| **INFORMATION POLICY (Data Protection and Freedom of Information)** |
|---|
| Approved by: Audit Committee |
| **Date approved: 6 March 2025** |
| Strategy/Policy Responsibility: Vice Principal Finance & Resources |
| **Publication on staff intranet: Yes** |
| **General publication on College website: Yes** |
| **Review date: March 2027** |

# Section A – Data Protection

# 1 Introduction

This policy sets out Croydon College's (the "College", "we" and "us") legal obligations in relation to personal data and what your responsibilities are to ensure that we comply with them. It includes requirements which everyone must follow, whether they are employees, students, academic staff, governors or volunteers, and regardless of their status or type of contract. In this policy, references to "you" mean anyone that processes personal data for the College, regardless of their employment status.

The College holds a large amount of information about its students, staff, visitors and other individuals, and about its organisation and administration. Information about individuals is covered comprehensively by data protection legislation. It is the College's policy to comply with all the legislative requirements in force and to co-operate with the bodies which monitor and enforce compliance. This policy applies whenever you handle personal data about anyone else, including colleagues, job applicants, students, visitors and suppliers who are individuals or partnerships and individuals at suppliers that are companies.

As a Public Authority, the College is obliged to comply with the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR), and policy matters concerning those requirements appear in Appendix 1 to this policy.

The Information Commissioner's Office (ICO) monitors compliance with data protection legislation, including the Data Protection Act (DPA) 2018, the UK General Data Protection Regulation (as defined in the DPA 2018, UK GDPR), and FOIA and EIR, and also provides guidance to organisations. The ICO can investigate complaints, audit use of personal data and take action against us (and in some cases against you personally) for breaches of the data protection legislation.

Details that are personal data are normally also confidential with additional confidentiality obligations with which the College must comply.

# 2 Data Protection

## 2.1 Introduction

Croydon College is a Controller within the meaning of the data protection legislation. The College is committed to preserving the privacy of students, employees and others about whom it holds personal data, and to complying with data protection legislation. That compliance includes protecting personal data, keeping adequate records, observing individuals' rights and reporting data security breaches.

As a public authority, the College is required by the UK GDPR to have a Data Protection Officer (DPO) whose role is to inform and advise the College about, and to ensure that we remain compliant with, data protection legislation. The College's DPO is the Director of MIS, who must be consulted in all significant data protection matters and when any policy decisions are made.

## 2.2 Compliance

Everyone within the scope of this policy is responsible for reading and complying with this policy and any other policies and/or procedures referred to in it, and raising any concerns about data privacy.

A "security breach" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It covers malicious incidents such as a cyber-attack, but it also covers other incidents, many of which can arise as a result of human error. Examples of security breaches include a lost laptop, device or file or giving personal data to the wrong person over the telephone or via email.

Any security breach or suspected security breach must be **immediately** reported to the Line Manager, Tutor or Data Protection Officer. The College must quickly assess the nature of the breach and may be legally obliged to report it to the ICO within 72 hours (whether or not over a weekend, bank holiday or College closure period). The College can be penalised if it fails to notify reportable breaches to the ICO within this strict timescale. Incidents which may be reportable to the ICO (and which must therefore be reported to us) include the unintended or unauthorised destruction, loss or alteration of personal data (whether accidental or otherwise), or access to or disclosure of personal data. The Data Protection Officer is responsible for making any required report to the ICO.

All members of staff are required to complete all relevant College provided training in data protection and keep that training up to date.

Any breach of the requirements of this policy will be investigated, and the College will use its Disciplinary Policy and procedures as necessary if a person is found to have deliberately, negligently or recklessly failed to comply with what the policy requires. Where a criminal offence is suspected the matter will be reported to the police.

## 2.3 Definitions

The following terms are used within the Data Protection section of the policy:

**Personal Data** is any information (in any format) from which a living individual can be identified, either by itself or when combined with other information. For example, names, addresses, contact details, salary details, job titles, CVs, photographs, CCTV images, credit card numbers, logon credentials, marketing preferences and data gathered from website cookies are all capable of being personal data.

**Special category personal data** (or sensitive personal data) is personal data which is likely to present a greater risk to individuals if lost. It is a specific list, comprising information about racial or ethnic origin, political opinions, religious or

other beliefs, trade union membership, physical or mental health or condition, sexual life and genetic and biometric data. Information about criminal offences and allegations, court proceedings and sentences is also included in a separate category.

**Criminal record data** is personal data relating to criminal allegations, charges, prosecutions, proceedings and outcomes.

A **Data Subject** is the living person who the personal data is about. For simplicity, in this policy, we sometimes refer to these people as "individuals".

The **Controller** is Croydon College.

