



# Freedom of Information, Environmental Information and Data Protection Policy, Procedure and Guidelines

Version:	V2
Policy Originator Role:	Chief Operating Officer (COO)
Approved by:	Audit Committee & Corporation
Date Approved:	Corporation 23/07/20
Review Interval:	Every 3 years or as required i.e. if legislation or guidance changes
Last Review Date:	June 2020
Reviewed by:	COO
Uploaded to external website by:	Marketing
Date uploaded:	12/08/2020
Uploaded to Staff Portal by:	
Date uploaded:	
Next Review Date:	June 2020 or as required
Audience:	Staff, Students, General Public

# Contents

1	Statement of Intent	3
2	Introduction and Purpose	3
3	Legal Background or Relevant Legislation	4
4	Related Policies	5
5	Link to Procedure or Guidance	5
6	Responsibilities – Nominated Persons	6
7	Monitoring, Review and Evaluation	7
8	Communication	7
	Appendix 1 - Information Request Procedure	8
	Appendix 2 - Freedom of Information Guidelines and Principles	14
	Appendix 3 - Environmental Information Regulations Guidance	22
	Appendix 4 - Data Protection Procedures & Guidelines	24
	Appendix 5 - Data Retention Plan	30

## 1 Statement of Intent

This policy provides the College statements, procedures and guidelines to ensure compliance with the following Acts and regulations:

- Freedom of Information Act 2000 (FoIA)
- Environmental Information Regulations 2004
- Data Protection Laws - Data Protection Act 2018 (DPA) and General Data Protection Regulation (EU) 2016/679 (GDPR)

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 the College. Any failure to follow the policy can therefore result in formal proceedings.

Any member of staff or stakeholder who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Data Controller initially ([see: Section 6.5 The Data Controller](#)). If the matter is not resolved it should be raised as a formal grievance.

Numerous other pieces of legislation cross refer to discipline issues. Some important examples include information that is already in the public domain and is exempt from the 2018 Act. It is College policy to make as much information public as possible, and in particular the following information will be available for inspection:

- Names of College governors and Register of Interests of Governing Body members and senior staff with significant financial responsibilities (for inspection during office hours only).
- List of key staff.
- Photographs of key staff.
- Information on examination results.

The College's internal phone list is not a public document.

## 2 Introduction and Purpose

This policy has been produced in the interests of all Further Education and Higher Education members of staff and stakeholders, whether they are full time or part time, permanent or temporary, irrespective of their length of service and period of any probationary service.

The policy details the processes, responsibilities and framework by which the College observes and adheres to the Freedom of Information Act (FoIA), Environmental Information Regulations (EIR) and Data Protection Laws.

### 2.1. Freedom of Information Act 2000 (FoIA)

This policy details the procedure ([see Appendix 1 – Information Request Procedure](#)) by which an organisation or member of the public may make a Freedom of Information (Fol) request to the College. Any Fol request will be considered in tandem with the information exemption regulations within the FoIA. In particular, for some cases Fol requests may not be approved if they contravene the DPA. [Appendix 2 - Freedom of Information Guidance and Principles](#) contains guidelines for charging the

requester should the number of hours required to gather and report on the information requested exceed a threshold.

## *2.2. Environmental Information Regulations 2004 (EIR)*

This part of the policy contains the procedure ([See Appendix 1 – Information Request Procedure](#)) by which an organisation or member of the public may obtain environmental information directly linked to the College infrastructure and associated services. A request does not have to specify or describe the information. Any clear sign that someone wants some environmental information is likely to count as a request under the Regulations. However, there are other provisions to help in order to deal with requests which are too broad, unclear or unreasonable.

## *2.3. Data Protection Laws - The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.*

All staff, students and other users are entitled to know:

- What information the College holds and processes about them and why.
- How to gain access to it.
- How to keep it up to date.
- What the College is doing to comply with its obligations under the Data Protection Act 2018.

The College and all staff who process or use any personal information must ensure that they follow the principles below at all times. In order to ensure that this happens, the College has developed Data Protection requirements within this policy.

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.

## **3 Legal Background or Relevant Legislation**

### *3.1 Freedom of Information Act 2000 (FoIA)*

The FoIA requires the following:

- Public authorities, including colleges, are obliged to publish certain information about their activities; and
- Members of the public are entitled to request information from public authorities (subject to certain restrictions which are discussed further in this document).

The FoIA covers any recorded information, including printed documents, computer files, letters, emails, photographs and sound or video recordings, that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland.

The Freedom of Information Act does not give people access to their own personal data (information about themselves), such as their health records or credit reference files. Individuals have a right of access to information held about them under the Data Protection Laws.

### *3.2 Environmental Information Regulations 2004 (EIR)*

The Regulations give people a right of access to information about the activities of public authorities that relate to or affect the environment, unless there is good reason for them not to have the information. This is sometimes referred to as a presumption in favour of disclosure.

The Regulations apply only to the environmental information held by public authorities. The Freedom of Information Act gives people access to most other types of information held by public authorities.

### *3.3 Data Protection Laws*

The College is required to keep certain information about employees, students and other users to allow it to monitor performance, achievements, health and safety, recruitment etc. The College also has legal obligations to submit data to government funding bodies/agencies. To comply with the law, information must be used fairly, stored safely and not be disclosed to any person unlawfully.

It is a requirement of the College that all records are retained for a minimum period, for legal, operational, research and safety reasons. This policy provides staff and stakeholders with procedures to be used when archiving records, and the retention policy to be applied to each class of record. The College archive will be held in a controlled secure environment, managed and maintained by appropriate departments.

## **4 Related Policies**

Other related policies are as follows:

- Whistleblowing Policy
- Safeguarding Policy
- Recruitment and Selection Policy
- Equality, Diversity and Human Rights Policy
- Computer Usage Policy
- Disciplinary Policy and Procedure (Staff)
- Grievance Policy and Procedure

## **5 Link to Procedure or Guidance**

The following appendices provide the procedures and guidelines for this policy:

[Appendix 1 - Information Request Procedure](#)

[Appendix 2 - Freedom of Information Guidance and Principles](#)

[Appendix 3 - Environmental Information Regulations Guidance](#)

[Appendix 4 - Data Protection Procedures and Guidelines](#)

[Appendix 5 - Data Retention Plan](#)

## **6 Responsibilities – Nominated Persons**

### *6.1 Information Requests*

All staff are responsible for relaying information requests they may receive under the Freedom of Information Act, Environmental Information Regulations and Data Protection Act to [foi@wlc.ac.uk](mailto:foi@wlc.ac.uk) or [dataprotection@wlc.ac.uk](mailto:dataprotection@wlc.ac.uk).

See [Appendix 1 - Information Request Procedure](#) for more detail.

### *6.2 Data Protection Laws Compliance*

Compliance with the DPA and the GDPR is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to 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 with the Data Protection Officer ([dataprotection@wlc.ac.uk](mailto:dataprotection@wlc.ac.uk))

Personal information is any information related to an individual. This may be any individual the College has dealings with such as students, staff, governors etc.

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.

*Staff to note that unauthorised disclosure may be a disciplinary matter, and may be considered gross misconduct in some cases.*

### *6.3 Responsibilities of Staff for their personal details*

- To ensure any information that they provide to the College in connection with their employment is accurate and up to date.
- To inform the College of any changes to information, which they have provided i.e. changes of address.
- Checking the information that the College will send out from time to time, giving details of information kept and processed about staff.

- To inform the College of any errors or changes. The College cannot be held responsible for any errors that have not been notified in writing/email/Human Resource Management System (HRMS) to HR.

#### 6.4 *Processing Sensitive Information*

Sometimes it is necessary to process information about a person's health, criminal convictions, race, gender and family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies. This information is considered sensitive, and it is recognised that the processing of it externally may cause particular concern or distress to individuals; staff and students will be asked to give express consent for the College to do this, although in cases where it is a legal requirement for the College to provide such information, it will do so. Offers of employment or course places may be withdrawn if an individual refuses to consent to internal information processing, without good reason. More information about this is available from the Data Controller.

#### 6.5 *The Data Controller*

The Data Controller is any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data. The College is the Data Controller under the Data Protection Act. A Data Controller is responsible for compliance with Data Protection Laws. (A common misconception is that individuals within organisations are the Controllers. This is not the case it is the organisation itself which is the Data Controller.) However, there is a designated Data Protection Officer that must be the first point of contact for all enquiries: [dataprotection@wlc.ac.uk](mailto:dataprotection@wlc.ac.uk), Data Protection Officer.

