Council for Higher Education in Art & Design

Responding to Data Subject Access Requests Policy

MANAGING SUBJECT ACCESS REQUESTS ("SAR")

1 Status and Scope

1.1 This policy for managing data subject access requests (the **policy**) has been approved by the Board of Trustees (**the Trustees**) of the Council for Higher Education in Art & Design (the **Charity**); it represents the standard to be applied by the Charity when responding to requests for access to data under the applicable data protection legislation.

1.2 This policy covers all individuals working at all levels and grades for the Charity, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as **staff** in this policy).

1.3 This policy is prepared in compliance with the requirements of the General Data Protection Regulation (EU 2016/679) (**GDPR**) and any UK law which implements the GDPR (together, **Data Protection Law**).

2 Introduction

2.1 The following sections provide information on subject access requests made under Data Protection Law and how to respond to them.

2.2 The key issues to understand in dealing with SARs are:

(a) The Charity's Director of Membership and Operations should be responsible for managing all SAR responses and **no action should be taken (including acknowledging the request)** without their authorisation;

(b) The Charity must be sure that the person making the request is the data subject, or authorised to make the request on behalf of the data subject (see below at 6);

(c) The data subject is only entitled to their own personal data and not to information relating to other people. Where information about one person cannot be separated from that of another, there are special rules about how to comply with the request (see below at 8);

(d) There are some limited circumstances in which the Charity is not required to provide information requested by a SAR (see below at 11);

(e) A request for personal data from someone other than the data subject is **not** a SAR but should still be passed to the Director of Membership and Operations who will decide how to handle it.

3 If you receive a SAR

3.1 All SARs must be forwarded to the Director of Membership and Operations, who will decide the most appropriate member of staff to deal with the SAR. Any member of staff assigned to deal with a SAR should circulate requests for information to the relevant departments and business units which may hold the personal data requested. The checklist in Annexe 1 should be used.

4 Time limit for response

4.1 The Charity must respond to a SAR without undue delay and, in any event, within one calendar month from the date the request is received.

4.2 Failure to respond to a SAR within the timeframe is a breach of Data Protection Law. It is the Charity's policy to respond promptly to valid requests and avoid behaviour that may be construed as delaying tactics (such as waiting until the deadline is nearly up before informing the applicant of any problems with their request).

4.3 If for any reason, the Charity is unable to respond to a SAR within the required timeframe, it should notify the individual promptly and keep the individual updated with information as to the ongoing status of their request.

5 Costs of a SAR

5.1 The Charity must generally provide the response and information free of charge.

5.2 However, if a request is manifestly unfounded or excessive, the Charity may either charge a reasonable fee or refuse to act on the request. In such circumstances, the Charity must be able to demonstrate that the request is indeed manifestly unfounded or excessive. If the Charity decides not to act on the request, it must give the reasons for doing so and inform the data subject of its right to complain to the Information Commissioner's Office and take legal action.

5.3 It is not yet clear how 'manifestly unfounded or excessive' is interpreted by Data Protection Law, although repetitive requests may be considered excessive. Until guidance is issued by the Information Commissioner's Office, the Charity should act on the request to the extent that it believes it is reasonable and proportionate, reserving any assertions that the

request is excessive or unfounded for use if that approach is challenged by the data subject.

6 What constitutes a valid SAR?

6.1 The data subject must, if required, provide evidence of their identity (such as a copy of their passport) to enable the Charity to satisfy itself that the person is the data subject.

6.2 The request must be in writing. However, the request does not need to mention Data Protection Law specifically or even say that it is a SAR.

6.3 If it is clear that the individual is asking for their own personal data it is a SAR and should be treated as such. A request by email (provided the requirements for proof of identity are met) is sufficient to meet the requirement for a written request.

7 Responding to SARs

7.1 The response must be provided in writing and the Charity will usually provide it in the form of a letter with attached schedule setting out the required information (see template at Annexe 2).

7.2 The Charity must not respond to a third party making a SAR on behalf of the data subject (for example, if a solicitor writes the request on behalf of an individual) without confirming first that it has the consent of the data subject himself. Any response should generally be sent to the individual and not the solicitor.

7.3 The right of subject access is to see the **information contained in personal data**. It does not include a right to see the documents that contain that information.

7.4 The following information must be included in the response to the SAR:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom data has been or will be disclosed;

(d) the period during which personal data will be retained;

(e) information on the source of the data;

(f) information regarding complaints and disputes: the right to complain to a supervisory authority, the right to request rectification or erasure

of personal data, to object to processing of data or to restrict that processing; and

(g) where personal data is transferred outside the EEA, information on any safeguards (for example, use of model clauses or binding corporate rules).

