INFORMATION POLICY
Approved by: Audit Committee
Date approved: 26 November 2020
Strategy/Policy Responsibility: *Vice Principal Finance & Resources*
Review date: November 2022

1 Introduction

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) came into force on 25 May 2018. This policy sets out Croydon College's approach to the information it holds and processes. 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.

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.

As a Public Authority, the College is obliged to comply with the Freedom of Information ('FOI') Act and the Environmental Information Regulations (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 and FOI legislation, and also provides guidance to organisations.

2 Data Protection

2.1 Introduction

Croydon College is a Controller within the meaning of the GDPR and the DPA. The College is committed to preserving the privacy of students, employees and others about whom it holds personal data, and to complying with the 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 GDPR to have a Data Protection Officer (DPO). 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 complying with the College's policy and procedures, and raising any concerns about data privacy.

Any breach or suspected breach of data protection compliance must be immediately reported to the Line Manager, Tutor or Data Protection Officer. The College can be penalised if it fails to notify breaches to the ICO within strict timescales. Incidents to be reported include the destruction, loss or alteration of personal data (whether accidental or otherwise), and any disclosure of, or access to personal data which has not been authorised. The Data Protection Officer is responsible for making any required report to the ICO.

All members of staff are required to complete 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 procedures as necessary if a person is found to have deliberately or negligently 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 from which a living individual can be identified, either by itself or when combined with other information.

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.

A **Data Subject** is the living person who the personal data is about.

The **Controller** is Croydon College.

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

The **Data Protection Officer** (DPO) 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.

A **Subject Access Request** is when an individual asks for a copy of the personal data which the College is holding about them and details about the processing.

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 in order to obtain any 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

GDPR requires compliance with six data protection principles. These state that personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals
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 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. The guidance on the ICO's web site lists what information must be provided. The College will do that in different ways as follows:

- in a Privacy Statement on the College's web site – this will give general information about processing, security, the DPO and individual's rights
- in Privacy Notices on individual forms 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.

2.7 Right of access

Individuals ("Data Subjects") have the right to access 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. 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 unless 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; for staff and students the personal data already held by the College will be used. The College will supply the information requested 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. The College will 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 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 is not inappropriately disclosed and that the College meets the strict response timescales laid down. Records will be kept in line with the ICO's guidance.

2.8 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, 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 data. Any request from an individual which is exercising any of these rights must be referred without delay to the DPO.

2.9 Security requirements

Measures that everyone is required to take to minimise the risk of unauthorised disclosure of personal data are contained in the 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 are:

- being aware of who else might be able to read information from computer screens
- 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.

2.10 Disclosure of personal data

Personal data is not to be disclosed to anyone except in the following circumstances:

(a) where a data sharing agreement is in place (and in line with that agreement)

(b) to individuals making a Subject Access Request (see 2.7above), or

(c) as required by law and/or on an ad-hoc basis where the risks and circumstances have been properly considered

Before disclosing personal data under (c) it is necessary to:

- ensure there is a lawful basis 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 where necessary, security measures for sending the data are adequate.

If you receive a request for personal data, whether that be a member of staff or a student past or present please contact [INSERT] prior to making any disclosures to any third party.

The data subject is to be advised of the disclosure if they are not already aware of it. However, that does not apply 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.

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.

2.11 Working from home or remotely

If a member of staff needs to work from home or outside the College, additional measures are needed to minimise the risk of loss or disclosure of personal data. Details are included in the Information Security Policy and include:

- use of the secure remote access facilities provided
- requirements and guidance for minimising risk of loss and access by anyone unauthorised (including family and friends), and
- 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 copied to a device for remote use must be securely deleted from that device as soon as the work is complete. The DPO should be consulted if further advice is needed.

2.12 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. 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 GDPR. Failure by any member of staff to notify the DPO of an additional source of personal data could therefore result in disciplinary action.

2.13 New processes and changes, and automated decisions

The College is required to assess the impact on individuals' privacy of all new or changed processes. The process is called a Data Protection Impact Assessment (DPIA) and should be conducted as early as possible when the changes are being designed. 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) it will be necessary to give those individuals additional information about how the decisions are made.

2.14 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.

2.15 Marketing

Use of personal data for marketing activities must comply with the requirements of the Privacy and Electronic Communications Regulations 2003 (PECR) as well as the GDPR.

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 the Public Records Act 1958, the Re-Use of Public Sector Information Regulations 2005, s46 FOIA, 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, which facilitates College business and activities and which is retained for a set period. 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. Directors and Heads of Department, 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 legislative 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 2.12 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/

Information Policy

Appendix 1: Freedom of Information

1.1 Introduction

The Freedom of Information (FOI) Act 2000 (the FOI Act) gives the public a general right of access to all recorded information held by public authorities in England, Wales and Northern Ireland, including Croydon College. The FOI Act 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.