A **Processor** is anyone processing personal data on behalf of the College.

The **Data Protection Officer** for the College is the Director of MIS.

**Processing** is everything we do with personal data including collecting, storing, using, disclosing and disposing of it and whether this is passive (simply storing details) or active, such as amending them.

Even if an individual is deceased, details which were personal data about them will still be confidential information and must be kept confidential.

## 2.4 General requirements

The College must process personal data only as permitted by law. It must be collected and used fairly, stored and disposed of safely, and not disclosed to any unauthorised person. Any queries should be raised initially with the Line Manager or Tutor; issues that cannot be resolved locally should be referred to the DPO.

No unfair pressure may be applied to a data subject in order to collect or obtain access to any of their personal data. It is against the law to require someone to make a Subject Access Request to a Controller in order to obtain their personal data for our use.

## 2.5 Data Protection Principles

There are six main data protection principles set out in UK GDPR which we must follow in respect of all personal data we process. It is essential that you also comply with them when processing personal data for us. These state that personal data must be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. Accurate and, where necessary, kept up to date
5. Kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed, and
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

The College is also required to demonstrate its compliance with these principles in the processing of personal data and to evidence it has appropriate processes in place to ensure its compliance.

## 2.6 Privacy notices

The College is required to tell individuals that it is processing their personal data as well as the reasons why the College needs this information, how it uses that information and who it will share the information with, providing specific types of information set by the data protection legislation. The College will do that in different ways as follows:

- in a Privacy Statement on the College's website – this will give general information about processing, security, the DPO and individual's rights, especially in respect of website users and general enquirers
- in Privacy Notices on individual forms, whether to job applicants, employees or students, and whether on paper or on line – these will give specific information about processing, disclosures and retention, and where consent is used, information about the right to withdraw it, and
- in separate communications about privacy after personal data has been received in an unsolicited way or disclosed to a new recipient.

You must not collect additional personal data compared to the details described in the relevant College Privacy Notice without express prior written approval from the [DPO]. You must not use personal data collected for any new purposes over and above those set out in the relevant Privacy Notice without express prior written approval from the DPO.

## 2.7 Communications in relation to personal data

If you receive any communication from an individual in relation to their personal data or from any other person or body (including the ICO) in relation to personal data, you must inform the DPO immediately and provide them with the relevant communication.

Under the data protection legislation the College must by law respond to certain requests from individuals in relation to their personal data within strict timescales, so it is very important that [the DPO] is made aware of each request as quickly as possible. This includes requests made by third parties acting as representatives and lawyers for such individuals. You must also cooperate with [the DPO] by providing any other information and assistance that they may require.

Please do not, under any circumstances, respond to requests or communications about personal data yourself without prior written approval and input from the DPO.

### 2.7.1 Right of access

Individuals have the right to request access to any personal data that the College holds about them in any format. This is usually referred to as a Subject Access Request ("SAR") which can be made by individuals verbally or in writing. Unless

and to the extend the DPO determines that details are exempt under the data protection legislation, the law allows individuals to:

- obtain confirmation that the College is processing their personal data
- obtain a copy of their own personal data, and
- obtain other supplementary information about the processing.

No fee is chargeable for making an SAR except in exceptional circumstances, such as where the request is 'manifestly unfounded or excessive' or the individual is asking for information they have already received. Only the DPO may determine that a fee is chargeable for a request, or decide to refuse a request.

The College will take reasonable steps to verify the identity of the requester where necessary. The College will supply the requested personal data to which the individual is entitled as soon as possible and in any event within one month of the date of the request (or the date the requester supplies evidence of their identity or the fee if appropriate).

A SAR may also be made via a third party on the requester's behalf. The College may need to verify that the third party who is making the request has the authority to do so on behalf of the individual, which may involve requiring proof of consent or the College contacting the individual to whom the request relates directly.

The DPO will oversee the responses to all requests to ensure that personal data about other people and exempt personal data is not inappropriately disclosed and so that the College meets the strict response timescales laid down in the data protection legislation. Records will be kept in line with the ICO's guidance.

You may be guilty of a criminal offence if you deliberately hide, destroy or delete or amend requested personal data to avoid or affect how the College can respond to a request by a data subject in respect of their personal data.

### 2.7.2 Other rights

Individuals have a number of other legal rights:

- to have inaccurate or incomplete personal data rectified
- to have personal data erased (also called 'the right to be forgotten')
- to restrict how the College processes their personal data.
- to have a copy of their personal data in a portable form to use with other service providers
- to object to the College processing their personal data (including to certain marketing), and
- to object to the College making automated decisions that affect them.

Some of these rights will only apply in limited circumstances and to certain personal data. Any request from an individual (or their representative or lawyer) which is exercising any of these rights must be passed without delay to the DPO.

