**Data Rights Request Procedure**

The UK GDPR includes a range of rights for individuals (hereafter ‘data subjects’ as in the language of the law) around their data. Anyone whose data is processed by the Trafford and Stockport College Group (the Group) can make a rights request. The rights are not absolute, and several restrictions apply in certain circumstances.

The following procedure is referenced in the Group’s Data Protection Policy and sets out the requirements for dealing with rights requests.

# GETTING READY

The Group will take the following steps to ensure it is ready to receive and respond to data rights requests:

* Information and contact details on how to make a data rights request will be made available on the Group website
* All staff will be trained and guidance provided
* Specific staff will be given responsibility for dealing with subject access requests (SARs)
* A log of SARs and other rights requests received will be kept and record of SAR responses will be retained in accordance with the Group’s retention schedule
* Other data protection measures, such as security and the maintenance of privacy notices, records of processing activities and Data Protection Impact Assessments (DPIAs) shall be maintained to support compliance in handling data rights requests



# RECEIVING THE REQUEST

## Recognising a request

You may receive a request from a data subject quoting GDPR rights, asking for a copy of their data or requesting data to be deleted. These can be in writing via email, letter or via social media. If so, please forward as soon as you can to the data protection officer at dpo@tcsg.ac.uk.

If you receive a request verbally, this can still be valid but please collect contact details and provide them to the data protection officer. The forms, for a standard SAR and a CCTV request, are included in the appendices of this procedure and can be used to help a data subject structure their request (but they are not necessary).

The Group cannot refuse to deal with a request if it contains all the valid components but is not submitted in its preferred form.

## Requests on behalf of a data subject

A data subject may have a solicitor or other third party make a request on their behalf. In these circumstances the Group should ensure that there is proof of the authority being given by the data subject (e.g., a signed form).

## Verifying the identity of the requester

The Group may need to request specific information from the individual to confirm their identity and ensure their right to access the information (or to exercise any of their other rights). This is a security measure to ensure that personal information is not disclosed to any person who has no right to receive it. The information the Group requires should be reasonable and proportionate. In some cases it may be appropriate to request a formal identification document, in other cases a username or login credentials may be sufficient.

# ASSESSING THE REQUEST

## Timescales

The Group has 30 days to respond to the request. In circumstances where the request is particularly complex, you may extend this time to 90 days. If you do this, you must inform the data subject within 30 days of the original request.

## Refusing a request

The the Group can refuse to comply with a request if it is

* Manifestly unfounded, i.e., malicious, disruptive or targets a specific member of staff)
* Excessive, i.e., will create a large burden on resources or is a repeat / overlapping request with others from the same individual

With both of the grounds for refusal, it is quite a high threshold to reach and the the Group would need to record how this threshold was reached in the event of an appeal. If the request is excessive, it may be possible to charge a fee (see below).

## Charges

In most cases, a data subject rights request is free. If, in exceptional circumstances, the request will take excessive resource to comply with, the the Group may consider a fee. This can include costs such as printing, equipment (such as disks or USB sticks) and staff time. The the Group should record a breakdown of how these costs are calculated.

# DEALING WITH THE REQUEST

Some rights only apply to personal data processed under a specific legal basis. Always review the legal basis the data at issue in the rights request as the right might not apply to that data:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Legal basis for processing the data**  | **Right of Access** | **Right to Rectification**  | **Right to Erasure**  | **Right to Restriction**  | **Right to Portability**  | **Right to object**  |
| Consent  | Yes | Yes | Yes | Yes | Yes | Yes |
| Contract  | Yes | Yes | Yes | Yes | Yes | No |
| Legal Obligation  | Yes | Yes | No | Yes | No | No |
| Vital Interests  | Yes | Yes | Yes | Yes | No | No |
| Public Task  | Yes | Yes | No  | Yes | No | Yes |
| Legitimate Interests  | Yes | Yes | Yes | Yes | No | Yes |

## Right of access (or “Subject Access Request,” “SAR” or “DSAR”)

A data subject has the right to receive a copy of the personal information that we hold about them and information about how we use it.