All information which the college holds is covered by the FOI Act, regardless of its format. This includes information in paper files, electronic documents, emails, databases and audio or video material. The FOI Act requires disclosure of information in two main ways: (a) by proactive publication through a Publication Scheme, on the College web site, and (b) to any person in response to valid requests. Some information will, however be exempt from disclosure (see 1.7 below).

The College is bound by the FOI Act not only to supply information when required to do so, but to advise and assist 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 may deal with the College are made aware of the College's duties under FOIA and the potential that information may be released under FOI Act unless an exemption applies.

1.2 Responsibilities

The Governing Body is legally responsible for compliance with FOI legislation. Day to day management of FOI is the responsibility of a Data Co-ordinator (DC), which is the Director of IT & Estates. The DC is responsible for collating the requested FOI information, determining any exemptions, issuing responses and refusals and keeping records of the requests.

All College staff are responsible when required to provide requested information or a reason for exemption. 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 Environmental Information Regulations 2004 (EIR) give a right of access to environmental information held by public authorities. The legislation is similar to the FOI Act's regime but with certain differences. The ICO provides guidance on the definition of environmental information and how the EIR applies. Requests under the EIR will be handled in the same way as requests under the FOI Act, and the DC will apply any differences in handling which are required.

The main differences between the application of FOI and the EIR is in relation to the exemptions which can be applied to environmental information, and the time limits for compliance. In addition, EIR requests can be made verbally as well as in writing, whereas FOI 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 the FOI Act 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 web site 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 the FOI Act.

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 the FOI Act.

1.5 Receiving requests

Requests for information can take many forms, but must be in writing, including email, fax and by social media. A request may fall under the provisions of the FOI Act regardless of its wording and whether or not it mentions 'freedom of information'. Anyone indicating that they are making a verbal FOI request should be advised to put it in writing. All requests for information which may need to be recorded as FOI requests should be forwarded without delay to the DC.

A request will be regarded as validly made if it states the name of the applicant (unless it is clearly a made-up name) and an address for reply (which may be an email address) and describes the information requested. The applicant does not have to say why they are making the 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, the FOI Act covers requests for information and this may require the College to collect the relevant information to answer the FOI query posed by the Requestor.

The College is required to offer advice and assistance to the requestor and therefore if an FOI 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. If you receive a request for information 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 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.

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 majority of 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. However, it can refuse to disclose information if:

- it does not hold that information
- an exemption applies (see 1.7 below)
- the cost exceeds a limit provided for in law (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 information is held. For example, if information has been supplied to the College in confidence and is therefore exempt from disclosure, it may be a breach of confidence to admit that it had been received.

If the College refuses to disclose information which has been requested it must issue a formal refusal notice (see 1.11 below).

Applicants have the right to appeal against a refusal to issue information and can also object if they believe the College has not properly answered their request (see 1.12 below). Appeals and objections can be logged with the ICO, who will investigate the circumstances and may require disclosure of the information.

1.7 Exemptions

The FOI Act provides for over 20 exemptions. EIR has similar exemptions, although there are some differences. Information will be exempt from disclosure if it is already accessible to the applicant by other means, if it is personal data, if disclosure would leave the College open to an actionable breach of confidence or if releasing the information would be contrary to the GDPR or the Data Protection Act 2018.

Information *may* be exempt from disclosure if it is intended for future publication, is commercially sensitive, confidential, contains personal data, is held for the purposes of an investigation or if its disclosure would inhibit the investigation of a crime. Before using these ‘qualified’ exemptions the DC will need to carry out a public interest test in accordance with ICO guidance.

The use of an exemption must be agreed by the DC. If one applies, the applicant will be informed as soon as possible that the information cannot be provided together with an explanation. When considering a qualified exemption the 20-day period may be extended provided an interim response is issued within the timescale together with an estimate of when the final response is expected.

1.8 Vexatious or repeated requests

A 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.

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 will be refused but no further explanation will be provided. 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. A record will be maintained so that the 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.

1.9 Limit on work required

A request may be refused if it will take more than 18 hours to determine whether the information is held, locate 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 sent to the requestor. 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.

1.10 Fees

The College will charge fees as permitted under the FOI Act where the fee amounts to at least £25. Details of the rates used in the calculation are included in the Publication Scheme.

Only expenses incurred in providing the information can be charged, such as photocopying and postage. However, where the time estimated for locating and extracting the information exceeds 18 hours, 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.

Where a fee is to be charged 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-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.

1.11 Sending the response

The College will aim to respond to the applicant within the set timescale, giving the information held. 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, 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.

1.12 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. The College will follow a separate procedure for conducting an internal review, following the ICO's guidelines. The College will notify the requestor of the outcome of the internal review no later than 20 working days after receiving the request for internal review. 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.

1.13 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 the FOI Act, 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.