## 2.8 Security requirements

Security arrangements are to protect the confidentiality, integrity and availability of personal data. Measures that everyone is required to take to minimise the risk of unauthorised access to, use or disclosure, corruption or loss of personal data are contained in the Information Technology (IT) and Monitoring Policy and Information Security Policy, including:

- acceptable and secure use of computers, other devices and software, and
- secure and effective use of passwords.

Other appropriate measures required for effective security include:

- being aware of who else might be able to read information from computer screens and avoiding this
- locking computer screens when away from the desk
- shredding printouts and other paper documents when no longer needed
- keeping paper documents locked in cabinets or rooms when not in use, and
- checking emails before hitting 'Send' to make sure that (a) they are going to the right recipients, and (b) that attachments are limited to what is necessary; note that particular care is needed with Excel files which can contain hidden rows, columns and sheets
- ensuring that recognised portals with, or other secure arrangements (rather than email) to, recognised authorised recipient bodies/persons, are used to send or share relevant information securely, especially where special category personal data, criminal record data, or personal data affecting a large number of individuals, or that is particularly private or sensitive or higher risk (e.g. passport, national insurance and bank account details.

You must not download and use on College devices, laptops, mobiles of systems (or personal devices used for College work purposes) or input any personal data or confidential information into, any Artificial Intelligence (AI) software, tool, product, platform or system, such as ChatGPT.

Any use of AI on any such College devices or personal devices used for College work purposes must be by express prior written approval from the Director of IT and Estates and no personal data or confidential information can be input into them.

All such AI systems retain details input and use them to 'train' and improve the system, including by making details input available to others in terms of outputs which the system produces and provides to other system users. This means that inputting details into such systems will involve a breach of data protection legislation, breach of privacy and breach of confidence.

You must not create your own systems for creating records of, documenting or storing personal data (only use College systems and follow its document and records management policies). You must not use College personal data /

confidential information for your own purposes or those of a third party, and must not:

- send any such details to, download it to or save it to, any personal device (unless expressly authorised by the DPO and in accordance with all conditions set by the College); or
- send it to any personal email or social media account; or
- publish any such details.

You must only access and use College personal data (in College databases, systems, devices and otherwise) that you are officially authorised to use and to the details you need to properly perform your role for the College. If you notice that you or others appear to be able to access systems, areas within systems or personal data that you should not be entitled or authorised to access or see, please immediately notify the DPO with details and do not continue to access any such details, print them, download them or copy them.

Deliberately or recklessly obtaining unauthorised access to College devices, systems, or databases is a criminal offence. Unlawfully obtaining College personal data (or disclosing it to or sharing it with any third party) without College consent is a criminal offence.

## 2.9 Disclosure of personal data and data sharing

Personal data is not to be disclosed to anyone unless it is relevant, necessary and lawful to do so, Data can also only be shared on a 'need to know' basis, taking account of the authorised role and responsibilities of the recipient (even if a College employee). This includes showing details to a person, or giving them access to them (including on screen or remotely) and even if the details are not 'sent' outside the College. These rules also apply where the sharing is necessary:

(a) for performance of a contract with a member of staff, for instance sharing salary information with a payroll provider (with which the College has a data processing agreement in place) for payment of salary
(b) to respond to a legitimate request for assistance by the police or other law enforcement agency
(c) to comply with a law, regulation or court order, for example, where requested by customs officials for the investigation of tax offences
(d) to engage and/or obtain advice from professional advisers (e.g. accountants, lawyers, external auditors etc);
(e) to deal with any legal dispute or administrative claim between us and a third party (e.g. to that third party and lawyers representing them);
(f) to liaise with third parties in connection with the disposal of any of the College's asset(s);
(g) to protect an individual's vital interests and/or
(h) as otherwise permitted by, and in accordance with, applicable laws.

Before disclosing personal data to a recipient other than a College employee, it is necessary to understand whether they will act as a Processor (e.g. using pension personal data on behalf of the College to provide pension services to the College

in respect of College staff), or as another controller, using the details on their own account, even if as part of providing their services to and helping the College (e.g. when obtaining legal advice from the College's external lawyers). This is important as the College needs to keep records about the types of body with which it shares personal data and whether they are a Processor or Controller; and different rules must be followed under data protection legislation depending on whether the recipient is a Controller or Processor.

Whether a Processor or Controller, no personal data or confidential information should be disclosed with any person or body outside the College unless authorised by the DPO.

Before a Processor can be appointed and used, the College's Financial Regulations on procurement must be followed. To comply with data protection legislation and mandatory clauses required when using a Processor, contract terms with approved Processors must include the College's template data processing agreement terms for use on a controller to processor basis (unless otherwise expressly authorised by the DPO).