7.5 The Charity is responsible for ensuring that all personal data of the individual, including data processed on its behalf by a data processor, is captured in the response to the SAR. The Charity must ensure that it has contractual arrangements in place to guarantee that subject access requests are dealt with properly, irrespective of whether they are sent to the Charity or to the data processor.

7.6 Please note that a response should only be sent to the address held by the Charity for the Data Subject. If a request is made for the response to be provided to a different address from the address known to the Charity, the Charity is required to ensure that the person making the request is actually the Data Subject. This can be done by requesting proof of address and a copy of the requester's driving licence or passport. If a request is made on behalf of the Data Subject, for example, by a Union or a Solicitor, the response should be sent to the Data Subject as providing the information to the Union or a Solicitor could be an unlawful disclosure.

7.7 Responses containing personal data should not be sent electronically (due to the inherent insecurity of email) and should be sent by registered mail, unless specifically requested otherwise.

7.8 In general terms the following actions are required:

(a) a search needs to be undertaken to obtain all information held about the Data Subject making the request;

(b) the information then needs to be evaluated to establish whether it is Personal Data or Special Category Data;

(c) once the data is obtained it needs to be categorised and entered into the table along with the information as to the purposes for which it is Processed and whether it has been provided to any third parties.

7.9 If the source of the Personal Data can also be established, this needs to be provided in general terms. If it is generated by other employees of the Data Controller, these are data generated by the Data Controller and not the individual employees.

8 Other people's personal data

8.1 Under the right of subject access, an individual is entitled only to their own personal data, and not to information relating to other people (unless they are acting on behalf of that person). Often, information about one person is inextricably intertwined with personal data about another person: for example, the notes made by the appraiser at a performance review that include the appraiser's opinion of the appraisee's performance. The Charity must not disclose personal information about another individual who can be identified from that information, including that other person's opinions or statements of intention relating to the person making the SAR, unless:

(a) the other individual has consented to the disclosure; or

(b) the Charity decides it is reasonable in all the circumstances to disclose the information without that individual's consent.

8.2 It is for the Charity to decide what is appropriate to do in each case. This will involve balancing the data subject's right of access against the other individual's rights in respect of their own personal data. The Charity should keep a record of, and be able to justify, its course of action and reasoning. Data Protection Law provides a non-exhaustive list of considerations to take into account when making these decisions, including:

(a) any duty of confidentiality owed to the third party individual;

(b) any steps it has taken to try to get the consent of the third party individual;

(c) whether in the circumstances it is reasonable to approach the third party for consent;

(d) whether the third party individual is capable of giving consent;

(e) any express refusal of consent by the third party individual;

If the third party information has previously been provided to the individual making the request, is already known by them, or is generally available to the public, it will be more likely to be reasonable to disclose that information.

8.3 If the Charity has not obtained the consent of the third party individual and is not satisfied that it would be reasonable in all the circumstances to disclose the third party information, then the information should be withheld. However the Charity must communicate as much of the information requested as it can without disclosing the identity of the third

party individual, for example, by anonymising the information. Disclosing information with third party information redacted may give rise to complaints from the data subject. This is why the Charity uses the table format (Annexe 2) to respond to SARs.

9 Repeated requests

9.1 There is no limit to the number of subject access requests an individual may make but the Charity is not obliged to comply with an identical or similar request to one it has already dealt with, unless a reasonable interval has elapsed between the first request and any subsequent ones. This is a matter for the Director of Membership and Operations to determine, taking into account:

(a) the nature of the data, including whether it is particularly sensitive.

(b) the purposes of the processing: is it likely to cause detriment to the individual; and

(c) how often the data is altered: if information is unlikely to have changed between requests, there is no obligation to respond to the same request twice.

10 Confidential references

10.1 The Charity is not obliged to provide copies of confidential references that it has written about an individual. However, it may choose to provide the information, for instance if a reference is wholly or largely factual in nature, or if the individual is aware of an appraisal of their work or ability.

10.2 References about an individual, received from third parties should be disclosed, unless to do so would mean disclosing information about another individual who can be identified from that information (see section 8, above).

11 Exemptions

11.1 There are some exemptions from the requirement to supply Personal Data. These include situations involving:

- Crime prevention and detection;
- Negotiations with the requester;
- Management forecasts;
- Confidential references given by the Charity for employment, training or educational purposes; and

- Information covered by legal professional privilege.

11.2 Generally, exemptions should only be used in conjunction with legal advice.

12 Compliance

12.1 Individuals may complain to the Information Commissioner's Office or take legal action if no response is received within the time limit. Therefore, it is important that a correct response is made.