### **7 Monitoring, Review and Evaluation**

The College will review the policy to take account of any new Government legislation, regulations or best practice documents, to ensure that staff are kept fully up to date with their responsibilities and duties with regard to this policy and procedures.

It is also recommended that the incidents are monitored by the seven strands of equality (i.e. gender, disability, race and ethnicity, age, LGBT - lesbian, gay, bisexual, transgender, religion and socio-economic) over a period of twelve months to identify any trends that need to be addressed.

### **8 Communication**

This policy is published on the College Staff intranet and made available to staff on request in a number of formats as required.

## **Appendix 1 - Information Request Procedure**

### Background

The College will approach requests for information in a positive manner with a view to disclosing the requested information. However, information does not have to be released in some situations, for example where release would contravene Data Protection law, endanger anyone's health and safety, breach confidentiality, or compromise commercial interests.

### **1 Aims**

To deal with all enquiries in relation to the Freedom of Information Act, Environmental Information Regulations or the Data Protection Laws in a fair and consistent manner and in accordance with the requirements of the law.

### **2 Reasons for the Procedure**

To provide a first class level of customer service and comply with the requirements of the Freedom of Information Act 2000, Environmental Information Regulations 2014 and the Data Protection Laws - Data Protection Act 2018 and The General Data Protection Regulation (EU).

### **3 Objectives**

To describe the formal procedure for dealing fairly and consistently with information requests.

### **4 Response Time**

The response time for requests are as follows:

- *Freedom of Information*: 20 working days commencing the working day following the receipt of the written request.
- *Environmental Information Regulations*: 20 working days commencing the first working day following the receipt of the request.
- *Data Protection Request*: One calendar month commencing the same day as the receipt of the request.

The information should be provided unless exemptions apply (see [Appendix 2, Section 5](#)). Working days exclude weekends and bank holidays, but include Principal's days.

### **5 Information Requests**

Requests for information do not need to mention the FoIA, the EIR or DPA/GDPR but must:

- Give the applicant's name and return address; and

Freedom of Information & Data Protection Policy V2

June 2020



- Describe the information being sought.
- Be in writing, including email and fax, if making an FOI request.

The College may also send the applicant the College's Information Request Form. The College will charge for the provision of such information in all cases where it is legally entitled to do so.

There is no legal requirement for the applicant to provide reasons for why they require the information and how the information will be used. The applicant does not need to demonstrate that they have a good reason or a legitimate interest for seeking the information.

The College may also find they receive requests via the website 'whatdotheyknow.com' which helps applicants find out inside information about UK Government and UK public bodies.

Where it is reasonable to do so, the College may ask the applicant for further details of the request to enable them to identify and locate the information requested, e.g.

- Where the request is not in English;
- Where the request is not sufficiently precise for the College to be clear what information is sought; or
- Where a more focused request would assist the College in reducing the cost of compliance below the appropriate limit.

## 6 Procedure

### *Step 1 - Receiving Requests (Responsibility: All staff)*

Information routinely provided to staff, students and the public should continue to be treated in accordance with normal procedures (this should not cover any information listed in the exempt categories in [Appendix 2](#) or [Appendix 3](#)). Any concerns about the information requested should be raised with the appropriate Line Manager in the first instance.

Requests for information should be made in a recorded format, e.g. email, letter, fax. The request must also provide the applicant's name and return address and describe the information being sought. Ideally, information requests should be submitted using the College's 'Information Request Form'.

### *Step 2 - Forwarding requests (Responsibility: All staff)*

Staff must not respond to Freedom of Information, Environmental Information or Data Protection information requests themselves. Requests for information that fall within these categories should be passed immediately to the Data Protection Officer ([dataprotection@wlc.ac.uk](mailto:dataprotection@wlc.ac.uk) or [foi@wlc.ac.uk](mailto:foi@wlc.ac.uk)). The date the information request was received must be included in the notification. Staff must not respond to employment reference requests for staff/ex staff. All requests must be passed to Human Resources.

### *Step 3 - Logging Requests (Responsibility: Data Protection Officer)*

On receipt of a request for information, the Data Protection Officer will log the date the request was received in the College, in order to comply with the specified response requirement. The Data Protection Officer will acknowledge requests and maintain a register to monitor responses to ensure timescales are adhered to.

If the provision of the information is subject to a fee, the applicant will be advised accordingly and payment must be received prior to the information being provided. Under the FoIA, the College is not required to comply with a request for information if the College estimates that the cost of complying would exceed the 'appropriate limit'. For the College, the current 'appropriate limit' is £450.

#### *Step 4 - Categorisation of Requests (Responsibility: Data Protection Officer)*

From the information request submitted by the requester, the category first needs to be established before it can be processed further. The categories are as follows:

- Freedom of Information request (information about the College).
- Environmental Information request (information about the College environment and controls).
- Data Protection request (personal information).

#### *Step 5 - Personal Identification (Responsibility: Data Protection Officer)*

If the information request falls within the Data Protection category, the requester must provide some form of personal identification. This may take one of the following forms:

- Staff member: College ID badge or email from individual College account.
- Student Member: College ID badge or email from individual College account.
- Member of the public: Photocopy of Driving Licence or Passport.

Details of the form of personal identification must be kept on file together with the information request.

#### *Step 6 - Initial Acknowledgement (Responsibility: Data Protection Officer)*

An initial response via email or letter should be sent to the information requester, stating that the information request has been received and is being processed.

At this stage it may be necessary to ask for further details from the requester in order to clarify the information required. In these instances, the specified time period for a request response will start on receipt of these further details, thus enabling the College to respond to the information requested.

Some requests may be for information included in the College Publication Scheme (see the [College Website](#)).

The initial response will be sent within **five** working days of the initial request.

#### *Step 7 - Issue of Response Pack to Request Processor (Responsibility: Data Protection Officer)*

The Data Protection Officer will send a copy of the request to the '**Request Processor**' (the member of staff nominated to process the request), clearly identifying timescales for reply. If any further information is required from the applicant, the Request Processor must advise the Data Protection Officer without delay.

The Request Processor selected will depend on the category of information request as follows:

- Freedom of Information request – Data Protection Officer.
- Environmental Information request – Director Infrastructure Services
- Data Protection request of staff (past and present) – HR Department.
- Data Protection request of students (past and present) – Director of MIS.
- Other Data Protection requests from the public – Data Protection Officer.

#### *Step 8 - Processing of Request (Responsibility: Request Processor) Exemptions*

For Fol or EIR requests the Request Processor must first establish whether or not any exemptions apply. The Request Processor should refer to [Appendix 2: Sections 5 – 8](#) or [Appendix 3: Section 3](#). Alternatively, the Request Processor should consult the ICO website (<https://ico.org.uk>) where guidance for Fol and EIR is published.

#### *Charges*

For Fol or EIR requests the Request Processor must ascertain the cost of processing a request. The guidelines for Fee Charges can be found under [Appendix 2: Section 4](#) and [Appendix 3: Section 5](#).

Under the FoIA, the College is not required to comply with a request for information if the College estimates that the cost of complying would exceed the 'appropriate limit'. For the College, the current 'appropriate limit' is £450.

Applicants must be notified of any costs as soon as possible and prior to the information being provided.

#### *Finding the Information Requested*

The Request Processor must obtain the information requested (if available) and complete the Information Request Tracking form. Following this the form should be returned to the Data Protection Team ([dataprotection@wlc.ac.uk](mailto:dataprotection@wlc.ac.uk) or [foi@wlc.ac.uk](mailto:foi@wlc.ac.uk)). This must be done within the specified time limit.

#### *Step 9 - Information Request Response (Responsibility: Data Protection Officer)*

The Data Protection Team must send a covering letter and:

- Provide the information requested, or
- Explain the reason why we have not been able to provide the information requested.

If a request for information falls within the list of absolute exemptions (see [Appendix 2: Section 6](#)), the applicant should be informed in writing that the College is unable to release the information because an absolute exemption applies. It is not necessary to state whether the College does or does not hold the information.

A Public Interest Test will be conducted to determine whether the public interest is better served by withholding or releasing the exempt information. If the arguments in favour and against disclosure are equal, the College has a duty to disclose. If it is decided to withhold information because a qualified exemption applies, the College will:

- State whether it holds any information of the type requested. Explain why the exempt information has been withheld.
- Inform the applicant of their right to complain to the Information Commissioner at the following address:

Information Commissioner  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

The FoIA allows the College to refuse to comply with a request for information that is vexatious or repeated.