Before sharing any personal data with another Controller, to comply with data protection legislation the College must:

- ensure there is a lawful basis under the data protection legislation for the disclosure
- check that the recipient is entitled to receive the personal data
- check that the individual has given consent if appropriate
- limit the personal data to only that which is necessary for the purpose, and
- ensure that security measures for sending the data are adequate.

Controller recipients must be expressly approved in advance in writing by the DPO together with the types of affected personal data that may be shared with them and for the types of specified processing purposes.

You should always check with the DPO if you are unsure whether you are permitted to disclose personal data to a third party. If you receive a request for personal data, whether that be a member of staff or a student past or present please contact the DPO prior to making any disclosures to any third party.

The individual is to be advised of the disclosure (what, why and to whom) if they are not already aware of it, or if it is not covered in the applicable privacy notice, in each case unless exempt from that data protection obligation (as determined by the DPO. Examples of such an exemption may be if the disclosure was requested for the prevention or detection of crime or was necessary for legal proceedings. Such requests will be dealt with by the DPO. The DPO should be consulted if a decision is required on whether to disclose information.

If disclosing personal data to or sharing it with a third party outside the College (whether a Controller or processor) will or may involve personal data being processed outside the UK (including through remote access from outside the UK to details on screen in, or to data in systems / data storage located in, the UK), additional 'data transfer' obligations under data protection legislation must be met.

This means that information about the 'data transfer' must be obtained to allow the College to ensure the data will still be adequately or appropriately safeguarded abroad. Often, additional clauses must be included in the contract. Personal data must not be sent outside the United Kingdom (including electronic transfer to the 'cloud' or hosted abroad) without the DPO's written authorisation.

## 2.10 Working from home or remotely

If a member of staff needs to work from home or outside the College, permission for time limited off site access will need to be requested from the Director of IT and Estates. Additional measures are needed and must be complied with by you to minimise the risk of loss or disclosure of personal data. Details are included in the Information Security Policy and include:

- mandatory use of college provided equipment only
- mandatory use of the secure remote access facilities provided
- complying with College requirements and guidance for minimising risk of loss and access by anyone unauthorised (including family and friends), and
- prohibiting use of personal Internet file storage facilities ('cloud storage')

Original documents containing personal data are not to be removed from the College, and paper copies are to be avoided where possible. Personal data / confidential information copied to a mobile or portable device for remote use is only permitted if the device is encrypted and of a type approved in writing in advance by the DPO and personal data and the details must be securely deleted from that device as soon as the work is complete. The DPO should be consulted if further advice is needed.

## 2.11 Storing personal data

All information assets that include personal data must be listed in the Information Asset Register and comply with the retention periods specified. The DPO must be notified of all computerised records, and structured sets of paper-based records, which contain personal data (and you must only use the relevant official College storage repositories and systems for data, records and documents). This includes records held outside the College, even temporarily.

It is important that the College records all the personal data it holds, to comply with the UK GDPR. Failure by any member of staff to notify the DPO of an additional source of personal data could therefore result in disciplinary action.

## 2.12 New processes and changes, and automated decisions

The College is required to assess the impact on individuals' privacy of all new or changed processes and proposed adoption of new technologies. Where such related processing may result in a high risk to individuals, a specific risk assessment is required under data protection legislation and the process is called a Data Protection Impact Assessment ("DPIA"). The DPIA should be conducted as early as possible when the changes are being designed. This is because the College has a legal duty to ensure privacy by design and default and to plan in

advance for and build in compliance with its data protection legal obligations. The DPO will provide guidance on the completion of a DPIA.

Where a process involves making decisions which affect individuals automatically (i.e. without human intervention), the DPO must be informed to assess the important and nature of the affected decision making and it may be necessary to give those individuals additional information about how the decisions are made and they may have additional individual rights in relation to those decisions.

### 2.13 CCTV

CCTV cameras used by the College will be operated, and the images processed, in accordance with the Codes of Practice published by the ICO. CCTV images of people involve processing their personal data. You must not install any CCTV cameras (or other surveillance, or monitoring or tracking devices), or change the approved location and use of existing CCTV cameras (or capture sound in addition to images) without the prior written approval of the DPO.

### 2.14 Marketing

Use of personal data for marketing must comply with the data protection legislation. Whether or not personal data is involved, most online / electronic unsolicited direct marketing activities (including by email, telephone call, text messages and SMS), plus collection of data online via 'cookies' or equivalent technologies, or collection or use of location and traffic data gathered through online activities / service provision (e.g. Wi-Fi provision) must comply with the requirements of the Privacy and Electronic Communications Regulations 2003 (PECR). You must not send any marketing communications, deploy any cookies type technologies, or collect and use location and traffic data, unless you have prior written approval from the DPO to do so and comply with all conditions imposed by the DPO.

