



DATA PROTECTION POLICY

Statement of Intent

This is the Ruskin College statement of intent towards the responsible compliance with the Data Protection Act 1998.

As a Data Controller, Ruskin College needs to collect and process information, including personal information, about the people that it deals with in order to operate effectively and efficiently.

Data subjects may include: Staff, Students, Alumni, Customers and Suppliers. The information processed may relate to present, past and prospective data subjects. In addition we may be required by law to collect and/or process certain types of data to comply with requirements of the Learning and Skills Council, the Higher Education Funding Council for England, government departments and regulatory agencies.

All personal data, however collected, must be processed in accordance with the eight principles of the Act. This applies equally to data recorded in automated systems, manual files and other storage media such as microfiche and CCTV.

To ensure the lawful processing of personal information, anyone processing personal data must comply with the eight enforceable principles of good practice, which state that personal data shall:

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

All staff, students and other users are entitled to:

- ◆ know what information Ruskin College holds and processes about them and why;
- ◆ know how to gain access to it;
- ◆ know how to keep it up to date;
- ◆ know what Ruskin College is doing to comply with its obligations under the 1998 Act.

The College will ensure that management controls are in place to:

- ◆ maintain an accurate and up to date notification of processing purposes;
- ◆ comply with the fair processing code regarding the collection and use of the data collected;
- ◆ maintain the quality and accuracy of data held and processed;
- ◆ review the retention periods for which data is reasonably retained;
- ◆ fully meet the rights of the data subject regarding data held and processed by the organisation;
- ◆ take appropriate technical and organisational measures to protect personal data from unauthorised or unlawful processing and accidental loss, destruction or damage;
- ◆ protect personal data from transfer outside of the EEA or, where such transfer is necessary, provide for adequate security of the information.

To ensure the effective application of the Principles of the Act, the College will ensure that:

- ◆ there is a nominated data co-ordinator within the organisation with the specific responsibility for data protection;
- ◆ all persons processing personal data on behalf of the organisation receive adequate and periodic awareness training to ensure that they understand;
 - ◇ their contractual and legal responsibility towards the personal information processed by the College;
 - ◇ the procedure for responding to a request for data subject access or enquiries about the responsible handling of personal information;
 - ◇ the procedure for responding to a request for personal information held by the College, made by third parties/persons who are not the data subject;
- ◆ adequate management supervision is in place for the processing of personal information;
- ◆ the methods for handling and managing personal information collected and processed by the organisation are periodically reviewed.

Ruskin College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, Ruskin College has developed this Data Protection Policy.

Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by Ruskin College from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal grievance.

Responsibilities of Staff

All staff are responsible for:

- ◆ checking that any information that they provide to Ruskin College in connection with their employment is accurate and up to date;
- ◆ informing Ruskin College of any changes to information which they have provided, i.e. changes of address;
- ◆ checking the information that Ruskin College will send out from time to time, giving details of information kept and processed about staff;
- ◆ informing Ruskin College of any errors or changes to their personal data.

In order to ensure the accuracy of staff data and to compile the annual staff individualised record required by the Learning and Skills Council, Ruskin College will provide all staff with a standard form of notification for completion and return. Ruskin College will do this at least annually.

If and when as part of their responsibilities, staff collect information about other people (e.g. about students' course work, opinions about ability, references to their academic institutions, or details of personal circumstances), they must comply with the guidelines for staff which are at Appendix 1.

Data Security

All staff are responsible for ensuring that:

- ◆ any personal data which they hold is kept securely;
- ◆ personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party;
- ◆ any suspected breaches of security are notified to an appropriate data co-ordinator.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should be:

- ◆ kept in a locked filing cabinet; or
- ◆ in a locked drawer; or
- ◆ if it is computerised, be password protected; or
- ◆ kept only on a disk which is itself kept securely.

Further guidance on information security good practice is provided at Appendix 2.

Student Obligations

Students must ensure that all personal data provided to Ruskin College is accurate and up to date. They must ensure that changes of address and other details are notified to the Academic Registry/other person as appropriate.