## **7 If the Information Requester Complains**

If an Information Requester complains, they should be referred to the College's Complaints Procedure.

In response to complaints the College should ensure the following:

Complaints should be acknowledged promptly and the complainant should be given the:

- College's target date for determining the complaint;
- The review should be undertaken by someone more senior than the person who took the original decision;
- The review should involve a full re-evaluation of the case;
- Where the outcome of the review is that the information originally requested should now be disclosed, this should happen as soon as practicable and the applicant should be informed when this will be.

## **8 Monitoring & Recording**

The Data Protection Officer will monitor the progress of the Information Requests at all times. All communications and records pertaining to the Information Request must be kept on file.

The Data Protection Officer will provide an analysis of the number and nature of the requests and their outcome to Senior Management. Auditors may ask to see the log and the log will be provided to the Audit Committee on an annual basis.

The Data Protection Officer is responsible for keeping a record of requests. The retention times for this information can be found in [Appendix 5 – Data Retention Plan](#).

## Appendix 2 - Freedom of Information Guidelines and Principles

### 1 General Compliance Principles

The College must comply with a request promptly and in any event will have 20 working days to respond. The 20 working day period starts on the working day after the day on which the College receives the request (for example, if the College receives a request on a Friday, time starts running on the following Monday). Working days exclude weekends and bank holidays but include days when the College is closed but which are neither weekends nor bank holidays.

Where the College reasonably asks for further details to enable it to comply with the request, the 20 working day period does not start running until those details have been received. The College must not delay in requesting further details simply to give more time to respond to the applicant's request.

If the College requires the applicant to pay a fee (see [section 4](#)), the 20 working day period stops on the working day before the day on which the College sends a fee notice to the applicant and re-starts the working day after the College receives the fee.

If one of the qualified exemptions applies to the information requested and the College has to apply the public interest test (see [section 8](#)), it may extend the 20 working day period for a reasonable time in order to consider the public interest test. The College must notify the applicant of the estimated date for response.

Under the FoIA there is a duty to advise and assist those making a request. This means that the College should try and be as helpful as possible when responding to a request. For example, if someone makes a request in the wrong way it would be expected that the College gives the individual information on how to make an appropriate request rather than ignoring the request because of the error.

The College is under a statutory duty to provide advice and assistance to applicants. The College should, amongst other things:

- Publish its procedures for dealing with freedom of information requests, including an address and telephone number for information and assistance;
- Ensure that appropriate assistance is given to enable an applicant to make a request in writing where the applicant is unable or has difficulty to do so;
- Provide assistance to the applicant to enable them to describe more clearly the information requested;
- Consider whether any suitable information is available free of charge if the applicant is not prepared to pay the requested fee; and
- Where the cost of complying with the request would exceed the appropriate limit, consider what, if any, information could be provided within the cost ceiling.

### 2 Refusing to Deal with a Request

The FoIA allows the College to refuse to comply with a request for information that contravenes the Data Protection Laws or is vexatious or repeated.

DPA/GDPR Infringement - The exemption clauses within the DPA and GDPR state that FOIA requests for personal data referring to an individual or individuals should be refused. This includes situations where individual personal information can be derived from the information requested. FOIA requests of this nature should be referred to the College Data Protection Officer in the first instance before formal notification of refusal.

A request is vexatious if a reasonable person would conclude that the effect of the request would be disproportionate or cause inconvenience or expense to the College and that the request:

- Clearly does not have any serious purpose or value; Is designed to cause disruption or annoyance;
- Has the effect of harassing the College; or
- Can otherwise fairly be characterised as obsessive or manifestly unreasonable.

Colleges must consider the nature of the request, not the nature of the requester (applicant). Factors which may suggest that requests are vexatious include:

- The declared intention of the applicant or College's knowledge of the applicant's intentions (e.g. where the College knows that there is an orchestrated campaign to cause the College inconvenience);
- The request clearly has no serious purpose or value (this will often arise where there has been a series of requests);
- The effect of legitimate editing of the information (e.g. the deletion of confidential materials) would render the information worthless; or
- The information requested is clearly exempt.

Requests from the same applicant that are identical or substantially similar may be deemed repeated requests.

In some cases, identical or substantially similar requests may not be repeated, e.g.

- A reasonable interval has elapsed between them;
- The applicant is different;
- The information to be disclosed has changed in the intervening period.

It is possible that many different individuals will make identical or substantially similar requests. If the College is, or becomes, aware that individuals are acting as part of a group seeking to make vexatious or repeated requests, the College is entitled to refuse the requests.

If the College considers that a request is vexatious or is a repeated request, they must notify the applicant and inform them of why the College considers the request to be vexatious or repeated.

The College must also make the applicant aware of the College's Complaints Procedure (see [Section 9](#)).

### **3 Holding Information**

The College only needs to deal with requests where it holds the information or has it available to it. This section sets out the basic concepts as to what information is regarded as being held by a public

authority for the purposes of the FoIA. It is not a simple case that everything the College has is subject to the FoIA.

The FoIA applies to information which the College possesses. This captures:

- Information which the College holds;
- Information which belongs to the College, but has been passed to another public authority, and
- Information which belongs to the College but is held by another party on the College's behalf (e.g. information held by College solicitors or accountants).

The College may hold information on behalf of somebody else. This information may not be covered by the FoIA. A distinction is drawn between the origin of information and whether it is held on behalf of another. Where the College effectively controls the information and holds it in its own right, for its own purposes, the information is unlikely to be held on behalf of another.

Different considerations apply depending on whether the information is held on behalf of another public authority or a private body.

Where an applicant asks the College for such information, the College is not obliged to provide it because it is the other public authority that holds the information under the FoIA. However, the College is under a duty to advise and assist the applicant.

There are various options in dealing with this situation:

- Ask the applicant to redirect the request to the originating public authority; or Transfer the request to the other public authority; or
- Deal with the request but consult with the other public authority as it is their responsibility to make the disclosure decision.

The College may hold some information on behalf of private individuals or companies in the private sector. This information is not covered by the FoIA. However, in most cases, private sector information held by the College will be for the College's own purposes and therefore it will be covered by the FoIA.

There may be cases where it is unclear whether private information would be subject to the FoIA. A good example is tender documentation used for the procurement of services. The documentation provided by the competing companies belongs to the individual companies; however, this information has been produced for a College purpose of determining who should carry out the work.

Even in cases where the College does not hold information for the purpose of the FoIA, it will still need to reply to the applicant. While the College will not be under any duty to provide the information, it is still required to provide advice and assistance.

#### **4 Fees and Charges**

Under the FoIA the College is not required to comply with a request for information if it is estimated that the cost of complying would exceed the appropriate limit. For Colleges (and all public authorities other than central Government departments), the current appropriate limit is £450 as laid out in [The Freedom of Information and Data Protection \(Appropriate Limit and Fees\) Regulations](#).



The appropriate limit has to be applied separately to each request; the duty to confirm or deny and the duty to disclose information pursuant to a request.

Further information is available in the ICO guidance document '[Fees that may be charged when the cost of compliance does not exceed the appropriate limit](#)'.

In estimating whether the cost of complying with a request for information is likely to exceed £450, the College can only take account of the costs it reasonably expects to incur in:

- Determining whether it holds the information requested;
- Locating the information;
- Retrieving the information; and
- Extracting the information from a document containing it or from archives.

The College must use a figure of £25 per person per hour in estimating the cost of the labour involved in any of these four activities, regardless of the actual cost. The labour can be either the

College's own staff or independent contractors engaged by the College to assist with handling the requests for information.

The College should consider whether it will take longer than 18 hours to carry out the above activities.

For these purposes, the College cannot consider the costs (including labour costs) of:

- Giving general advice and assistance to the applicant;
- Considering whether further details are required from the applicant;
- Considering whether the request is vexatious or repeated;
- Calculating any fees to be charged;
- Consulting with third parties; or
- Considering whether any exemptions apply, including any legal costs incurred in deciding whether any exemptions apply.

Where the estimated cost of complying with a request is less than £450, the College can charge for costs that it reasonably expects to incur in informing the applicant whether the College holds the information and communicating the information to the applicant, including post, copying and if necessary, converting the information into the format requested by the applicant. The College cannot charge for the labour involved.

Costs have to be reasonable. For example, photocopying is expected to cost no more than 10p per sheet.

Where the cost of complying is very low (less than £10), Colleges are encouraged to waive the fee altogether.