## 3 Records Management

### 3.1 Introduction

The College's records are an important asset. The College will manage its records efficiently and systematically, in a manner consistent with, sections 45 and 46 FOIA, the Code of Practice on the discharge of the obligations of public authorities under the Environmental Information Regulations 2004 (SI 2004 No. 3391), ISO15489 and the Lord Chancellor's Code of Practice on Records Management, to support the College's operations and meet legislative, regulatory and funding requirements.

Records will be created, maintained and retained in order to provide information about, and evidence of, the College's transactions and activities. Staff having responsibility for managing records will be appropriately trained, and guidance documents published.

A record is defined as any document regardless of format and whether or not it contains personal data. Records may be created, received or maintained in hard copy or electronically.

Specific guidance will be issued for employees, students, contractors, consultants, applicants, visitors and guests, to explain how and why we collect their data and their roles and responsibilities in keeping data secure.

## 3.2 Scope

This section of the policy applies to all records in hard copy and electronic format that are created, received and maintained by College staff in the course of carrying out their functions. It is binding on all those who create or use College records such as employees, students, contractors, consultants, visitors and guests.

## 3.3 Responsibilities

The Director of MIS is responsible for defining and overseeing records management activities within the College, and for promoting good practice in records management. Heads of Schools and Pathways and Directors of Service areas, as data owners, are responsible for ensuring that all records in their area are managed in accordance with this policy.

Anyone acting in breach of this policy will be subject to the College's disciplinary procedures.

## 3.4 Principles

The principles which the College will follow in managing its records are to:

- create and capture authentic and reliable records to demonstrate evidence, accountability and information about its decisions and activities
- ensure records are held on the most appropriate medium for the task they perform
- securely maintain and preserve access to those records as long as they are required to support College operations
- maintain a retention schedule to guide staff in the agreed retention for each type of record
- use appropriate destruction methods for records which have reached the end of their life, which reflect the sensitivity of the information contained in the records
- comply with legal requirements for keeping records
- identify and preserve securely those records deemed worthy of permanent preservation using appropriate archive facilities, and
- identify and protect vital records which the College needs in order to function effectively, in line with Business Continuity and Disaster Recovery processes.

Retention periods in the retention schedule are referenced where appropriate from entries in the Information Asset Register (see section 2.11 above).

# 4 Policy review

Comments on this policy are welcomed and should be forwarded to the Director of MIS. This Policy will be reviewed every two years or whenever a significant change to legal requirements, processes or procedures occurs to ensure this policy remains consistent and effective with the requirements of data protection legislation. The Vice Principal Finance and Resources is responsible for scheduling and conducting the review.

# 5 References

The Information Commissioner's Office (ICO): https://ico.org.uk/

Open Government Licence (version 3.0):
http://www.nationalarchives.gov.uk/information-management/re-using-public-sector-information/uk-government-licensing-framework/open-government-licence/

# Section B - Freedom of Information, environmental information and re-use of public sector information

## 1.1 Introduction

The combination of FOIA and EIR (together the Information Laws) give the public a general right of access to all recorded information held by a relevant public authority, including Croydon College. The right of access under EIR is limited to records of 'environmental information' (see section 1.3 below) and, under FOIA, to records of all other information.

The request may be for the information, a copy of it in a specific document or record, for a digest or summary of the information, or to inspect the requested information. The requester may want the information in a specific format if possible. Under FOIA, such requests must be accommodated unless not reasonably practicable. Where possible a similar approach should be adopted under EIR.

FOIA is designed to promote openness and accountability across the public sector, particularly in relation to official decision making and to the spending of public money. Its aims of transparency and accountability also apply to relevant environmental issues under EIR.

For a record of information to be 'held' by the College under FOIA or EIR, it is used by the College on its own account and for its own purposes and not solely on behalf of a third party) and whether in the direct possession of the College or under its control but in the possession of a third party and held on behalf of the College.

All information records which the College holds is covered by FOIA or (if environmental information) EIR, regardless of its format. This includes information in paper files, electronic documents, emails, databases and audio or video material.

FOIA requires disclosure of information in two main ways: (a) by proactive publication through a Publication Scheme, on the College website, and (b) to any person in response to valid written requests, subject to applicable FOIA grounds for refusal, including exemptions. Some information will, however be exempt from disclosure (see 1.7 below).

EIR does not have the same publication scheme obligations but the College must respond to any valid request made to it for environmental information, whether a written or oral request, subject to EIR exceptions and other EIR grounds for refusal.