12.2 Please note that a data subject may complain to the Information Commissioner if they believe that a full response has not been given.

12.3 Further detailed guidance in relation to subject access requests is available on the Information Commissioner's Office website (www.ico.gov.uk).

13 Updating and monitoring this policy

13.1 The Charity's Director of Membership and Operations in conjunction with the Trustees shall be responsible for reviewing this policy periodically to ensure that it meets legal requirements and reflects best practice.

13.2 Staff are invited to comment on this policy and suggest ways in which it might be improved by contacting the Director of Membership and Operations.

Annex 1 SAR Response Checklist

Consider whether the SAR provides sufficient information with which to identify the data subject and the relevant data. If it does not, contact the person to request clarification.

Appoint a manager who is responsible for overseeing the collation of relevant data and ensuring that an adequate search is carried out, preparing a response to the data subject and redacting third party data if appropriate. This could be the Director of Membership and Operations, a manager in the relevant department or, where the request is from an employee, a personnel manager or the line manager of the employee making the request.

Check whether the subject made a previous request and, if so, has the personal data held changed since that request. Consider whether a further response required and if not, provide the subject with the reason.

Provide the heads of departments which might hold information on the data subject with an explanation of the types of data which are required. These include databases, word processing systems, emails, CCTV records, telephone records for landline and mobile phones, internet logs, automated payroll systems, and records of automated door entry systems such as swipe cards.

Contact external data processors which might hold information on the data subject and arrange for them to carry out the relevant checks (as above).

Inform everyone involved of the timescale within which the data needs to be collated and instruct them not to delete any relevant data unless it would have been deleted in the ordinary course of events.

After collating data, consider whether to seek consent from any third parties which might be identifiable from the data being disclosed. Notify the data subject if this is likely to lead to a delay in the provision of a response

- Does the information refer to a third party?
- Does this comprise personal data about the third party?
- Can this be anonymised?
- Has third party consent been sought? If not, record the reason
- Has third party consent been given? If not, consider if it is reasonable in all the circumstances to disclose the information, and record the reasons for your decision.

Consider whether any data is exempt from disclosure.

Provide the written response.

Annex 2: Form of Response

[ON THE HEADED PAPER OF
[CHARITY]]
[Date]

Private and Confidential
[Insert Name]
[Insert Address]
[Insert Address]

Dear [name]

Data Subject Access Request

Following your request for information under the General Data Protection Regulation (**GDPR**) we are writing to confirm that the Council for Higher Education in Art & Design (the **Charity**) does process your personal data.

You made the following request to the Charity (**your Request**):

[*Insert request*]

Under GDPR we are required to provide you with the source of the personal data, a description of the personal data, the purposes for which we process that data and the recipients or class of recipients to whom that data is or may be disclosed. There is no right under GDPR for you to have a copy of documents held by us.

We meet this requirement by setting out in the attached Schedule:

- the classes of personal data which we process in relation to your request (e.g. your name and your contact details);
- a description of your personal data in respect of each class;
- the purposes for which each class of your personal data is processed; and
- the recipients or classes of recipients to whom we disclose your personal data.

The sources of the information in the Schedule are:

- [you]; and
- [*insert other*]

[We have conducted reasonable and proportionate searches of our electronic systems and relevant filing systems to establish all of the personal data relating to you that we process. However, due to the number of different areas in which the Charity operates and without any more specific guidance from you as to where such data may be located, it is possible that there may be data processed in respect of you which the Charity has not been able to locate. If you believe there is specific information that we process about you that does not fall within the above exemptions but is not listed in the table and please provide us with sufficient details to enable us to locate such data and we will review our searches accordingly.]

In responding to your request we have disclosed as much of your personal data as we are able to without providing confidential personal data relating to third parties who have not consented to its disclosure, and where we do not consider it is reasonable in all the circumstances to disclose their information to you without such consent..

Some personal data is exempt from disclosure under GDPR and has been omitted from the schedule for the following reasons: **[*delete if not applicable*]**

[It consisted of a confidential reference given by us for employment purposes.]

[It consisted of personal data processed in connection with management forecasting or planning, disclosure of which we considered would prejudice the conduct of our business.]

[It consisted of records of intentions in relation to negotiations between us and you, disclosure of which we considered would be likely to prejudice those negotiations.]

[It is subject to legal privilege.]

[Where you have already been provided with copies of documents we have not summarised the contents of those documents in the Schedule.]

[We confirm that we have not undertaken any automated processing in relation to your personal data.]

Please refer any queries you may have in respect of this reply to your Request to [Data Protection Officer OR Other] at the above address.

