Title:	**Rights of Individuals Procedure**
Reviewed by:	**Data Protection Officer**
Date of Review:	**June 2019**
Approved by:	**SMT**
Date of next review:	**June 2021**
Associated documents/policies:	• *Rights of Individuals Policy* • *Data Protection Policy* • *Retention of Records Policy* • *Personal Data Breach Policy* • *Information Security Policy* • *Confidentiality Policy*

TABLE OF CONTENTS

1. OVERVIEW

The College's reputation and future growth are dependent on the way the College manages and protects Personal Data. All individuals have rights over their Personal Data. This Rights of Individuals Procedure must be read in conjunction with the College's Rights of Individuals Policy. It explains the process the College follows to comply with its legal obligations to allow individuals to exercise their rights over their Personal Data which are detailed in the Rights of Individuals Policy.

This Policy does not form part of any College Personnel's contract of employment and the College reserves the right to change this Policy at any time. All College Personnel are obliged to comply with this Policy at all times.

2. ABOUT THIS PROCEDURE

This Procedure explains the process the College has in place to ensure that the College complies with its legal obligations to allow individuals to exercise their rights over their Personal Data. The College has a corresponding Rights of Individuals Policy that sets out what those rights are and explains College Personnel's' obligations in relation to ensuring that the College meets its obligations in this area.

3. SCOPE

This Procedure applies to all College Personnel who collect and/or use Personal Data relating to individuals.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

4. DEFINITIONS

4.1. **College** – Bath College.

4.2. **College Personnel** – Any College employee or contractor who has been authorised to access any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.

4.3. **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.

4.4. **Data Protection Officer** – The Data Protection Officer is currently the Director of Human Resources & Organisational Development, and can be contacted at: telephone 01225 328765 or e-mail dataprotection@bathcollege.ac.uk.

4.5. **ICO** – the Information Commissioner's Office, the UK's data protection regulator.

4.6. **System Owner** – The member of college personnel responsible for the specific College Information System e.g. the Head if Information Systems for the Student Records System or the Head of Finance for the Finance system.

4.7. **Personal Data** – any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier.

4.8. **Special Categories of Personal Data -** Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their

physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record.

5. HOW DO WE ALLOW INDIVIDUALS TO EXERCISE THEIR RIGHTS UNDER DATA PROTECTION LAWS?

5.1. **Right of access (subject access requests) – see Appendix 1 flowchart**

5.1.1. Subject Access Requests (SARs) can be made by:

- The Data Subject
- A person lawfully acting on their behalf:
  - Their lawyer (with a consent form)
  - Person with parental responsibility for under 13s
  - Person with authority to manage the affairs of an incapacitated adult

5.1.2. The College should be provided with sufficient information to validate the identity of the person making the request in order to ensure information is only given to the person who is entitled to it. If the requestor is not the data subject, written confirmation that the requestor is authorised to act on behalf of the data subject is required;

5.1.3. the College is not able to charge a fee for responding to SARs unless a second or subsequent copy of the Personal Data is requested (in which case the College can charge its administrative costs) or the request is unfounded or excessive (see paragraph 5.8 below);

5.1.4. Where a large quantity of information is processed about an individual, the College can ask the individual to specify the information the request relates to;

5.1.5. Searches for data need to be reasonable and proportionate. Dis proportionate effort is not restricted to supply of copies, but includes difficulties which occur in the process of complying with the request. The threshold of proportionality is high. The person dealing with the request must be able to provide evidence to show what has been done to identify personal data and the relevant plan of action;

5.1.6. If a member of the College Personnel receives a request from an individual to access or to receive a copy of their Personal Data, the following procedure will be followed:

5.1.6.1. the College Personnel must forward or report the request to the Data Protection Officer as soon as they receive it. A request from an individual does not have to be in a particular format, for example it does not have to be in writing. If the request is made verbally (e.g. it is taken over the telephone) best practice is that the College asks the individual to confirm the request in writing;

5.1.6.2. the Data Protection Officer will diarise the date the request was received, the deadline to respond and follow up, as appropriate, all College Personnel involved in dealing with the request, in order to track its progress;

5.1.6.3. As soon as possible after receipt, the Data Protection Officer will decide whether any further information is needed from the individual to clarify the identity of the individual or to understand the request and will ask the individual for any further information that is needed;

5.1.6.4. if further information is required, no action will be taken until the further information has been received from the individual;

5.1.6.5. once the further information has been received and/or the College is satisfied that it knows what has been asked for, the College will begin locating the individual's Personal Data;

5.1.6.6. depending on who the individual is, this may involve locating staff files, student files, information on parents, notes, minutes, correspondence and other relevant documents containing Personal Data either on the College's information systems, or in the College's structured paper filing systems. The Data Protection Officer will let College Personnel know what information has been requested;

