

RIGHTS OF INDIVIDUALS TO ACCESS PERSONAL DATA PROCEDURE

Contents

1. OVERVIEW	1
2. ABOUT THIS PROCEDURE	1
3. SCOPE.....	1
4. DEFINITIONS.....	2
5. HOW DO WE ALLOW INDIVIDUALS TO EXERCISE THEIR RIGHTS UNDER DATA PROTECTION LAWS?	3
5.1. Right of access (subject access requests)	3
5.2. Right to rectification	4
5.3. Right to erasure (right to be forgotten).....	5
5.4. Right to restrict processing	6
5.5. Right to data portability	7
5.6. Right to object.....	8
5.7. Rights in relation to automated decision making/profiling.....	8
5.8. Are there any requests the College does not have to respond to?.....	10
5.9. Response Times.....	10
5.10. Legal Advice	11

RIGHTS OF INDIVIDUALS TO ACCESS PERSONAL DATA PROCEDURE

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.

College Employees will be directed to this Procedure when they start, as part of their induction, and may receive periodic revisions of this Procedure. This Procedure does not form part of the contract of employment and the College reserves the right to change it at any time. All College Employees are obliged to comply with this Procedure at all times.

2. ABOUT THIS PROCEDURE

The College's General Data Protection Policy is the College's fundamental policy which sets out the types of Personal Data that the College may be required to handle, as well as the College's legal purposes for doing so, and it sets out how the College complies with its obligations under Data Protection Laws.

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 Employees' obligations in relation to ensuring that the College meets its obligations in this area.

3. SCOPE

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

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

RIGHTS OF INDIVIDUALS TO ACCESS PERSONAL DATA PROCEDURE

4. DEFINITIONS

- 4.1. **College** – Shrewsbury College
- 4.2. **College Employees** – 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 UK General Data Protection Regulation and all applicable laws relating to the collection and use of Personal Data and privacy , including the Data Protection Act 2018 as amended from time to time, and any applicable codes of practice issued by the Information Commissioner's Office (ICO).
- 4.4. **Data Protection Officer** – The Data Protection Officer is Mark Brown, Vice Principal – Quality, Apprenticeships, and Information, and can be contacted at: 01743 653000, dpo@shrewsbury.ac.uk .
- 4.5. **ICO** – the Information Commissioner's Office, the UK's data protection regulator.
- 4.6. **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.
- 4.7. **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 and sexual life or sexual orientation.
- 4.8. **Criminal offence data** – Personal data relating to criminal convictions and offences or related security measures, which is processed in accordance with Data Protection Laws and subject to additional safeguards.

RIGHTS OF INDIVIDUALS TO ACCESS PERSONAL DATA PROCEDURE

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

5.1. Right of access (subject access requests)

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

- 5.1.1.1. the College Employees must forward or report the request to the Data Protection Officer and Director of Technical Services 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 not made in writing (e.g. it is taken over the telephone) best practice is that the College asks the individual to confirm in writing so it can ensure it is complying correctly with the request. If they do not wish to do this, then please confirm the request in writing and ask them to indicate if there are any inaccuracies. Please note that the College can no longer charge a fee for responding to these requests 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);
- 5.1.1.2. the Data Protection Officer will log the date the request was received, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances as set out in paragraph 5.9), and send weekly chasers to all College Employees involved in dealing with the request in order to track its progress;
- 5.1.1.3. within 2 working days of 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 as soon as possible;
- 5.1.1.4. if, for any reason, the Data Protection Officer is not available to consider whether further information is available, the Director of Technical Services will decide;
- 5.1.1.5. if further information is required, no action will be taken until the further information has been received from the individual;

RIGHTS OF INDIVIDUALS TO ACCESS PERSONAL DATA PROCEDURE

- 5.1.1.6. 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;
- 5.1.1.7. depending on who the individual is, the College will identify and retrieve personal data using reasonable and proportionate searches, based on the scope of the request, the systems used and the likelihood that relevant data is held. The Data Protection Officer will let College Employees know what searches they need to carry out;
- 5.1.1.8. once the College has located the Personal Data of the individual, the Data Protection Officer will review it and decide whether any of the Personal Data does not need to be disclosed as there are exemptions which may apply;
- 5.1.1.9. once the College has 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
- 5.1.1.10. if the College deems the request to be complex, it can apply an additional two months extension. In this circumstance the College will ensure that it has contacted the individual within the initial one month period to explain the basis for the decision and provide any elements of the request it has already completed.
- 5.1.1.11. throughout a Right of Access Request the Data Protection Officer may be supported by the Director of Technical Services and/or the Quality Co-ordinator.

5.2. Right to rectification

- 5.2.1. If a member of the College Employees receives a request from an individual to correct their Personal Data, the following procedure will be followed:
 - 5.2.1.1. the College Employees must forward or report the request to the Data Protection Officer and MIS Manager as soon as they receive it;
 - 5.2.1.2. the Data Protection Officer will log the date the request was received, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances as set out in

RIGHTS OF INDIVIDUALS TO ACCESS PERSONAL DATA PROCEDURE

paragraph 5.9), and send weekly chasers to all College Employees involved in dealing with the request in order to track its progress;

- 5.2.1.3. 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;
- 5.2.1.4. the College will ascertain whether the College has disclosed the incorrect 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;
- 5.2.1.5. the Data Protection Officer will decide whether the College needs to keep a copy of the original Personal Data for evidence reasons or otherwise; and
- 5.2.1.6. 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;
- 5.2.1.7. throughout a Right of Rectification Request the Data Protection Officer may be supported by the MIS Manager and/or the Quality Co-ordinator.