The College is bound by FOIA and EIR not only to supply requested records of relevant information it holds when required to do so, but to provide reasonable advice and assistance to applicants who are making requests.

Requests for information may also involve third parties and the College will ensure that any third parties who either supply it with information or who deal with the College are made aware of the College's duties under FOIA and EIR and the risk that requested information may be released under FOIA or EIR as relevant unless a valid ground for refusal applies.

Subject to complying with its other legal obligations (e.g. in relation to statutory prohibitions, court orders, confidential information and personal data), the College determines at its discretion to what extent it should: proactively make information publicly available under its FOIA Publication Scheme; or reactively disclose relevant requested information held in response to a request under FOIA or EIR. The College may be required under FOIA or EIR to disclose information without consulting or obtaining consent from an affected third party or despite the third party having expressed negative views when the College consulted them.

FOIA and EIR disclosure is treated by law as not only disclosure to the requester but disclosure to the world at large i.e. publication and no conditions to limit use may be imposed when making a disclosure of requested information under FOIA or EIR. FOIA and EIR provide for public access to but not re-use of the requested information (unless a relevant dataset under FOIA is requested and disclosed).

## 1.2 Responsibilities

The Governing Body is legally responsible for compliance with FOIA and EIR. Day to day management of FOIA and EIR is the responsibility of a Data Co-ordinator (DC), which is the Director of MIS. The DC is responsible for collating the relevant requested information, determining whether FOIA or EIR applies and any relevant grounds for refusal, such as any FOIA exemptions or EIR exceptions, issuing responses and refusals and keeping records of the requests. Strict timescales are set by law for responding to requests.

If you receive a request for information or its re-use which you think may be a FOIA or EIR request, you should forward it immediately to the DC and should not respond to the request or disclose information in response to it unless you have been authorised to do so and then only as directed to do so.

All College staff must cooperate with the DC in relation to FOIA and EIR and when requested by the DC must promptly provide requested information to the DC and any requested reasons for why any specific FOIA exemption, EIR exceptions, or other ground for refusal, may be relevant and apply. That information must be supplied to the DC within the timescale required. Guidance is provided on the staff Intranet. The Marketing Team will maintain the Publication Scheme on the web site on behalf of the DC.

## 1.3 Environmental Information Regulations

The EIR give a right of access to environmental information held by public authorities. The ICO provides guidance on the definition of environmental information and how the EIR applies. If you receive a request for environmental information from the College under the EIR, or are asked to provide information in connection with an EIR request, you should notify the DC and provide assistance in the same way as you would for requests under FOIA. The DC will apply any differences in handling which are required.

The main differences between the application of FOIA and the EIR is in relation to the exceptions which can be applied to environmental information which differ in some respects from the FOIA exemptions. In addition, EIR requests can be made verbally as well as in writing, whereas FOIA requests must be made in writing.

## 1.4 Publication Scheme

The College is committed to being open and transparent, to help the public understand what it does and how it is run. It is required by FOIA to have a Publication Scheme, and has adopted the ICO's model scheme. This sets out the classes of information it routinely publishes, the manner in which that is done and any charges involved. The Guide to Information on the website indicates which documents are available and provides a link to them.

Where the College has been asked for disclosure of datasets, those datasets will then be published regularly, as required by FOIA.

Unless otherwise stated, all the College's published information is (a) available free of charge and (b) usable under the terms of the Open Government Licence. Information which is not published by the College in accordance with this scheme can be requested in accordance with FOIA.

The College is also required under EIR to make certain and more limited environmental information available proactively. The College should follow the code of practice on the discharge of the obligations of public authorities under EIR which sets out when public authorities should make information available proactively.

The DC will determine what if any information is published under FOIA (as part of the Publication Scheme) or under EIR.

## 1.5 Receiving requests

Requests for information can take many forms. FOIA requests must be in writing (as set out above), including email, fax and by social media, identify the sender (unless it is clearly a made-up name), provide an address for correspondence and describe the information requested. The EIR do not specify how a valid request must be made and so any request for environmental information should be assumed to be a valid EIR request but you will still need to have details so that you can reply to the request and enough information to understand and action the request.

A request may fall under the provisions of FOIA or EIR as applicable regardless of its wording and whether or not it mentions 'freedom of information' or the 'environmental information regulations'. Anyone indicating that they are making a verbal FOIA request should be advised to put it in writing. All requests for information which may need to be recorded as FOIA or EIR requests should be forwarded without delay to the DC.

The applicant does not have to say why they are making a FOIA or EIR request or what they propose to do with the information, and these questions should not be asked. In addition, the requestor does not need to ask for a specific document, although they should give a description of the information they are asking for and there are exemptions and exceptions which may apply if the College is unable to deal with a request because it is too broad, unclear or unreasonable.