Yours faithfully

For and on behalf of the Council for Higher Education in Art & Design

Insert/delete fields and headings (as appropriate) depending on the personal data identified as the result of the search. *Purposes and recipients are included only as a guide. Delete if not applicable. If others are identified, they should be included.*

[Data Subject's name] **Data Access Request – [date of request]**		
<u>Personal Data</u>	**<u>Purposes</u>**	**<u>Recipients of information</u>**
<u>Name:</u> [insert]	Internal administration purposes [other]	*Clients* *Suppliers* *Consultants* *Providers of employee services and benefits* *Professional Advisors*
<u>Address</u>: [insert]	Internal administration purposes	*Providers of employee services and benefits* *Professional Advisors*
<u>Contact numbers:</u> [insert]	Internal administration purposes	*Providers of employee services and benefits* *Professional Advisors*
<u>E-mail address</u>: [insert]	Internal administration purposes	*Providers of employee services and benefits* *Professional Advisors*
<u>Qualifications</u>: [insert]	Internal administration purposes	*Professional Regulators* *Professional Advisors*

Profession: [insert]	Internal administration purposes	*Professional Regulators* *Clients* *Suppliers* *Consultants* *Professional Advisors*
Medical Information [insert]	Internal administration purposes Sickness Records	*Professional Advisors* *Providers of employee services and benefits* *[Occupational Health]*
National Insurance Number: [insert]	Employment Administration Statutory Compliance Confirmation of permission to work in the UK	*HM Revenue and Customs* *Payroll* *Pensions* *Professional Advisors*
Nationality: [insert]	Internal administration	*Professional Advisors*
Education [insert]	Internal Administration Confirmation of relevant details provided for job application Decision to offer conditional employment	*Professional Advisors*

Current and Former Employers: [insert]	Internal administration	*H M Revenue and Customs* *Professional Advisors* *Former employers to obtain references.*
Photograph: [insert] OR [Contained within copy of passport]	Internal Administration Identification Procedures for confirmation of identity	*Professional Advisors*
Passport Number: [insert]	Identification purposes for confirmation of identity	*UKPA – confirmation that passport genuine* *Professional Advisors*
Next of Kin Details: [insert]	Employment administration and emergency planning	*Professional Advisors* *Next of Kin (if required)* *Emergency Services (if required)*
Ethnic Origin: [insert]	Equal Opportunities	*Professional Advisors*
Bank Details: [insert]	Internal Administration Payment for employment	*Payroll* *HM Revenue & Customs* *Professional Advisors*
Medical Report: [insert]	[Confirmation of fitness for work in respect of offer of employment]	*Professional Advisors*
Interview Comments: [insert] OR [Destroyed in line with HR Document Management Procedure – 1 year after vacancy completed and closed.]	Decision on offering position	

Observations: [insert] OR [Destroyed in line with HR Document Management Procedure – 1 year after vacancy completed and closed.]	Internal consideration.	*Professional Advisors*
References: [insert]	Internal consideration. Compliance with condition of offer of employment Internal Administration	*Professional Advisors* *Third parties seeking a reference*
Opinions [insert]	Internal administration purposes	*Professional Advisors*

[**Please insert any other headings and personal data identified as the result of the search. Purposes and recipients are only a guide. If others are identified, they should be included].**

Annex 3: Glossary

DPA terms relevant to subject access requests are explained below.

1 "Personal Data"

- Personal Data comprises information from which a living individual can be identified e.g. name, address, telephone number, email address. It includes biographical information and covers both work and personal information.
- However, just because a name is mentioned in a document, this does not make that document Personal Data. Personal Data also includes expressions of opinion about an individual and any indication of the intentions of the Charity or any person in relation to the individual.

2 "Special Categories" of data

"Special Categories" of Personal Data (under GDPR) are a subset of Personal Data, comprising data falling within the following categories:

- the racial or ethnic origin of the data subject;
- his political opinion;
- his religious beliefs or other beliefs of a similar nature;
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- his physical or mental health or condition;
- his sexual life;
- the commission or alleged commission by him of any offence; or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

3 "Processing"

Processing is defined by GDPR as meaning: obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data,
- retrieval, consultation or use of the information or data,
- disclosure of the information or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data.

4 "Relevant Filing System"

A relevant filing system is a manual filing system in which files are structured in a systematic way that allows ready access to information about individuals. For example, where personnel files are structured alphabetically by staff surname, or labelled by staff reference number (where the Charity holds information elsewhere connecting numbers to individuals), this would be a relevant filing system. However, loose papers held in a filing cabinet labelled "sickness records", where every page would have to be searched to check if any Personal Data about a particular individual was held, would not constitute a relevant filing system.

5 An individual whose Personal Data are Processed is known as a "Data Subject".