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

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

- 5.3.1.1. the College Employees must forward or report the request to the Data Protection Officer and the MIS Manager as soon as they receive it;
- 5.3.1.2. the Data Protection Officer will log the date the request was received, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances as set out in paragraph 5.9), and send weekly chasers to all College Employees 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;

RIGHTS OF INDIVIDUALS TO ACCESS PERSONAL DATA PROCEDURE

- 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;
- 5.3.1.8. throughout a Right of Erasure Request the Data Protection Officer may be supported by the MIS Manager and/or the Quality Co-ordinator.

5.4. Right to restrict processing

- 5.4.1. If a member of the College Employees 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 Employees must forward or report the request to the Data Protection Officer, MIS Manager and Director of Technical Services as soon as they receive it;
 - 5.4.1.2. the Data Protection Officer will log the date the request was received, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances as set out in paragraph 5.9), and send weekly chasers to all College Employees 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 limits the processing of the Personal Data in accordance with the restriction request. This may include moving documents to folders where they can no longer be accessed, removing details from files and locking paper files away;

RIGHTS OF INDIVIDUALS TO ACCESS PERSONAL DATA PROCEDURE

- 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;
- 5.4.1.7. throughout a Right to Restrict Processing Request the Data Protection Officer may be supported by the MIS Manager and/or Director of Technical Services and/or the Quality Co-ordinator.

5.5. Right to data portability

- 5.5.1. If a member of the College Employees 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 Employees must forward or report the request to the Data Protection Officer and the Director of Technical Services as soon as they receive it;
 - 5.5.1.2. the Data Protection Officer will log the date the request was received, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances as set out in paragraph 5.9), and send weekly chasers to all College Employees 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;
 - 5.5.1.5. throughout a Right of Data Portability Request the Data Protection Officer may be supported by the Director of Technical Services and/or the Quality Co-ordinator.

RIGHTS OF INDIVIDUALS TO ACCESS PERSONAL DATA PROCEDURE

5.6. Right to object

5.6.1. If a member of the College Employees 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 Employees must forward or report the request to the Data Protection Officer, MIS Manager and Director of Technical Services as soon as they receive it;
- 5.6.1.2. the Data Protection Officer will log the date the request was received, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances as set out in paragraph 5.9), and send weekly chasers to all College Employees 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 or it can demonstrate compelling legitimate grounds to continue;
- 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;
- 5.6.1.6. throughout a Right to Object Request the Data Protection Officer may be supported by the MIS Manager and/or Director of Technical Services and/or the Quality Co-ordinator.

5.7. Rights in relation to automated decision making/profiling

5.7.1. If a member of the College Employees receives a request from an individual in relation to an automated decision, including profiling, which produces legal or similarly significant effects, the following procedure will be followed:

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

RIGHTS OF INDIVIDUALS TO ACCESS PERSONAL DATA PROCEDURE

- 5.7.1.2. the Data Protection Officer will log the date the request was received, the deadline to respond (ordinarily one month from the date of receipt but an extension may be possible in certain circumstances as set out in paragraph 5.9), and send weekly chasers to all College Employees involved in dealing with the request in order to track its progress;
- 5.7.1.3. the Data Protection Officer will determine whether the decision in question:
- was based solely on automated processing; and
 - has legal or similarly significant effects on the individual;
- 5.7.1.4. where the decision is not based solely on automated processing, the request will be handled under the relevant rights procedure (e.g. right to object) as appropriate.
- 5.7.1.5. where the individual has the right to intervene in the automated decision-making process, the College will:
- carry out a meaningful human review of the decision;
 - consider all relevant factors, including any additional information provided by the individual;
 - allow the individual to express their point of view;
 - assess whether the original decision remains appropriate; and
 - where necessary, amend or retake the decision.
- 5.7.1.6. the College will provide the individual with meaningful information about the logic involved in the automated decision-making process and the likely consequences of the decision.
- 5.7.1.7. the Data Protection Officer will ensure that appropriate safeguards are in place, including oversight, accuracy checks, and measures to address any bias or inaccuracies identified. The College will write to the individual within one month of the date of their request confirming:
- the outcome of the review;
 - whether the decision has been upheld, amended, or withdrawn; and

RIGHTS OF INDIVIDUALS TO ACCESS PERSONAL DATA PROCEDURE

- the individual's right to complain to the College in the first instance and, if unresolved, to the Information Commissioner's Office (ICO).

5.7.1.8. the Data Protection Officer will ensure that a record is kept of the request, the assessment undertaken, and the outcome of the decision.

5.7.1.9. throughout a Right to Intervene in Automated Decisions Request the Data Protection Officer may be supported by the Quality Co-ordinator.

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 one month of receipt of the request. The communication shall include details of the

RIGHTS OF INDIVIDUALS TO ACCESS PERSONAL DATA PROCEDURE

College's reasons for not actioning the request and the ability of the individual to make a complaint to the college in the first instance and the ICO.

5.10. **Legal Advice**

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