The College is required to offer advice and assistance to the requestor and therefore if an FOIA or EIR request is unclear the College will contact the requestor as soon as possible in order to gain the clarification needed to deal with the request.

## 1.6 Handling requests

All requests will be logged by the DC. As above, if you receive a request for information or its re-use you should provide this to the DC immediately. The DC will calculate the due date according to the time limit laid down (20 working days after the day of receipt). Saturdays, Sundays and public holidays and periods during which the College is closed (see below) are excluded from the calculation, but no allowance can be made for other days on which the College is closed or when staff are on leave.

Unless a response is being provided immediately, the request will be acknowledged and the applicant informed of the due date. If another member of staff is to supply the information requested, the DC will advise them and check that they will be able to meet the required timescale.

Should the period for responding include days when the College is closed for school holidays or inset days, then the deadline will be calculated to exclude any closure days (unless the College closure period would make the deadline longer than 60 working days, in which case the College will respond in 60 working days).

In certain circumstances where a request for environmental information is complex and/or voluminous, the College may be allowed extra time (up to an additional 20 working days) under EIR for responding.

If the public interest test must be considered under FOIA, extra time for carrying out this assessment may be claimed if needed (provided the College has already within the initial 20 working day period explained to the requester which exemptions apply and why, and what additional reasonable time it needs to complete any remaining relevant public interest test decision making). The DC will inform the requestor of any extension to the deadline and reason why within the standard time limit for compliance.

The applicant may only be charged a fee in limited circumstances and only after the College has sent the applicant a Fees Notice (see 1.10 below). The vast majority of FOIA and EIR requests are dealt with by the College free of charge.

The College is, in most circumstances, required to state whether it holds the information, and disclose the information itself, subject to applicable exceptions or exemptions. However, it can refuse to disclose requested information if:

- it does not hold that information
- an exemption or exception applies (see 1.7 below)
- the cost for responding to a FOIA request exceeds a limit provided for in law or an EIR request is manifestly unreasonable (see 1.9 below), or
- the request is vexatious or repeated (see 1.8 below).

If the request asks for information which is not held, the reply will usually say so. However there may be circumstances where it will be appropriate neither to confirm nor deny that the requested information is held. For example, if information has been supplied to the College in confidence and is therefore exempt from disclosure, it may be an actionable breach of confidence to admit that it had been received.

If the College refuses to say whether or not it holds requested information, or to disclose information which it holds and which has been requested, it must issue a formal refusal notice within the statutory timescales (explained above).

Applicants have the right to appeal against any such refusal and can also object if they believe the College has not properly answered their request (see 1.12 below). Any complaint should be treated as a request for internal review which must be notified to the DC who will arrange for an internal review in accordance with the relevant legal regime, codes of practice and guidance. Once the internal review process is completed, the requester has a right to complain to the ICO.

Appeals and objections can be logged with the ICO, who will investigate the circumstances and may require the College to take specified actions, including ordering disclosure of requested information. ICO decisions are normally published by the ICO in a decision notice on the ICO website. It is important the College is compliant or its reputation may be damaged.

You may be guilty of a criminal offence if you deliberately or recklessly alter, hide, delete or destroy requested information to avoid a FOIA or EIR request.

## 1.7 Exemptions and exceptions

FOIA provides for over 20 exemptions and EIR also has many exceptions, although there are some differences in the relevant grounds for refusal under FOIA and EIR. For example, information may be exempt from disclosure under FOIA if it is already reasonably accessible to the applicant by other means, if disclosure would leave the College open to an actionable breach of confidence or if it is personal data and its disclosure would be contrary to the data protection principles under UK GDPR. A full list of exemptions under FOIA and for the exceptions under EIR are available on the ICO website.

Some FOIA exemptions (and all EIR exceptions save in some cases for personal data) are ‘qualified’ by the need to undertake a public interest test which the DC must carry out in accordance with ICO guidance.

The use of an exemption or exception or other ground for refusal must be agreed by the DC. If one or more applies, the applicant will be informed as soon as possible (and within the statutory timescales) what is being refused and why, together with an explanation.

For purposes of a section 36 FOIA exemption, the Principal & CEO, who has been authorised as the Qualified Person, will need to provide an opinion confirming that they reasonably believe the exemption is engaged and the reasons why.

## 1.8 Vexatious or repeated requests

A FOIA request can be treated as vexatious where it would impose a significant burden on the College in terms of expense or distraction, and:

- clearly does not have any serious purpose or value
- is designed to cause disruption or annoyance
- has the effect or harassing the College, or

- can otherwise fairly be regarded as obsessive or manifestly unreasonable.