Students who use Ruskin College computer facilities may, from time to time, process personal data. If they do, they must notify the data controller. Any student who requires further clarification about this should contact the appropriate facilities supervisor.

Rights to Access Information

Staff, students and other users of Ruskin College have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the college 'Access to information' form and give it to the Finance office (in the case of staff) or Academic Registry (in the case of students), as appropriate.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing using the standard form.

Ruskin College will make a charge to students of £10 on each occasion that access is requested, although the College has discretion to waive this.

Ruskin College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receiving a request unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

Individuals also have certain rights under the Act to require the College to cease processing or using their personal information in certain circumstances. Further information will be provided if required.

Publication of Ruskin College Information

Information that is already in the public domain is exempt from the 1998 Act. It is Ruskin College policy to make as much information public as possible and, in particular, the following information will be available for inspection:

- ◆ Name and contact addresses of members of the Ruskin College Governing Executive
- ◆ List of key staff
- ◆ Annual Report and accounts.

Ruskin College's internal phone list and student room list will not be public documents.

Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the designated data controller.

Subject Consent

In many cases, Ruskin College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, **express consent** must be obtained. Agreement to Ruskin College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This may include information about previous criminal convictions.

Ruskin College has a duty of care to all staff and students and must therefore make sure that employees and those who use the College facilities do not pose a threat or danger to other users. In future, it is anticipated that the new requirements on protecting vulnerable adults will apply to the College, with effect from 2009/10, and that criminal records checks involving the Independent Safeguarding Authority will be required.

Ruskin College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. Ruskin College will only use the information for the protection of the health and safety of the individual, but will need consent to process it in the event of a medical emergency, for example.

Therefore, all prospective staff and students will be asked to sign a Consent to Process form, regarding particular types of information, when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure Ruskin College is a safe place for everyone, or to operate other college policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for Ruskin College to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this without good reason. More information about this is available from the Academic Registry, Central Support Office at the Headington site and from line managers.

The Data Controller and the Designated Data Co-ordinators

Ruskin College as a body corporate is the data controller under the Act, and the Governing Executive is therefore ultimately responsible for implementation. However, the designated data controllers will deal with day-to-day matters.

Ruskin College has 10 designated data co-ordinators. They are the General Secretary, the Dean, the Finance Director, the Academic Registrar, the Warden, the administrators to the four Academic Groups, the Secretary to the Senior Management Team.

Examination Marks

Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. Ruskin College may withhold results, certificates, accreditation or references in the event that fees or other owings have not been paid, or books and equipment have not been returned to the College.

Retention of Data

Ruskin College will keep some forms of information for longer than others. A minimal record will be kept of all past students (whenever the information remains to hand). This will include:

- ◆ name and address (including email address and phone number)
- ◆ academic achievements, including marks for coursework
- ◆ copies of any reference written, and
- ◆ donation record

All other information, including any information about health, race or disciplinary matters, will be destroyed within 6 years of the course ending and the student leaving Ruskin College.

Ruskin College will need to keep information about staff for longer periods of time. In general, all information will be kept for 12 years after a member of staff leaves Ruskin College. Some information, however, will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. A full list of information with retention times is available from the data controller.

Conclusion

Compliance with the 1998 Act 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.

Appendix 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 to this sort of processing and are notified of the categories of processing, as required by the 1998 Act. The information that staff deal 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 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 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

- ◆ Do you really need to record the information?
- ◆ 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?
- ◆ 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?

Appendix 2

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.

Information security can be defined as covering three core principles:

- ◆ **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.

Password Security

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.

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.

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 floppy 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;
- ◆ 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.

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;
 - ◇ 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 a designated data co-ordinator. The reporting of any incidents will be treated in confidence if necessary.

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 to floppy disk, USB or CDR media (if available) by the user and securely stored.

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 floppy disks, 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.

In addition, the eighth principle of the Data Protection Act directs that 'personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of 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 and who you send it to. 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.

Finally

If in doubt contact your designated data co-ordinator.