Further information is available in the ICO guidance document 'Fees that may be charged when the cost of compliance does not exceed the appropriate limit', linked above.

The College is not required to comply with a request for information where the estimated cost of doing so would exceed £450. However, the College still has a duty to confirm or deny whether it holds the information, unless the cost of even doing this would exceed £450.

Colleges will be under a continuing duty to provide the applicant with advice and assistance. Therefore, the College should consider whether:

- It is prepared to comply with the request, even though the estimated cost would exceed £450; or
- There is other information that the College could provide at a lower cost or free of charge; or Whether the information is available elsewhere.

If the College does not wish to comply with a request where the cost of complying would exceed £450, it must notify the applicant that the estimated cost of complying with the request is above £450 and make the applicant aware of the College's Complaints Procedure.

Further information is available in the ICO guidance document 'Fees that may be charged when the cost of compliance exceeds the appropriate limit', linked above.

In calculating the fee, the College must disregard the costs of considering whether any exemptions apply and cannot charge one applicant for the total cost of complying with aggregated requests received from a number of applicants.

The College can aggregate the estimated costs of complying with a request for information, for the purposes of assessing whether the £450 limit is exceeded, where the College receives two or more requests for information which:

- Are from the same person or from different persons who appear to Colleges to be acting in concert or in pursuance of a campaign; and
- Relate to the same or similar information; and
- Have been received by the College within a space of 60 consecutive working days.

As a matter of good practice, the College should exercise extreme caution when deciding whether requests should be aggregated. The College should only aggregate the core requests where there are strong grounds for believing that they have been framed precisely in order to circumvent the £450 limit.

The College should note the following quirk when charging fees:

- If the information requested is held by a public authority, the fees charged would not be subject to VAT.
- If the information requested is available from another source that is not a public authority, the fees charged would be subject to VAT.
- Fees charged for information that is provided in accordance with a public authority's publication scheme will attract VAT.

## **5 Exemptions**

The exemptions are split into two categories – absolute exemptions and qualified exemptions. The College has two duties:

- To confirm or deny whether it holds the information; and
- To provide the information.

The exemptions must be used separately in relation to each duty. The exemptions are worded by reference to whether the requested information may not be disclosed. Care must be taken to assess whether the duty to confirm or deny arises.

A list of exemptions can be found at <http://www.legislation.gov.uk/ukpga/2000/36/contents>.

The refusal notices must also be accompanied by information making the applicant aware of the College's Complaints Procedure.

## **6 Absolute Exemptions**

Where the College is seeking to rely on an absolute exemption, it is also generally the case that the duty to confirm or deny will also be exempt. However, this does not always have the same effect for all the absolute exemptions. This is highlighted for each exemption in the following pages. The duty to confirm or deny must always be considered separately.

Set out below are the absolute exemptions which are likely to be applicable to Colleges. Colleges considering applying other absolute exemption(s) should seek legal advice.

- Information accessible to the applicant by other means - Section 21 of the FoIA Court Records - Section 32 of the FoIA
- Personal Information - Section 40 of the FoIA
- Information provided in confidence - Section 41 of the FoIA Prohibitions on disclosure - Section 44 of the FoIA

## **7 Qualified Exemptions**

The exemptions are split into two categories – absolute exemptions and qualified exemptions. This section looks at qualified exemptions and how these operate.

A qualified exemption means that there are two tests to be applied:

- Whether the exemption applies;
- Whether the public interest test in disclosing the information outweighs the public interest in not disclosing (the public interest test).

The term public interest is not defined in the FoIA. However, it is clear that something that is in the public interest is something which serves the interest of the public not something which is merely of interest to the public. In applying this test, the College should decide whether in any particular case it serves the interests of the public better to withhold or to disclose information.

The FoIA requires Colleges to disclose information unless there is a good reason not to. The exemption can only be maintained (upheld) if the public interest in doing so outweighs the public interest in disclosure.

There is a general presumption that it is in the public interest to disclose information but this must be balanced against the need to facilitate effective government and public administration. Therefore, there may be particular public interest considerations in favour of refusing the request. In effect, the qualified exemptions provide the public interest considerations for withholding information.

In applying the public interest test, the College will have to balance two competing public interests: the public interest in disclosing the information and the public interest in maintaining the relevant exemption and withholding the information.

When making its determination, the College **should not** give weight to:

- The private interest of Colleges in withholding information because the information would reveal incompetence or cause embarrassment; or
- The fact that the information is complicated or incomplete. In these circumstances, Colleges may explain or give the context for the requested information.

Factors favouring disclosure	Factors against disclosure
<p>Disclosure would:</p> <ul style="list-style-type: none"> <li>• Further understanding and debate of current issues especially issues in the media.</li> <li>• Promote accountability and transparency in the spending of public money.</li> <li>• Promote understanding of decisions taken by Colleges and how to challenge them.</li> </ul>	<p>The factors are set out in the exemptions. For example, it is in the public interest to protect:</p> <ul style="list-style-type: none"> <li>• Law enforcement.</li> <li>• Investigations and proceedings.</li> <li>• Legal professional privilege.</li> </ul> <p>In some cases, disclosing information will hinder effective government where:</p> <ul style="list-style-type: none"> <li>• Information is disclosed prior to its proposed publication date.</li> <li>• Information is disclosed which will inhibit proper discussion.</li> </ul> <p>In other cases, disclosure will make it difficult to ensure that effective government occurs if:</p> <ul style="list-style-type: none"> <li>• Commercially sensitive information is released.</li> <li>• Trade secrets are revealed.</li> </ul>

The College must make sure that it makes it clear in the refusal notice that it has applied the public interest test in respect of each duty.

## 8 Main Qualified Exemptions for Colleges

Set out in the following section are details of the main exemptions which are likely to be useful for Colleges:

- Information intended for future publication - Section 22 of FoIA
- Prejudice to effective conduct of public affairs - Section 36 of FoIA Legal professional privilege - Section 42 of FoIA
- Commercial Interests - Section 43 of FoIA

Information intended for future publication - This exemption allows public authorities to refuse a request where the information is intended for future publication. The decision to publish must have been taken before the request is received, although a definite date for the future publication need not have been set. The exemption is subject to the public interest test and so the College must decide whether it is in the public interest to disclose the information early.

Prejudice to effective conduct of public affairs – This exemption allows the designated person to determine in his reasonable opinion whether disclosure of the information would have one or more of the following effects:

- Would or would be likely to inhibit the free and frank provision of advice; or
- Would or would be likely to inhibit free and frank exchange of views for the purpose of deliberation; or
- Would otherwise prejudice or be likely otherwise to prejudice, the effective conduct of public affairs.

In exercising their reasonable opinion, the Principal must be objective and make their decision based on evidence. Their opinion must be within the range of reasonable opinions and should not be based on irrelevant material or without consideration of all the relevant facts.

If the Principal believes that disclosure of the information would prejudice the aspects outlined above, then the public interest test must also be applied.

## **9 Complaints Procedure**

The College is required to have a procedure for dealing with complaints both in respect of its handling of requests for information and in respect of its publication scheme. The complaints procedure should allow for a fair and thorough review of the way in which colleges handle requests for information and of decisions taken by colleges pursuant to the FOIA, including decisions relating to the application of exemptions and the public interest test.

In response to complaints the College should ensure the following:

- Complaints should be acknowledged promptly and the complainant should be given the College's target date for determining the complaint;
- The review should be undertaken by someone more senior than the person who took the original decision;
- The review should involve a full re-evaluation of the case;
- Where the outcome of the review is that the information originally requested should now be disclosed, this should happen as soon as practicable and the applicant should be informed when this will be.

Wherever the College serves a refusal notice on an applicant, it must also make the applicant aware of the College's Complaints Procedure.

## **Appendix 3 - Environmental Information Regulations Guidance**

### **1 Main Principles**

The Regulations give people a right of access to information about the activities of the College that relate to or affect the environment, unless there is good reason for them not to have the information.

This means that everyone has a right to access environmental information. Disclosure of information should be the default – in other words, information should be kept private only when there is a good reason and the Regulations allow it.

An applicant (requester) does not need to give a reason for wanting the information. All requests for information must be treated equally.

The Environmental Information Regulations do not prevent you voluntarily giving information to people outside the provisions of the Regulations.

### **2 Information Covered**

The Regulations cover any recorded information the College holds that falls within the definition of 'environmental information'. It is not limited to official documents or information created by the College. It can cover, for example, drafts, emails, notes, recordings of telephone conversations and CCTV recordings.

