SUBJECT ACCESS REQUEST PROCEDURE

PR52

If you receive a Subject Access Request, please notify Kelly Sooben, Vice Principal People & Resources in the first instance.

Introduction

Organisations process significant amounts of individuals' personal data. As data controllers, organisations are bound by the rights of data subjects, such as students/employees, including the right of access to personal data concerning them. It is very common for current or former employees/students to submit data subject access requests asking for personal data that South Devon College holds about them, often as a way of obtaining documents in connection with a grievance or dispute. Subject access requests are sometimes referred to as SARs or DSARs.

The General Data Protection Regulation (2016/679 EU) (GDPR) sets out a new EU data protection regime and has been in force throughout the EU since 25 May 2018. At the end of the Brexit transition period, the GDPR was converted into domestic law, as the UK GDPR, so South Devon College needs to continue to comply with the GDPR regime. The Data Protection Act 2018 supplements the requirements of the UK GDPR.

This guide explains individual's rights to make a Subject Access Request under the UK GDPR and sets out the processes that the College has in place to deal with those requests effectively.

Subject access rights under the UK GDPR

When responding to a subject access request, the College must provide the individual with the following information:

- the purposes for which the College processes the data;
- the categories of personal data it processes;
- the recipients, or categories of recipients, to whom the data has been or will be disclosed, (in particular, where the recipients are outside the European Economic Area (EEA));
- for how long it will hold the data (or how that period is determined);
- the individual's right to request rectification or erasure of data and to restrict or object to processing;
- the individual's right to complain to the ICO;
- the source of any data not provided by the College

- the existence of any automated decision-making (including profiling), the logic involved and the envisaged consequences of such decision-making for the employee; and

The UK GDPR requires the College to provide the individual with a copy of the personal data requested. If the individual makes a subject access request electronically, the response has to be provided in electronic form, unless the individual asks for another format.

If the individual asks for an additional copy of the information provided in response to a subject access request, the College can charge a reasonable fee, based on the administrative costs of providing the copies. The Data Protection Act 2018 allows the Government to set limits on the fees that employers can charge.

Under the UK GDPR, the College must comply with a subject access request without "undue delay" and at the latest within one month of receipt. If the request is complex, the College can extend the time limit for responding to three months. The College must inform the requestor of the extension and the reasons for it within one month of the original request.

The College does not have to process a subject access request if it cannot identify the data subject (although this is unlikely to be the case in the context of an ongoing relationship) (see Identifying data subjects).

If a request is manifestly unfounded or excessive (see below), in particular because it is repetitive, the College can charge a reasonable fee to reflect the administrative costs of providing the information (such as photocopying, printing or postage), or it can refuse to act on the request. The College must tell the individual, without undue delay and within one month of receipt, why it is not responding to the subject access request and of the individual's right to complain to the ICO and/or a court. If challenged, the College will need to demonstrate that the request is manifestly unfounded or excessive and justify any fee that it has charged.

Individuals may complain to the ICO and to the courts if they believe that the College has failed to respond to a subject access request properly.

On receipt of a subject access request, the coordinator should initially assess whether or not the request is complex. Subject access requests often will be complex, because of the volume and sensitivity of data organisations typically hold; although a request will not be complex solely because the individual has asked for a large amount of information. If the College intends to rely on the extended three-month time limit for dealing with complex subject access requests, it must notify the individual of this and the reasons for it within one month of receipt of the request. The College should also keep the individual informed if there is likely to be a delay in responding to a request. Communication with the individual may help reduce the risk of them making a complaint to the ICO.

The next step for the coordinator is to identify where the individual’s personal data is being stored, both electronically and manually. Internal processes should make it clear that the coordinator will share responsibility for collating information with other employees with access to relevant personal data. This may include the HR team, the individual's line manager and the IT department.

Identifying subject access requests

The College's data protection policy asks individual's to submit subject access requests in a particular way. However, the College cannot require individuals to use its preferred channel. If an individual submits a subject access request in some other way, including verbally, the College still has to respond to it within the relevant time limits. In its guidance on the right of access, the ICO recommends recording details of verbal requests and keeping a log of such requests. The College will confirm verbal requests in writing to ensure that it has properly understood the request being made.

There is no prescribed format for a valid subject access request under the UK GDPR. Individual's do not have to use particular language, refer to the UK GDPR, or state that they are making a subject access request. It just has to be clear that they are asking for copies of their personal information. For example, a request for "a copy of all information that you hold about me" or "all information relating to my recent grievance" will be a valid subject access request.

Subject access requests can be submitted by email, whether to an individual or public email address, or even through social media such as Facebook or Twitter.

Related policies and documents

- Form for individual to make subject access request

Identifying data subjects
Under the UK GDPR, the College is not required to comply with a subject access request if it cannot verify the identity of the data subject making the request.

Related policies and documents

- Letter responding to subject access request asking for more information

Clarifying the request
It is common for organisations to receive a subject access request that asks for "all information that you hold about me". Individuals are entitled to make such a request and the ICO regards the rights of data subjects to access their personal data as fundamental. However, in some circumstances it may be possible for the College to show that the individual's request would require the College to take steps that are unreasonable.

Under the UK GDPR, the College can refuse to comply with a subject access request if it is manifestly unfounded or excessive. This exception is likely to be interpreted strictly. A request is likely to be excessive in the employment context if it is repetitive and designed to force an employer to repeat an onerous exercise. Under the Data Protection Act 1998 regime, factors such as the purpose of processing and how quickly the data changes were relevant to deciding whether or not a reasonable interval has elapsed between two requests. ICO guidance on the right of access confirms that these factors are also relevant under the UK GDPR in deciding whether or not a request is excessive.