The copy of the data subject’s information can include, but is not limited to, correspondence, reports run from a database or scans of hard copy records.

Any response should also explain:

* The purpose we are holding their data e.g., ‘your contact details to keep in touch with you’
* The types or categories of data e.g., photographic images, identification documents
* Who we would give the data to e.g., HMRC for a member of staff’s payroll information
* How long we are going to keep the data for and why
* Further information about the other GDPR rights to correct or have us remove their data
* How to make a complaint against the the Group about how their data is used
* Where the the Group holds data that has been provided to us by other people or organisations rather than the data subject
* If the the Group carries out any automated decision making about them and why and how we do it
* If the the Group sends their data outside the country, and especially outside the UK or European Economic Area (EEA), what checks are in place to protect their privacy where they have different data protection laws

Some of this information may be already be available in the the Group privacy notice.

### Data about other people

The right of access does not give the right to data about other data subjects. In many cases you will have to consider redactions or extraction of data where it may include third party data. Examples might include:

* Redacting the “bcc” list on an email sent to multiple recipients
* Extracting only the interview notes of the data subject from a document containing feedback on all candidates

You can disclose third party data to the data subject where that third party has consented to do so or it is reasonable to do so without the third party’s consent. Examples might include:

* If you are disclosing correspondence between the data subject and the the Group, there is no need to redact the correspondent’s name when it has already been disclosed to the data subject in the course of the correspondence.
* An interview panellist has given written authorisation that their feedback on the data subject can be attributed to them

### Exemptions

There are a several exemptions available in the UK Data Protection Act 2018,where explaining how data is processed or disclosing a copy of the data is not required. Some of the most common are:

* If you have provided data to the police requested by them to pursue an investigation
* If the data is formal legal advice provided to the Group by its solicitors
* If it relates to confidential references given or received

For further details, please consult the Data Protection Officer at dpo@tcsg.ac.uk.

## Right to rectification

An individual has right to ask us to correct their personal information where it is incorrect or incomplete.

**Action:** The the Group will assess the inaccuracy and correct it. If it holds that the information is accurate, it will explain to the requester why. If the inaccuracy has been shared with a third party, the the Group will take reasonable steps to inform them.

## Right to erasure (or “right to be forgotten”)

An individual has the right to ask that their personal information be deleted in certain circumstances, such as where consent has been withdrawn, where it is no longer necessary to keep it or where it legally needs to be deleted. There are a number of restrictions to this right:

* There is a legal obligation to keep it
* For the establishment, exercise or defence of legal claims
* It is being used for statistical purposes
* It is being used for occupational heath or public health purposes

**Action:** The the Group will assess the data held and erase any eligible data. If the inaccuracy has been shared with a third party, the the Group will take reasonable steps to inform them. This may include removing images or posts from social media accounts.

## Right to restrict the use of personal information

An individual has the right to request that we suspend our use of their personal information in certain circumstances. This is linked to the right to rectification and the right to object and often acts as a temporary state of affairs while a decision is made on correcting an inaccuracy or making a decision on legitimate interests.

**Action:** The Group will, whilst this is happening:

* Move the data to a different physical or virtual location
* Ensure the data is not accessed by staff in the normal course of work
* Remove data from a website or social media account

If the inaccuracy has been shared with a third party, the the Group will take reasonable steps to inform them. If a decision is made to lift the restriction, the the Group will inform the data subject first.

## Right to data portability

A data subject has the right to obtain certain types of their personal data in a structured, commonly used, and machine-readable format and for it to be transferred to another organisation, where this is technically feasible. The right only applies to data provided to us by the individual or obtained in monitoring that individual and where that data is processed under the legal bases of consent and contract.

**Action:** This isgenerally a right applied in commercial customer contexts and unlikely to apply to the Group. The Group should assess which data is eligible and is technically feasible to provide.

