8.2 Information that needs to be relayed to the individual on all data collection forms.

All forms of data collection regardless of the GDPR principal that is being used to collect the data must include everything in the below table.

- The College name and contact details
- Details of your representative if necessary
- Contact details of your Data Protection Officer (i.e. dataprotection@ruskin.ac.uk)
- What you will use the data for, including whether it will be used for automated decision making (please note you can only use the data you have collected for the specific purposes told to the natural person at time of data collection.)
- The legal basis for obtaining the information (usually Performance of Contract or Consent)
- What categories of people will receive/have access to the data
- Whether data will be sent or stored abroad and on what basis (and whether third party software's are involved)
- How long the data will be stored
- Whether provision of data is required and the consequences of not doing so
- Their right to withdraw consent
- Their right of access, rectification, erasure, restriction, objection and portability
- Their right to complain to the ICO

8.3 New Consent Rules

The new rules for consent are listed below, these are required for all data collection that relies on consent, whether the data is currently held or whether the data is about to be collected.

Must Be	Must Not
Given by a statement or clear affirmative action.	Be inferred from silence, pre-ticked boxes or inactivity
Freely given, specific, informed and unambiguous	Make consent a condition for receiving a service unnecessarily
Approved by the Data Controller	Use confusing language
Withdraw as easily as it is given	Bundle with other terms and conditions

8.4 Information Security (see also IT policy, Social Media Policy and IT rules and Regulations)

Information Security – Good Practice Guidance What is

information security?

Information can be defined as an important business asset of Ruskin College which, like all other assets, will have a value. The value of personal information, coupled with a dependency on the systems which process the information, means that it must be afforded adequate protection from the wide ranging threats which may affect it and result in unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The General Protection Regulations and this policy covers all personal data whether stored electronically or in paper form.

Information security can be defined as: -

- **Confidentiality** ensuring that information is accessible only to those authorised to have access;
- **Integrity** safeguarding the accuracy and completeness of information and processing methods;
- **Availability** ensuring that authorised users have access to information and associated assets when required

From a data protection perspective data security links to the principle that the controller "ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical of organisational measures" (article 5(f)). Therefore whether data is held electronically or in paper form the data has to be secure from unauthorised access, whether intentionally or by accident. Paper form should always be kept in locked filing cabinets and all electronic data should be kept on the relevant systems for that information (usually the MIS system). Neither should ever be taken off site. Passwords provide a means of validating a user's identity and thus of establishing access rights to information processing facilities or services. Users should follow good security practices in the selection and use of passwords and storage of personal data.

Remember:

- Passwords should be easy for the user to remember, but difficult to guess by anyone else;
- Avoid the use of the following as your password, for example;
  - Family names, pet names, birthdays, car registration number, football or other sporting teams.
  - Under no circumstances should the word 'password' be used as a password.

- Quality passwords include at least 6 characters, using a mixture of upper and lower case, and including the numeric and non-standard character set.
- Keep passwords confidential;
- Do not share your password with any other user.
- Change your password and inform your data co-ordinator immediately if you believe your password has been compromised.
- Always keep all data secure and never take it off site without explicit permission from a data co-ordinator/data protection officer.

Clear Desk/Clear Screen Policy

In order to reduce the exposure to risk arising from unauthorised access, loss of, and damage to personal information during and outside normal working hours, there must be a clear desk policy for papers and removable storage, such as storage discs or USB, and a clear screen policy for information processing facilities where processing of personal, sensitive or confidential information takes place.

Staff must adhere to the following general principles for clear desk and clear screen.

- When leaving a workstation/workspace, staff must ensure that all sensitive and confidential paperwork or other media is removed from the desk to either a lockable drawer or cabinet;
- When leaving a workstation, either during or at the end of the day, the user must ensure that their session is correctly logged out or that a screensaver is configured (i.e. the computer is locked);
- Any sensitive or confidential information sent to print must be removed from the printer immediately and securely destroyed if not required for file evidence;
- The printer tray must be clear at the end of the day and the printer turned off.
- If you leave your office then the office door should always be locked

Responding to Security Incidents

A security incident may be defined as any event which has resulted, or could result, in:

- The disclosure of personal, sensitive or confidential information to any unauthorised individual;
- The integrity of the College's systems or data being put at risk;
- An adverse impact, for example:
  - financial loss;
  - Loss of data
  - errors resulting from incomplete or inaccurate data;
  - disruption of activities and denial of service;
  - information system failure or loss of service;
  - embarrassment to Ruskin College;
  - threat to personal safety;
  - any legal obligation or penalty.

Any suspected security incident must be reported to the data protection officer. The reporting of any incidents will be treated in confidence if necessary but we have a legal obligation to inform the ICO.

Backups

It is important that there are procedures in place to maintain the availability of data and information and the integrity of information being processed in the event of failure.

Core systems will be backed up automatically by IT staff. However, this will not include data and files written to the local drive of the PC, which should be backed up on a daily basis.

Viruses

Viruses and other malicious codes can have a devastating effect on the information and service continuity of the College. It is important that users bear in mind the following points of good practice:

- Ensure that any new piece of software is checked for viruses first before it is loaded on to any local office machine. Always check memory sticks, from whatever source, before use;
- Do not download software or files of an unknown origin from the Internet – talk to IT staff about how you can 'surf' the net without putting the College at risk;
- Inform IT staff immediately if you believe your PC has a virus.

Electronic Transmissions

It is important that staff recognise the risks associated with electronic transmission of data and take the appropriate precautions when sending personal, sensitive or confidential information by electronic methods. It is the responsibility of the College to ensure that the security of personal information processed is afforded adequate protection. Do not use unauthorised third party software including personal email addresses to send or receive personal data.

Staff should consider the following good practice points for electronic transmission:

- Never disclose personal information over the phone, even if the caller appears genuine or claims to be from the police or a government agency;

- Check before you send a fax containing personal or sensitive information. If the intended recipient fails to collect the fax or the number is incorrect, the College may be held responsible for unlawful disclosure;

- Be careful about what you send via email, who you send it to and always use the College provided email. Email and the Internet are worldwide resources, and transmitting information via these means has no guarantee that the routing of your message will not take it outside of the EEA. It is important that staff ensure that email and the Internet are not used inappropriately and confidential or sensitive data inadvertently put at risk of interception outside of the EEA, putting the data at risk or inadvertently allowing a unintended recipient to view the message. Only authorised third party software's can be used by the College which will have had an initial Privacy Impact assessment done on them.