The ICO's guidance indicates that a request will not necessarily be excessive simply because of the volume of personal data sought, or the effort that will be involved in locating or reviewing data.

A request may be manifestly unfounded if its purpose is not genuinely to exercise the right of access. The ICO's guidance indicates that this may be the case if an individual makes a request but offers to withdraw it in return for some benefit from the organisation. A malicious request that is made in order to harass an organisation or cause disruption will also be manifestly unfounded. This may be obvious from the terms of the request. Requests that make unfounded allegations, target specific employees or are made as part of an ongoing campaign may also fall within this category. However, a request is unlikely to be manifestly unfounded if an individual genuinely wants to exercise their subject access rights.

If a request is manifestly unfounded or excessive, the College can refuse to respond, in which case we must advise the individual, within one month of the request, about their right to complain to the ICO or to the court. Alternatively, we can charge a "reasonable" fee, reflecting the administrative costs of providing the information, such as photocopying, printing and postage; equipment and supplies; and estimated staff time for responding to the request, charged at a reasonable hourly rate. The Data Protection Act 2018 allows the Government to introduce limits on what can be charged as a "reasonable" fee, although there are no limits currently in place.

It is important for the College to consider each request on its merits and keep a record of the reasons for thinking that it is manifestly unfounded or excessive. In the event of a complaint, the College may have to explain to the ICO its reasons for refusing to respond to the request or justify any fees charged.

Related policies and documents

- Letter refusing subject access request or asking for an administrative fee

Assembling the data

Assembling and reviewing the data is the most onerous element of dealing with a subject access request, given the quantity of data held by employers and the fact that it will probably be held in many different places. The College is under a duty to carry out a search that is proportionate to the benefits to the individual of receiving the information, bearing in mind the importance of subject access in the data protection regime.

The first step for the College is to consider what personal data it holds and where it is stored.

The College will hold various types of records about students/staff. All these will contain personal data that the College may have to provide in response to a subject access request. Individual personal data may be held outside personnel files and HR management systems. IT systems (particularly email) and employee monitoring systems will store large amounts of personal data.

Searching for data

Searching for personal data stored in email systems can be onerous. This is one element of the principle of data protection by design and default under the UK GDPR. However, given the volume of data processed through email, it is still likely to be necessary for the College to discuss and agree the scope of any search with the employee. This could include agreeing which email accounts will be searched, over what period, and the search terms that will be used to identify personal data. The

College needs to allow sufficient time to review the results of email searches properly to identify personal data.

In some cases, the College may have to search local drives of computer equipment for personal data.

Reviewing the data

Under the UK GDPR, on receipt of a subject access request, the College is required to give the individual a copy of the personal data undergoing processing. However, the personal data of the individual making the request may be mixed with the personal data of other people. The College must assess whether or not it should disclose such third-party data to the individual making the request. The UK GDPR states that the data subject's right to obtain a copy of the data must not adversely affect the rights and freedoms of others. Under the Data Protection Act 2018, the College can disclose information to the data subject making the request if the third party who is identified consents to this. Otherwise, the College has to consider whether or not it would be reasonable to disclose it without the third party's consent. What is reasonable depends on factors such as if the College owes the third party a duty of confidentiality, or if the third party has expressly refused consent. The College can redact the third party's personal data to avoid disclosing it to the individual.

The Data Protection Act 2018 contains exemptions in relation to some types of data. If personal data falls within an exemption, the College does not have to provide it in response to a subject access request. The exemptions that are most likely to apply in the employment context include:

- confidential employment references;
- personal data processed for management forecasting or planning if disclosure would prejudice the running of the College (such as plans for a forthcoming reorganisation);
- records of the College's intentions in relation to negotiations with the data subject if this would prejudice the negotiations; and
- information that is subject to legal professional privilege.

Under the UK GDPR, a data subject has the right to be given certain information in addition to the personal data itself. This includes a description of the categories of data and the purposes for which it is processed, among other things (see Subject access rights under the UK GDPR).

Providing the data to the individual

Once the College has collated and reviewed the personal data, it must provide it to the individual. The UK GDPR contains a recommendation that data controllers should provide access to personal data via remote access to a secure system.

If remote access is not possible, the response should still be provided electronically if the subject access request has been made electronically, unless the individual requests otherwise. This could be by way of password-protected documents, although this may be administratively cumbersome where large numbers of

documents are concerned, or a password-protected portable hard drive or USB device.

The College may decide to redact information to remove third-party data or where an exemption applies that means the information should not be disclosed. In some cases, whole documents may be withheld, for example documents that are subject to legal professional privilege, or where the data is so intermingled with third-party data that it is impossible to redact. The College must explain why it has made any redactions, to reduce the risk of a complaint to the ICO.

Related policies and documents

- Letter responding to subject access request providing requested information

Maintaining records of subject access requests
Under the UK GDPR, organisations are obliged to demonstrate that they comply with the personal data principles. This is known as the "accountability principle".

The College must keep a record of the steps they have taken to comply with subject access rights. This will include our policies and internal procedures for dealing with subject access requests and any template documentation it uses to respond to subject access requests.

The College will also keep a log of subject access requests that it receives and the steps taken to comply (this is a recommendation in the ICO's Accountability framework). This might include information about reliance on the extended time period for a response, whether or not the employee was advised of this within the relevant time period, which systems or departments have been searched and whether or not the employer provided the response within the extended time period. If the College did not provide the response within the relevant time period, the College will record the reasons for that along with the action it has taken because of the failure. If the individual's rights to access have been restricted (for example to protect the rights and freedoms of others), the College will also record the reasons for any restriction.

Related policies and documents

- Register of subject access requests

If you have any queries in relation to this procedure, please contact the Vice Principal People & Resources.

July 2021