5.1.6.7. once the College has located all the Personal Data of the individual, the Data Protection Officer will review it, redact as appropriate, and decide whether any of the Personal Data does not need to be disclosed as there are exemptions which may apply;

5.1.6.8. once it has been decided what the College is going to provide to the individual, the College will respond providing copies of the Personal Data, which, if the request is made electronically, shall be provided in a commonly used electronic form; and

5.1.6.9. In principle the College will not normally disclose the following types of information in response to a Data Subject Access Request:

- Information about other people – a SAR may cover information which relates to an individual or individuals other than the data subject. Access to such data will not be granted, unless the individuals consent to the disclosure of their data;
- Repeat requests – where a similar or identical request in relation to the same data subject has previously been complied with within a reasonable time period, and where there is no significant change in personal data held in relation to that data subject, any further request made within a six-month period of the original request will be considered a repeat request, and the College will not normally provide a further copy of the same data;
- Publicly available data – the College is not required to provide copies of documents which are already in the public domain;
- Opinions given in confidence or protected by copyright law – the College does not have to disclose personal data held in relation to a data subject that is in the form of an opinion given in confidence or protected by copyright law;
- Privileged documents – any privileged information held by the College need not be disclosed in response to a SAR. In general,

privileged information includes any document which is confidential (e.g. a direct communication between a client and their lawyer) and is created for the purpose of obtaining or giving legal advice;

- EHCPs are the data property of the issuing authority and any request for an EHCP should be directed to the relevant local authority.

5.1.6.10. Where a decision is made to refuse to respond to a request, an explanation of the reason must be given to the individual, informing them of their right to complain to the Information Commissioners Office (ICO). The individual should be informed of the decision at the latest within one month of receipt of the request.

5.2. **Right to rectification**

5.2.1. Personal data should be 'accurate and, where necessary, kept up to date: every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay';

5.2.2. If a member of the College Personnel receives a request from an individual to correct or complete their Personal Data, the following procedure will be followed:

5.2.2.1. the College Personnel must forward or report the request to the Data Protection Officer as soon as they receive it;

5.2.2.2. the Data Protection Officer will diarise the date the request was received, the deadline to respond, and follow up all College Personnel involved in dealing with the request in order to track its progress;

5.2.2.3. the College will then locate the Personal Data concerned and verify whether it is incorrect or incomplete and will correct it or complete it as soon as possible;

5.2.2.4. the College will ascertain whether the College has disclosed the incorrect or incomplete Personal Data to any third parties and, if so, the College will contact those third parties as soon as possible to tell them to correct the Personal Data;

5.2.2.5. the Data Protection Officer will decide whether the College needs to keep a copy of the original Personal Data for evidence reasons or otherwise;

5.2.2.6. the College will confirm to the individual in writing within one month of the date of their request that the College has complied with the request; and

5.2.2.7. If the College decides not to take action in response to a request for rectification, an explanation as to why must be given to the individual, informing them of their right to complain to the ICO.

5.3. **Right to erasure (right to be forgotten)**

5.3.1. If a member of the College Personnel receives a request from an individual to delete their Personal Data, the following procedure will be followed:

5.3.1.1. the College Personnel must forward or report the request to the Data Protection Officer as soon as they receive it;

5.3.1.2. the Data Protection Officer will diarise the date the request was received, the deadline to respond, and follow up all College Personnel involved in dealing with the request in order to track its progress;

5.3.1.3. the Data Protection Officer will reach a decision as to whether the right to be forgotten applies;

5.3.1.4. if the right to be forgotten does apply, the Data Protection Officer will decide whether the College is required to keep any parts of the Personal Data for evidence reasons and, if so, this Personal Data will be excluded from the request;

5.3.1.5. the College will then securely delete all the Personal Data about that individual that the College has which is not excluded. This will include securely shredding all hard copy documents and ensuring that computer records are securely deleted from the College's information systems in line with the processes detailed in the College's Data Retention Policy;

5.3.1.6. the College will ascertain whether it has disclosed the deleted Personal Data to any third parties and, if so, the College will contact those third parties as soon as possible to tell them to delete the Personal Data; and

5.3.1.7. the College will confirm to the individual in writing within one month of the date of their request that the College has complied with the request.

5.4. **Right to restrict processing**

5.4.1. If a member of the College Personnel receives a request from an individual to restrict the College's use of their Personal Data, the following procedure will be followed:

5.4.1.1. the College Personnel must forward or report the request to the Data Protection Officer as soon as they receive it;

5.4.1.2. the Data Protection Officer will diarise the date the request was received, the deadline to respond, and follow up all College Personnel involved in dealing with the request in order to track its progress;

5.4.1.3. the Data Protection Officer will reach a decision as to whether the right to restrict processing applies;

5.4.1.4. if the right to restrict processing does apply, the College will action the request as soon as possible and ensure that the

College no longer uses the individual's Personal Data in the way they have objected to. This may include moving documents to folders where they can no longer be accessed, removing details from files and locking paper files away;

5.4.1.5. the College will ascertain whether the College has disclosed the Personal Data to any third parties and, if so, the College will contact those third parties as soon as possible to tell them to stop using the Personal Data in the restricted way; and

5.4.1.6. the College will confirm to the individual in writing within one month of the date of their request that the College has complied with the request.