Unlike the Freedom of Information Act, the Regulations do not explicitly exclude information that you hold solely on behalf of another person or body. The Regulations say that any information that is in your possession that you have produced or received is considered to be 'held'.

The College only has to respond to an Environmental Information request if it already has the information in recorded form. The College does not have to create new information or find out the answer to a question.

The Environmental Information Regulations do not provide a right of access to a person's own information. If someone makes a request for their own personal information, this should be dealt with under the Data Protection Act.

### **3 Exemptions and Request Refusals**

A request for information can be refused if:

- The information is not held.
- The request is manifestly unreasonable such as vexatious requests.
- The request is too general (after fulfilling the duty to advise and assist).
- The request is for unfinished documents or data (in which case an estimated time for completion should be given).
- It is not in the public interest to release the requested information (following a Public Interest test).

Information may also be withheld to protect the following:

- Confidentiality of proceedings.
- International relations / public security / defence. The course of justice and fair trial.
- Commercial confidentiality. Intellectual property rights. Personal Information.
- Data supplied voluntarily. Environmental protection.

#### **4 Publication Scheme**

One of the College's obligations under the Environmental Information Regulations is to publish environmental information proactively. The Regulations require you to do this in the following two ways:

- The College should publish information by easily accessible electronic means.
- The College should organise its records in such a way that it can publish certain information routinely.

These obligations are separate from the College's duty to make information available in response to individual requests.

The College does not have to publish all the environmental information it holds. The minimum the College should routinely publish to comply with its obligations under the Regulations is listed in Article 7(2) of the European Directive 2003/4/EC. It includes things like policies, plans and procedures relating to the environment, reports on the state of the environment, and environmental impact studies. It also includes data taken from monitoring activities and risk assessments that affect or are likely to affect the environment.

#### **5 Charges and Fees**

There are two broad types of costs for which a public authority can charge:

- The cost of staff time spent locating, retrieving and extracting the information.
- The costs incurred when printing or copying the requested information and sending it to the requester.

For staff time, the standard rate per hour is set at £25. This is in line with current ICO recommendations.

## **Appendix 4 - Data Protection Procedures & Guidelines**

### **1 Updating and Processing of Data**

#### **1.1 Regular Updating**

The College will update staff data at least annually. Students' data is updated annually through the enrolment process.

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 other academic institutions, or details of personal circumstances), they must comply with the retention schedule.

#### **1.2 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 the 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 the 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 Data Controller.

### **2 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.

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
- In a locked room, or if it is electronic (computerised), be password protected and also encrypted if saved to a portable device.

### **3 External Data Sharing**

Where personal data is being shared with an external organisation the following must be adhered to:



- A Data Sharing Agreement must be in place between the College and the external organisation, and the type of data being shared must be on the External Data Sharing Register.
- Where there is no established record on the External Data Sharing Register, the Data Protection Officer should be contacted with a request for the data to be shared. The Data Protection Officer will then determine whether or not the request is to be approved. If the request is approved, a Data Sharing Agreement must be completed and the External Data Sharing register must be updated before the data can be shared.
- Electronic data must always be encrypted and password protected before being shared. Paper based personal records must be sent via recorded delivery or via courier.

## Student Obligations

Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of address, etc. are notified to the Student Support department or other person as appropriate.

## 4 Rights to Access Information

### 4.1 Information Access in Order to Fulfil Job Role

Staff will only be given access to student and/or staff information held by the College if they require this information in order to fulfil their job role. For specific cases, members of the Senior Leadership Team may request that special access be granted to a member of staff. This request should be made to the Data Protection Officer who will ultimately approve or reject the request.

The IT department is responsible for administering access to electronic file areas. Access to core applications such as Finance, are the responsibility of the department administrators given control of the application concerned.

### 4.2 Information Access in order for Individuals to View Data Kept about Them

Staff, students and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files. Ideally, any person who wishes to exercise this right should complete the College's Information Request form.

The completed form should then be sent via email to [dataprotection@wlc.ac.uk](mailto:dataprotection@wlc.ac.uk) or sent to the following address:

Data Protection Officer  
 Ealing, Hammersmith & West London College  
 Gliddon Road  
 London  
 W14 9BL

The College will make no charge for the first occasion that access is requested, but may make a charge of £10 per each subsequent request at its discretion.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 20 working days 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.

## **5 Processing of Personal Data**

In many cases, the 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 the 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 includes information about previous criminal convictions.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The College has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the courses offered. The College also 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.

The 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. The College will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

## **6 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. The College may withhold accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned to the College.

## **7 Retention of Data**

The College will keep some forms of information for longer than others. Because of data retention legislation, information about students will not be kept indefinitely, unless there are specific requests to do so. A list is attached of the archiving guidelines and retention time spans employed by the College (see [Appendix 5 – Data Retention Plan](#)).

## **8 Disposal of Data**

When personal data is no longer required, or has passed its retention date, paper records must be shredded. If there is a significant amount of material which cannot be dealt with by normal shredding

machines, the [Estates helpdesk](#) should be contacted for a secure shredding bag which can be topped up and shredded by the College's agreed third party.

Computerised records must be permanently deleted, with particular care taken that 'hidden' data cannot be recovered. Where old or broken computer equipment is being sent for scrap, all associated media devices must be cleaned of all data using the permanent deletion method as agreed by the IT department.

## 9 Archiving

Where staff have identified records that require archiving these must be boxed, tagged and recorded using the following process:

- Records must be boxed in the designated archive boxes. For clarification contact the Estates department.
- Boxes should not be over-packed.
- A list of the box contents should be retained by the department. An Archiving Record Book / Database must be kept in each department, and contain the following information:
  - Box Number (bar code sticker provided by the Estates department).
  - Box Description.
  - Name of College / Department.
  - Archive Date.
  - Destruction Date.
  - List of Contents (created during packing stage).
- A duplicate list of contents must be secured to the inside of the lid of the box once packed. When the boxes are ready to be sent to archive, a request for collection should be raised on the [Estates Helpdesk](#).

Following this process will ensure the College / Department know what records have been archived, for retrieval and audit purposes. All staff must be aware of the book / database and where it is stored. Electronic databases should be stored on network drives for backup and recovery purposes.

To request the retrieval of records from the archive staff should log a request on the [Estates Helpdesk](#) with:

- Name of College / Department (as recorded on box)
- Box Number
- Delivery address

Boxes will be delivered by the Estates department.

Each year the Estates Department will check the archive in the August holiday period. Any boxes with the destruction date within the previous year will be disposed of. An inventory of those boxes sent for destruction will be taken and sent to the relevant Programme Area/Department to allow the withdrawal of these items from locally held records.

## 10 Responsibilities – Nominated Persons

Compliance with the Data Protection Laws is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to 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 with the Data Protection Officer.

### *10.1 Responsibilities of Staff*

- To check that any information that they provide to the College in connection with their employment is accurate and up to date.
- To inform the College of any changes to information, which they have provided i.e. changes of address.
- To check the information that the College will send out from time to time, giving details of information kept and processed about staff.
- To inform the College of any errors or changes. The College cannot be held responsible for any errors that have not been notified.

### *10.2 The Data Controller*

The College as a corporate body is the Data Controller under the DPA, and the Senior Leadership Team is therefore ultimately responsible for implementation. However, there is a designated Data Protection Officer ([dataprotection@wlc.ac.uk](mailto:dataprotection@wlc.ac.uk)) that deals with data protection issues and requests.

## **11 Authorised staff**

The College will designate staff as 'authorised staff'. These 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 the 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. Example: a student is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the student is pregnant or a Jehovah's Witness.

Authorised staff will be responsible for ensuring that all data is kept securely.

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

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

## **12 Staff Checklist for Recording Data**

Before processing any personal data, all staff should consider the checklist:

- 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 or the staff member been told that this type of data will be processed? Are you authorised to collect/store/process the 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 it is in the best interests of the student or the staff member to collect and retain the data?
- Have you reported the fact of data collection to the authorised person?