## Right to object to the use of personal information (including to object to direct marketing, automated decision making and profiling)

A data subject has the right to object to the use of their personal information. For direct marketing this is an absolute right. If the objection is for data where the the Group has a legitimate interest to process, then the the Group will need to demonstrate why this legitimate interest is compelling and overrides the rights of the individual.

The right to object to automated decision making or profiling applies to wholly automated decision making. If it carries out this type of processing, the the Group must allow the data subject to challenge the decision and conduct a human assessment of the decision.

**Action:** The Group will cease any direct marketing. It will assess any other eligible processing and communicate its decision to the data subject.

# MAKING THE FINAL RESPONSE

## Redaction

In the right of access, the data subject only has the right to receive a copy of their personal data. Any redactions should be added to a document to ensure other people’s data is not disclosed. Redaction software is available on applications such as PDF. Always ensure that redactions cannot be read through (for example if carried with a marker pen) or undone (if carried out on a word processing programme). If redaction is difficult, you may consider extracting information into a new document.

## Reasonable adjustments

The Group has an obligation under the Equality Act 2010 to make a reasonable adjustment for data subjects with disabilities. It is, for example, unacceptable to provide PDF scans of documents without optical character recognition to a data subject who requires a screen reader to access information. The the Group should check with the data subject if they have any special requirements for accessing the data.

## Secure sending / sharing

Disclosing the response to a subject access request requires the same commitment to data security as the other processing the the Group carries out. To ensure the secure transfer or sharing of the response, the the Group will:

* provide the responses in electronic format, unless the data subject makes a reasonable request for the data in hard copy
* double check all contact details for accuracy before dispatch or pressing send
* if providing the data via email the the Group should ensure that all attachments are password protected, with the password be communicated to the data subject in a separate communication, such as an email or phone call
* if providing the data by post the the Group will use registered delivery
* if providing remote access to the information for the data subject, the the Group will ensure controls are in place about how access is granted and for how long

## Content of the response

The response should clearly state any reasons why information has been refused, include the details of the complaint’s procedure as well as reference to the right to contact the ICO after exhausting the internal procedure. The response should also include a link to the relevant organisational privacy policy.

# apPENDIX A- DSAR template response

**Our ref:** [*enter case reference number*]

Dear ---

Thank you for your data subject access request, received [ENTER DATE].

Please find attached a copy of the data you requested.

The the Group is also obliged to provide the following information:

The purposes we are holding your data

e.g., *“your contact details to keep in touch with you”*

The types or categories of data

e.g., photographic images, identification documents

Any recipients of the data

e.g., *“Relevant staff payroll information will be provided to HMRC for tax purposes”*

How long the the Group will keep the data for and why

e.g., “*we will retain personnel records for six years following the financial year in which your employment ended.”*

The source of your data

e.g., “The the Group received the data directly from you and in the course of your work / project / subscription with us.” AND / OR “The the Group received your data as you were employed by one of the partners we were collaborating with.”

Automated decision making

Either “N/A” OR [*If the the Group carries out any automated decision making about them and why and how we do it (e.g., “automated recruitment tests for shortlisting purposes”)*]

International data transfers

Where your data is transferred outside the UK or European Economic Area (EEA), the the Group ensures appropriate safeguards are in place. We have Standard Contractual Clauses in place with our partner providers and carry out risk assessments on destination countries.

Your other rights as a data subject

You have a number of other rights in regard to your data, including the right to rectification, erasure and restriction of processing. You can opt-out of any direct marketing we send to you. To find out more please contact dpo@tcsg.ac.uk.

For further information on how your data is used please see our [***privacy policy***].

How to make a complaint

If you are unsatisfied with the response you have received, please contact dpo@tcsg.ac.uk. You can also make a complaint to the Information Commissioner’s Office (ICO) at the following address:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Telephone: 0303 123 1113

Website: <https://ico.org.uk/>

Yours sincerely,

[contact details]