5.5. **Right to data portability**

5.5.1. If a member of the College Personnel receives a request from an individual to provide a copy of their Personal Data in a structured, commonly-used and machine-readable format, the following procedure will be followed:

5.5.1.1. the College Personnel must forward or report the request to the Data Protection Officer as soon as they receive it;

5.5.1.2. the Data Protection Officer will diarise the date the request was received, the deadline to respond, and follow up all College Personnel involved in dealing with the request in order to track its progress;

5.5.1.3. the Data Protection Officer will reach a decision as to whether the right to data portability applies and to which subset of the individual's Personal Data it applies; and

5.5.1.4. if the right to data portability does apply, the College will action the request as soon as possible. This will include creating an electronic copy of the individual's Personal Data which can be transferred to another organisation if the individual asks the College to.

5.6. **Right to object**

5.6.1. If a member of the College Personnel receives an objection from an individual to the College's processing of their Personal Data, the following procedure will be followed:

5.6.1.1. the College Personnel must forward or report the request to the Data Protection Officer as soon as they receive it;

5.6.1.2. the Data Protection Officer will diarise the date the request was received, the deadline to respond, and follow up all College Personnel involved in dealing with the request in order to track its progress;

5.6.1.3. the Data Protection Officer will reach a decision as to whether the right to object applies;

5.6.1.4. if the right to object does apply, the College will action the request as soon as possible. This may include suppressing the individual from the College's direct marketing lists, or stopping the processing of Personal Data that has been objected to; and

5.6.1.5. the College will write to the individual within one month of the date of their request to tell them either that the College has complied with, or intends to comply with, their request or that the College has not complied and the reasons why the College has not complied.

5.7. **Rights in relation to automated decision making**

5.7.1. If a member of the College Personnel receives an objection from an individual to an automated decision that the College has made about the individual which produces legal effects concerning them or similarly significantly affects them, the following procedure will be followed:

5.7.1.1. the College Personnel must forward or report the request to the Data Protection Officer as soon as they receive it;

5.7.1.2. the Data Protection Officer will diarise the date the request was received, the deadline to respond, and follow up all College Personnel involved in dealing with the request in order to track its progress;

5.7.1.3. the Data Protection Officer will reach a decision as to whether the right to intervene in the automated decision-making applies;

5.7.1.4. if the right to intervene does apply, the College will action the request as soon as possible. This will involve reviewing the automated decision-making process, reviewing the decision that was made, having a College Personnel consider whether the decision needs to be retaken and allowing the individual to give their view on the decision; and

5.7.1.5. the College will write to the individual within one month of the date of their request to tell them what the outcome of the College's review is.

Automated decision making happens where the College makes a decision about an individual solely by automated means without any human involvement; and

Profiling happens where the College automatically uses Personal Data to evaluate certain things about an individual.

5.8. **Are there any requests the College does not have to respond to?**

5.8.1. If the request the College receives from an individual is unfounded or excessive then the College may either:

5.8.1.1. refuse to action the request; or

5.8.1.2. charge a reasonable fee taking into consideration the College's administrative costs of providing the information or taking the action requested.

5.8.2. Any decisions in relation to not actioning the request or charging a fee shall be made by the Data Protection Officer.

5.9. **Response Times**

5.9.1. All requests set out above must be responded to within a month unless the request is complex in which case the period may be extended up to a further two months. Any decision in relation to whether the request is complex is to be made by the Data Protection Officer who shall inform the individual making the request of the extension. Any notification of the extension to the individual shall be made within the initial one-month period and shall give reasons for the delay.

5.9.2. If the College is not going to action the request made by an individual, the Data Protection Officer shall communicate this to them within month of receipt of the request. The communication shall include details of the College's reasons for not actioning the request and the ability of the individual to make a complaint to the ICO.

5.10. **Legal Advice**

Specialist external legal advice may be taken on the above, but this shall be the decision of the Data Protection Officer.

6. MONITORING & INTERNAL REPORTING

6.1. Information Compliance, including requests by individuals regarding their data will be reported to the SMT meetings on a quarterly basis.

6.2. Information Compliance reports will be presented to each Audit Committee meeting, outlining requests or nil returns.

Appendix 1

Subject Access Flowchart

(assuming no need for additional time to complete request)