## Appendix 5 - Data Retention Plan

Responsibility	Class No.	Description	Retention Period
Finance	Financial and Management Accounting	Records documenting the payment and/or reimbursement of employees' expenses.	Current financial year + 6 years
Finance	Financial and Management Accounting	Records documenting the payment of expenses to third parties (e.g. honorary appointees).	Current financial year + 6 years
Finance	Financial and Management Accounting	Records documenting the handling of petty cash.	Current financial year + 6 years
Finance	Financial and Management Accounting	Records documenting the receipt and processing of students' fees.	Current financial year + 6 years
Finance	Payroll and Pensions	Records documenting employees' authorisation for non-statutory payroll deductions.	Current financial year + 6 years
Human Resources	Payroll and Pensions	Records documenting calculation and payment of payroll payments to employees.	Current tax year + 3 years
Human Resources	Payroll and Pensions	Records documenting the operation of the Statutory Sick Pay scheme.	Current tax year + 3 years
Finance	Payroll and Pensions	Records documenting payments of the institution's employers' contributions to pension schemes for its employees.	Termination of employment + 75 years
Finance	Payroll and Pensions	Records documenting payments of the institution's employees' contributions to pension schemes.	Termination of employment + 75 years
Finance	Cash, Investments and Assets	Records documenting the opening, closure and routine administration of bank accounts.	Closure of account + 6 years
Finance	Cash, Investments and Assets	Records documenting routine bank account deposits / withdrawals / transfers (paying-in slips, transfer instructions, bank statements etc.).	Current financial year + 6 years
Finance	Procurement	Records documenting supplier evaluation criteria.	Superseded + 5 years
Finance	Procurement	Records documenting invitations to prospective suppliers to apply for approval.	Expiry of invitation OR Rejection of

<b>Responsibility</b>	<b>Class No.</b>	<b>Description</b>	<b>Retention Period</b>
			application + 6 months OR Completion of approval
Finance	Procurement	Records documenting the evaluation of applications for approval from prospective suppliers, and notification of the outcome: approved suppliers.	Termination of approval
Finance	Procurement	Records documenting the evaluation of applications for approval from prospective suppliers, and notification of the outcome: rejected suppliers.	Rejection + 1 year
Finance	Procurement	Records documenting the process of inviting and evaluating pre-qualification submissions from prospective suppliers.	Award of supply contract + 1 year
Finance	Procurement	Records documenting Invitations to Tender and tender evaluation criteria.	Termination of supply contract awarded + 6 years
Finance	Procurement	Records documenting the issue of Invitations to Tender and handling of incoming tenders.	Award of supply contract + 1 year
Finance	Procurement	Records documenting the evaluation of tenders, the conduct of negotiations with tenderers and the notification of the results of the tender evaluation process: rejected tenders.	Award of supply contract + 1 year
Finance	Procurement	Records documenting the evaluation of tenders, the conduct of negotiations with tenderers and the notification of the results of the tender evaluation process: accepted tenders.	Termination of supply contract awarded + 6 years
Finance	Procurement	Contract award report (as required by the Regulations cited).	Termination of supply contract awarded + 6 years
Finance	Procurement	Statistical reports to HM Treasury on contracts awarded (as required by the regulations cited).	Current year + 3 years

<b>Responsibility</b>	<b>Class No.</b>	<b>Description</b>	<b>Retention Period</b>
Finance	Procurement	Records documenting variations to contracts (e.g. revisions, extensions).	Termination of contract + 6 years
Finance	Procurement	Records documenting the monitoring of supplier performance and action taken regarding under-performance.	Termination of contract + 6 years
Human Resources	Human Resources Strategy and Planning	Records containing data on and analyses of, performance against the plans for the implementation of the institution's personnel strategy.	Current year + 3 years
Human Resources	Human Resources Strategy and Planning	Records containing reports of performance against the plans for the implementation of the institution's personnel strategy.	Current year + 3 years
Human Resources	Human Resources Strategy and Planning	Records documenting the conduct and results of audits and reviews of the personnel management function, and responses to the results.	Current year + 3 years
Human Resources	Human Resources Strategy and Planning	Records documenting the assessment and analysis of workforce requirements, and the identification and evaluation of options for meeting these requirements.	Current year + 3 years
Human Resources	Human Resources Strategy and Planning	Records documenting management succession plans.	Current year + 3 years
Human Resources	Human Resources Strategy and Planning	Records documenting the development and evaluation of job specifications.	Current year + 3 years
Human Resources	Recruitment	Records documenting internal authorisation for recruitment.	Current year + 1 year
Human Resources	Recruitment	Records documenting enquiries about vacancies and requests for application forms.	Completion of appointment + 6 months
Human Resources	Recruitment	Records documenting the handling of applications for vacancies: unsuccessful applications.	Completion of appointment + 6 months
Human Resources	Recruitment	Records documenting the handling of applications for vacancies: successful applications.	Termination of employment + 6 years
Human Resources	Recruitment	Records documenting the handling of unsolicited applications for employment.	Current Year + 6 months



<b>Responsibility</b>	<b>Class No.</b>	<b>Description</b>	<b>Retention Period</b>
Human Resources	Induction, Training and Development	Records containing summary information on workforce training and development needs.	Current year + 3 years
Human Resources	Induction, Training and Development	Completion of analysis of feedback + 6 months	Completion of analysis of feedback + 6 months
Human Resources	ICT Systems Management	Records documenting the opening, maintenance and closure of staff user accounts for ICT systems.	Closure of account + 1 year
Human Resources	Performance and Reward	Records documenting pay reviews.	Current year + 3 years
Human Resources	Performance and Reward	Records documenting special reward schemes e.g. Merit Reviews.	Merit review +3 years
Human Resources	Workforce Welfare	Records documenting the monitoring of hours worked by employees, as required by the Regulations cited.	Date of record + 2 years
Human Resources	Workforce Relations	Records containing (identifiable) individual responses to workforce surveys and consultations.	Completion of analysis of responses +1 year
Human Resources	Workforce Relations	Records documenting grievances raised by staff (which relate directly to their own contracts of employment), the institution's response, action taken and the outcome.	Last action on case + 6 years
Human Resources	Contracts/Conditions of Employment	Records documenting an employee's initial application for employment with the institution.	Termination of employment + 6 years
Human Resources	Contracts/Conditions of Employment	Supporting documentation (e.g. references) for an employee's initial application for employment with the institution. For records documenting pre-employment health screening, see Health & Safety Management, Employee Health Surveillance.	Termination of appointment +6 years
Human Resources	Contracts/Conditions of Employment	Records documenting an employee's subsequent applications for other jobs within the institution.	Termination of employment + 6 years

<b>Responsibility</b>	<b>Class No.</b>	<b>Description</b>	<b>Retention Period</b>
Human Resources	Contracts/Conditions of Employment	Records documenting an employee's contract(s) of employment with the institution.	Termination of employment + 6 years
Human Resources	Contracts/Conditions of Employment	Records documenting changes to an employee's terms and conditions of employment.	Termination of employment + 6 years
Human Resources	Contracts/Conditions of Employment	Records documenting the job descriptions of positions held by an employee within the institution.	Duration of job + 1 year
Human Resources	Contracts/Conditions of Employment	Records documenting induction programmes attended by an employee.	Termination of employment + 6 years
Human Resources	Contracts/Conditions of Employment	Records documenting an employee's identified training and development needs, and the action taken to meet these needs.	Completion of actions + 3 years
Human Resources	Contracts/Conditions of Employment	Records documenting job-specific statutory / regulatory training requirements for an employee, and the training provided to meet these requirements.	Termination of employment + 6 years
Human Resources	Contracts/Conditions of Employment	Records documenting routine assessments of an employee's performance, and any consequent action taken.	Termination of employment + 6 years
Human Resources	Contracts/Conditions of Employment	Records documenting disciplinary proceedings against an employee, where employment continues.	Termination of employment + 6 years
Human Resources	Contracts/Conditions of Employment	Records documenting disciplinary proceedings against an employee, where employment does not continue.	Termination of employment + 6 years
Human Resources	Contracts/Conditions of Employment	Records documenting an employee's remuneration and rewards (e.g. bonuses, merit awards, long service awards).	Current year + 3 years
Human Resources	Contracts/Conditions of Employment	Records relating to the administration of an employee's contractual holiday entitlement.	Current Year + 3 years
Human Resources	Contracts/Conditions of Employment	Records documenting the authorisation and administration of special leave, e.g. compassionate leave, study leave.	Current year + 3 years