A request for environmental information will be refused where it is 'manifestly unreasonable' on the basis that an equivalent request would be found 'vexatious' if it was subject to FOIA.

The College is not obliged to comply with similar requests from one individual unless there is a reasonable interval between them.

Vexatious or repeated requests may be refused and in such cases the College will still issue a refusal notice to the requestor, unless this has been issued previously to the same requestor for other vexatious requests and they have been warned that the College will not provide explanations for refusal in future. The DC will make this determination.

A record will be maintained so that any refusal can be justified to the ICO if a complaint is made.

In considering whether a request is vexatious the College will look at the context in which the request is made to determine whether the request has any value or serious purpose as its objective as against the detrimental impact it could have on the College, its employees or students.

## 1.9 Limit on work required

A FOIA request may be refused if it will take more than 18 hours to determine whether the information is held, and to locate, retrieve and extract it. Time needed to format or present the information cannot be counted, nor any time in deciding whether any exemptions apply or seeking legal advice. That limit comes from the regulations which prescribe a cost of £450 and a rate of £25 per hour.

If it appears that for a particular request the limit will be exceeded, the calculation must be recorded and a written refusal notice [may be] sent to the requestor. The DC will make this determination. As the College is required to advise and assist applicants, the request must not be refused until the applicant has had the opportunity to adjust the request to bring it within the limit. This will then be dealt with as a new request.

If the requester has sent a number of requests (particularly where on the same subject matter) in a short time period of (60 days or less) then the time taken in respect of each request can be calculated collectively.

There is no equivalent limit under EIR to the “appropriate limit” provided under FOIA, but requests may be refused where the costs of dealing with them would be “manifestly unreasonable”. The EIR do not define a ‘reasonable’ amount of money or time that a public authority should spend on a request, although the costs limit under FOIA may be a useful starting point for working out if a request can be treated as manifestly unreasonable.

## 1.10 Fees

In some circumstances, and where it is reasonable to do so, the College may charge fees as permitted under FOIA, or EIR, as relevant. The DC will make this determination. Details of the rates used in the calculation are included in the Publication Scheme and only these rates may be used.

Under FOIA, only disbursements, i.e. expenses incurred in providing the information can be charged, such as photocopying and postage, except where the time estimated for locating and extracting the information exceeds 18 hours (see 1.9 above). Where answering a FOIA request exceeds the cost limit, the College can offer to supply the information and recover its costs, rather than refusing the request. In this case, a charge may be made to cover the cost of doing that calculation, the cost of communication (including photocopying and postage) and the staff time spent on communicating the information.

EIR permits reasonable charges for the actual costs of staff time in locating information and putting the information in an appropriate format for disclosure, in addition to disbursements. This would be unusual for the College to do and the DC will make this determination. The College will only make charges in line with the schedule of charges in the Publication Scheme. We will never charge requestors for access to public registers or lists of environmental information.

Where a fee is to be charged under FOIA or EIR, the College will issue a Fees Notice. The requested information will then only be supplied after payment has been received.

When a Fees Notice is issued the 20 working day period is placed ‘on hold’ from the date of its issue, and taken ‘off hold’ when the fee is received. If no fee is received within three months of the Fees Notice the request will be refused.

## 1.10 Sending the response

The College will respond to the applicant within the set timescale, giving the information held, subject to applicable exemptions or exceptions. If requested information is not held the response will give a brief explanation and if possible say where the applicant may be able to obtain the information. The set timescale allies to all types of response.

When responding to a FOIA or EIR request, the College will inform the applicant of their right to appeal to the ICO if they are dissatisfied with the response, and provide the ICO’s contact details. If the request was made using social media and the length of the reply makes it impossible to respond through the same media, the applicant must be asked to either supply an email address or to collect the response by arrangement from the College.

## 1.11 Complaints

If an applicant is dissatisfied with the response they have received from the College they may appeal the decision and request an internal review of this decision in order for the College to reconsider its response. They must do so within 40 working days of receiving the refusal letter under FOIA or EIR.

The College will follow a separate procedure for conducting an internal review, following the ICO's guidelines. The College will usually notify the requestor of the outcome of the internal review within 20 working days of receiving the request for internal review, but in exceptional circumstances, this may be extended to up to 40 working days and we will inform the requester of this.

This process is separate from the College's standard complaints procedures. Where an appeal or objection is logged with the ICO, the ICO will investigate the circumstances and may require the College to disclose the information.

## 1.12 Register

The College maintains a full register of requests and complaints as well as the outcomes and timescales in responding to such requests, in order to ensure compliance with FOIA and EIR and so that it can respond effectively to any complaints made directly to the ICO. The DC maintains this register for the College. The ICO may ask for performance figures and may monitor organisations whose performance is below an acceptable level.