<b>Responsibility</b>	<b>Class No.</b>	<b>Description</b>	<b>Retention Period</b>
Human Resources	Contracts/Conditions of Employment	Records documenting an employee's absence due to sickness.	Termination of employment + 6 years
Human Resources	Contracts/Conditions of Employment	Records documenting the authorisation and administration of statutory leave entitlements, e.g. parental leave.	Completion of entitlement + 6 years
Human Resources	Contracts/Conditions of Employment	Records documenting entitlements to, and calculations of, Statutory Maternity Pay.	Current tax year + 3 years
Human Resources	Contracts/Conditions of Employment	Records containing an employee's basic personal details (e.g. address, next of kin, emergency contacts).	Duration of employment
Human Resources	Contracts/Conditions of Employment	Records documenting pre-employment health screening of an employee: employees exposed to hazardous substances during employment.	Termination of employment + 6 years
Human Resources	Contracts/Conditions of Employment	Records documenting major injuries to an employee arising from accidents in the workplace.	Termination of employment + 10 years
Human Resources	Contracts/Conditions of Employment	Records documenting an employee's termination of employment by voluntary resignation, redundancy, retirement (including on medical grounds) or dismissal	Termination of employment + 6 years
Human Resources	Contracts/Conditions of Employment	Records documenting references provided in confidence in support of an employee's application(s) for employment by another organisation.	Duration of employment + 3 years
Human Resources	Pensions	Records documenting the institution's relationships with pension schemes to which all or part of its workforce belong.	Termination of relationship + 5 years
Human Resources	Pensions	Records documenting routine communications with the pension schemes. For administration of individual employees' relationships with the pension schemes, use Employee Contract Management.	Termination of employment + 6 years

<b>Responsibility</b>	<b>Class No.</b>	<b>Description</b>	<b>Retention Period</b>
Human Resources	Pensions	For administration of individual employees' relationships with the pension schemes, use Employee Contract Management.	NA
Human Resources	Trades Unions/Industrial Relations	Records documenting routine communications with trade union representatives, including minutes of meetings.	Current year + 10 years
Human Resources	Trades Unions/ Industrial Relations	Records documenting consultations/negotiations with trades unions on specific issues.	Last action on issue + 10 years
Estates	Estate Management	CCTV Recordings.	Creation +1 Month
Services	Estate Management	Records of security passes issued to visitors, employees, other staff and students.	Expiry of pass + 1 week
Estates	Estate Management	Records documenting the conduct of routine security surveillance of properties.	Creation +1 Year
Estates	Estate Management	Records documenting security breaches or incidents, and action taken.	Last action on incident + 1 year
Estates	Health and Safety	Records documenting notifications of appointments of safety representatives by trade unions under the Safety Representatives and Safety Committees Regulations 1977.	Termination of appointment + 1 year
Estates	Health and Safety	Records documenting the provision of time off, and other facilities and assistance, for safety representatives appointed under the Safety Representatives and Safety Committees Regulations 1977.	Current year + 5 years
Estates	Health and Safety	Records documenting consultations and other communications with safety representatives appointed under the Safety Representatives and Safety Committees Regulations 1977.	Current year + 50 years
Estates	Health and Safety	Records documenting the election of members of a safety committee formed under the Safety Representatives and Safety Committees Regulations 1977.	Termination of membership + 1 year

<b>Responsibility</b>	<b>Class No.</b>	<b>Description</b>	<b>Retention Period</b>
Estates	Health and Safety	Records documenting the election of representatives of employee safety under the Health and Safety (Consultation with Employees) Regulations 1996.	Termination of appointment + 1 year
Estates	Health and Safety	Records documenting consultations and other communications with representatives of employee safety elected under the Health and Safety (Consultation with Employees) Regulations 1996, or with all employees directly.	Current year + 50 years
Estates	Health and Safety	Records documenting the provision of training (specifically related to their functions as representatives) for representatives of employee safety elected under the Health and Safety (Consultation with Employees) Regulations 1996.	NA
Estates	Health and Safety	Records documenting the provision of time off, and other facilities and assistance, for representatives of employee safety appointed under the Health and Safety (Consultation with Employees) Regulations 1996.	Current year + 5 years
Estates	Health and Safety	Records documenting the provision of information, instruction and training for employees, students and others on health and safety in the institution's premises.	Current year + 5 years
Estates	Health and Safety	Records documenting the content of information and instruction on health and safety matters provided for members of the public and others who have legitimate access to the premises, and the methods of delivery.	Superseded + 5 years
Estates	Health and Safety	List of employees exposed to Group 3 or Group 4 biological agents (defined in the Regulations).	Last entry + 40 years
Estates	Health and Safety	Records documenting accidents and incidents involving Group 3 or Group 4	Date of recording + 40 years

<b>Responsibility</b>	<b>Class No.</b>	<b>Description</b>	<b>Retention Period</b>
		biological agents (defined in the Regulations).	
Estates	Health and Safety	Records documenting the examination, testing and repair of plant and equipment provided to control exposure to substances hazardous to health.	Date of examination
Estates	Health and Safety	Records documenting the conduct and results of monitoring of exposure of employees to substances hazardous to health: general exposure.	Date of action + 5 years
Estates	Health and Safety	Records documenting the conduct and results of monitoring of exposure of employees to substances hazardous to health: exposure of identifiable individual employees.	Date of monitoring + 40 years
Estates	Health and Safety	Records documenting air monitoring conducted in accordance with the requirements of the Regulations: where exposure requires individual employees to be under medical surveillance under Regulation 10.	Date of monitoring + 40 years
Estates	Health and Safety	Health surveillance records of identifiable individual employees who are exposed to lead.	Date of last entry on record + 40 years
Estates	Health and Safety	Records documenting the conduct and results of risk assessments of work which exposes employees to asbestos: where the exposure of employees may exceed the action level.	Duration of work to which assessment relates
Estates	Health and Safety	Records documenting the conduct and results of risk assessments of work which exposes employees to asbestos: in all other cases.	Completion of work to which the assessment relates + 5 years
Estates	Health and Safety	Records documenting air monitoring conducted in accordance with the requirements of the Regulations: where exposure requires health records to be	Date of monitoring + 40 years

<b>Responsibility</b>	<b>Class No.</b>	<b>Description</b>	<b>Retention Period</b>
		kept for individual employees under Regulation 21.	
Estates	Health and Safety	Records documenting air monitoring conducted in accordance with the requirements of the Regulations: in all other cases.	Date of monitoring + 5 years
Estates	Health and Safety	Health surveillance records of identifiable individual employees who are exposed to asbestos.	Date of last entry on record + 40 years
Estates	Health and Safety	Certificates of medical examination of identifiable individual employees who are exposed to asbestos.	Date of certificate + 40 years
Estates	Health and Safety	Records documenting the recording of accidents, dangerous occurrences and outbreaks of notifiable diseases on the institution's premises.	Date of recording + 3 years
Estates	Health and Safety	Records documenting the investigation of accidents, dangerous occurrences and outbreaks of notifiable diseases on the institution's premises.	Closure of investigation + 40 years
Estates	Health and Safety	Reporting of reportable accidents, dangerous occurrences and outbreaks of notifiable diseases to enforcing authorities.	Date of notification + 3 years
Estates	Health and Safety	Records documenting accidents and incidents involving Group 3 or Group 4 biological agents (defined in the Regulations).	Date of recording + 40 years
Estates	Health and Safety	Records documenting pre-employment health screening of an employee.	Termination of employment + 40 years
Estates	Health and Safety	Health (surveillance) records of identifiable individual employees, other than those specified below.	Date of last surveillance action + 40 years
Estates	Health and Safety	Health (surveillance) records of identifiable individual employees who are exposed to substances hazardous to health, as defined by the Regulations cited.	Date of last entry on record + 40 years

<b>Responsibility</b>	<b>Class No.</b>	<b>Description</b>	<b>Retention Period</b>
Estates	Health and Safety	Health (surveillance) records of identifiable individual employees who are exposed to lead, as required by the Regulations cited.	Date of last entry on record + 40 years
Estates	Health and Safety	Health (surveillance) records of individual employees who are exposed to asbestos, as required by the Regulations cited.	Date of last entry on record + 40 years
Estates	Health and Safety	Certificates of medical examinations of individual employees who are exposed to asbestos, as required by the Regulations cited.	Date of last entry on record + 40 years
Estates	Health and Safety	Records documenting the nomination/appointment of fire wardens.	Termination of appointment
Estates	Health and Safety	Records documenting the provision of role-specific training for fire wardens	Termination of appointment + 5 years
Estates	Health and Safety	Records documenting the appointment of official first aiders.	Termination of appointment
Estates	Health and Safety	Records documenting the provision of approved training (specifically related to their functions as first aiders) for first aiders.	Termination of appointment + 5 years
Estates	Environmental Management	Records documenting the recording of environmental incidents on the institution's premises or caused by its operations.	Last action on incident + 40 years
Estates	Environmental Management	Records documenting the investigation of environmental incidents on the institution's premises or caused by its operations.	Closure of investigation + 40 years
Estates	Environmental Management	Records documenting the notification and reporting of reportable environmental incidents to enforcing authorities.	Date of notification + 5 years
Estates	Environmental Management	Register of 'special waste' removed from the premises for disposal by registered / licensed contractors.	Removal of waste consignment + 3 years



<b>Responsibility</b>	<b>Class No.</b>	<b>Description</b>	<b>Retention Period</b>
MIS	Student Recruitment	Records documenting the handling of enquiries from prospective students.	Current academic year + 1 year
MIS	Student Admission Policies and Procedures	Records documenting the handling of applications for admission: successful, unsuccessful and HE/Clearing.	End of student relationship + 6 years
MIS	Student Admission and Registration/Enrolment	Records documenting the initial assessment of Students (including E&M and ESOL)	Termination of student relationship + 6 years
Student Support	Student Record Administration	Records of administration of Student Finance	Current + 6 Years
Student Support	Student Discipline	Records documenting the conduct and results of disciplinary proceedings against individual students.	Last action on case + 6 years
Student Support	Student Support and Welfare Management	Records documenting the provision of Welfare / Advice Services to individual students.	Current year +6 years
Student Support	Student Support and Welfare Management	Records Relating to Careers Advice.	Duration of enrolment +3 years
Student Support	Student Support and Welfare Management	Records relating to Learning Support for Students with specific needs.	Current +7 Years
Student Support	Student Support and Welfare Management	Records documenting the handling of user / customer complaints about a student support service.	Last action on complaint + 6 years
Student Support	Student Complaint Handling	Records documenting the handling of complaints by individual students where the formal complaints procedure is not initiated.	Last action on complaint
Student Support	Student Associations and Unions	Records relating to the operation and activities of the Students Union, and other clubs, associations and non-academic activities organised by students	Permanent
MIS	Student Record Administration	Records containing full personal data on individual students.	ESF match funded to be retained for x 12 years (depending on ESF start) all other data used

Responsibility	Class No.	Description	Retention Period
			for funding x 6 years
MIS	Student Record Administration	Core student data.	ESF match funded to be retained for x 12 years (depending on ESF start) all other data used for funding x 6 years
MIS	Student Record Administration	Published reports - retain for same duration as the data	6 years / 12 years
MIS	Student Record Administration	Records documenting the handling of individual students' / employers requests for statements of results/transcripts.	Last action on request + 1 year
MIS	Student Record Administration	First Destination Surveys: individual responses.	6 years / 12 years
MIS	Student Progress and Assessment Administration	Records documenting the organisation of examination facilities, including special arrangements for students with special needs.	Current academic year + 1 year
MIS	Student Progress and Assessment Administration	Records documenting the termination of individual students' programmes.	Termination of student relationship + 6 years
MIS	Student Progress and Assessment Administration	Records documenting the selection, appointment and training of external examiners.	Termination of appointment + 1 year
MIS	Student Progress and Assessment Administration	Records documenting the withdrawal of individual students from the institution.	Termination of relationship with student + 6 years / 12 years
MIS	Student Progress and Assessment Administration	Records documenting the control of examination papers and examination scripts.	Current academic year + 1 year
MIS	Student Progress and Assessment Administration	Arrangements for Assessments and examinations.	Current year + 6 years
MIS	Student Progress and Assessment Administration	Pass/Qualification/Awards lists.	ESF match funded to be retained for x 12 years (depending on ESF start) .

<b>Responsibility</b>	<b>Class No.</b>	<b>Description</b>	<b>Retention Period</b>
Programme Areas	Student Progress and Assessment Administration	Records documenting individual students' submission of assessed work and handling of reports of mitigating circumstances.	Current academic year + 1 year
Programme Areas	Student Progress and Assessment Administration	Records documenting feedback on academic progress, and general academic guidance and support, given to individual taught students.	Completion of student's programme + 1 years
Programme Areas	Development and Execution of Programmes and Courses	Records documenting routine solicited feedback on taught programmes from staff and examiners: individual feedback.	Life of course + 1 year
Programme Areas	Internal and External Review of Courses	Records documenting routine solicited feedback on taught courses from staff and examiners: individual feedback.	Life of course + 1 year
Programme Areas	Internal and External Review of Courses	Records documenting routine solicited feedback on taught courses from students: individual feedback.	Life of the course + 1 year
Programme Areas	Course Administration	Assignment of students to classes/groups.	Current year
Organisational Development and Talent	Student Complaint Handling	Records documenting the handling of formal complaints made by individual students against the institution.	Last action on case + 6 years
Quality	Student Liaison	Results of user / customer surveys: individual responses.	Completion of analysis of survey responses
Data Protection Compliance	Information Resources Management	Records documenting the handling of requests for access to personal information held by the institution under the General Data Protection Regulation (GDPR).	Last action on request + 1 year
Data Protection Compliance	Information Resources Management	(Anonymised) statistics, analyses and reports of requests for access to personal information held by the institution under current data protection laws (the Data Protection Act 2018 and General Data Protection Regulation (GDPR) (EU) 2016/679).	Current year + 10 years

<b>Responsibility</b>	<b>Class No.</b>	<b>Description</b>	<b>Retention Period</b>
Freedom of Information	Information Resources Management	Records documenting the development and maintenance of the institution's Publication Scheme, as required by the Freedom of Information Act 2000 (c. 36) and the Freedom of Information (Scotland) Act 2002 (asp 13).	Completion of revision of Publication Scheme + 5 years
Freedom of Information	Information Resources Management	Records documenting the handling of requests for access to information held by the institution under the Freedom of Information Act 2000 (c. 36) or the Freedom of Information (Scotland) Act 2002 (asp 13).	Last action on request + 6 years
Freedom of Information	Information Resources Management	(Anonymised) management statistics, analyses and reports of requests for information held by the institution, made under the Freedom of Information Act 2000 (c. 36) or the Freedom of Information (Scotland) Act 2002 (asp 13).	Current year + 10 years
Environmental information compliance	Information Resources Management	Records documenting the handling of requests for environmental information held by the institution, made under the Environmental Information Regulations 2004 (SI 2004/3391) or the Environmental Information (Scotland) Regulations 2004 (SSI 2004/520).	Completion of request handling process + 3 years
Environmental information compliance	Information Resources Management	(Anonymised) management statistics, analyses and reports of requests for environmental information held by the institution, made under the Environmental Information Regulations 2004 (SI 2004/3391) or the Environmental Information (Scotland) Regulations 2004 (SSI 2004/520).	Current year + 10 years
ILT	Information and Communications Systems Management	Records documenting user requests for technical and application support, and assistance provided.	Last action on request + 1 year
ILT	ICT Systems Management	Records documenting faults reported by users of ICT systems, and action taken to	Last action on fault + 1 year

<b>Responsibility</b>	<b>Class No.</b>	<b>Description</b>	<b>Retention Period</b>
		investigate and resolve the problem.	
ILT	ICT Systems Management	Records documenting attempted or actual security breaches of the institution's ICT systems, and action taken.	N/A
ILT	ICT Systems Management	Records documenting the development of technical and application training for ICT system users.	Superseded + 1 year
Directorate	Government and Regulator Relations	Records containing information that institutions are legally obliged to provide to the funding Bodies.	6 years / 12 years
Directorate	Community Relations	Records documenting formal complaints from members of the local community, the internal handling of these complaints and the responses provided.	Last action on complaint + 6 year
Directorate	Fundraising/Grants	Records containing details of individual responses to fundraising campaigns.	Academic year they fall into
Directorate	Alumni Relations	Records containing personal data on individual alumni.	While current (or likely to be current)
Directorate	Governing Body	Records documenting the appointment of members of the institution's governing body.	Termination of appointment + 6 years
Directorate	Governing Body	Records documenting the development and establishment of the institution's governance strategy: key records.	Superseded + 10 years
Directorate	Governing Body	Records documenting the provision of training and development for members of the institution's governing body.	Current year + 3 years
Directorate	Governing Body	Records documenting the conduct and proceedings of meetings of the institution's governing body	Life of the Institution
Directorate	Governing Body	Register of Interests of members of the Governing Body, senior staff and others covered by conflict of interest policies.	Termination of appointment + 6 years
Directorate	Quality Management	Formal Public Complaints.	Date of last action + 6 years

