DATA SUBJECT ACCESS REQUEST POLICY AND PROCEDURE

CONTENTS

1. PURPOSE

1.1. This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance with the requirements for The Canterbury Auction Galleries (CAG) By the *GDPR.*

2. SCOPE

2.1. This policy and procedure applies across all entities or subsidiaries owned, controlled, or operated by CAG and to all employees, including part-time, temporary, or contract employees, that handle CAG data.

3. POLICY STATEMENT

3.1. The GDPR details rights of access to both manual data (which is recorded in a relevant filing system) and electronic data for the data subject. This is known as a Data Subject Access Request (DSAR).

3.2. Under the GDPR, organisations are required to respond to subject access requests within one month. Failure to do so is a breach of the GDPR and could lead to a complaint being made to the Data Protection Regulator.

3.3. This policy informs staff of the process for supplying individuals with the right of access to personal data and the right of access to staff information under the General Data Protection Regulation (hereinafter called GDPR). Specifically:

- All staff need to be aware of their responsibilities to provide information when a data subject access request is received. When a subject access request is received, it should immediately be reported to the Data Protection Officer to log and track each request.
- Requests must be made in writing (template form is provided, but not mandatory).
- The statutory response time is one month.
- Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the GDPR, information relating to the individual must only be disclosed to them or someone with their written consent to receive it.
- No fee can be charged for initial DSAR for all types of records, whether manual or electronic format.

4. PROCEDURE

How should DSARs be processed after receiving

When a subject access request is received from a data subject it should immediately be reported to the Data Protection Officer who will log and track each request. If you are asked to provide information, you will need to consider the following before deciding how to respond:

- Under GDPR Articles 7(3), 12, 13, 15-22 data subjects have the following rights:
  - to be informed;
  - to access their own data;
  - to rectification;
  - to erasure (Right to be Forgotten);
  - to restriction of processing;
  - to be notified;
  - to data portability;
  - to object;
  - to object to automated decision making.
- Requests must be made in writing (template form is attached, but is not mandatory). All DSARs received by email, mail, fax, social media, etc. must be processed.
- The type of access you must provide and the fee you are allowed to charge may vary depending on how the records are held. It does not have to state ‘subject access request’ or ‘data protection’ to constitute a request under the GDPR.

- If a request has already been complied with and an identical or similar request is received from the same individual a fee can be charged for the second request unless a reasonable interval has elapsed.
- The statutory response time is one month.
- Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the GDPR, information relating to the individual must only be disclosed to them or someone with their written consent to receive it.
- Before processing a request, the requestor's identity must be verified. Examples of suitable documentation include:
  - Valid Passport
  - Valid Identity Card
  - Valid Driving Licence
  - Birth Certificate along with some other proof of address e.g. a named utility bill (no longer than 3 months old)

Fees

4.1. No fee can be charged for providing information in response to a data subject access request, unless the request is 'manifestly unfounded or excessive', in particular because it is repetitive.
If CAG receives a request that is manifestly unfounded or excessive, it will charge a reasonable fee taking into account the administrative costs of responding to the request. Alternatively, CAG will be able to refuse to act on the request.

Subject access requests made by a representative or third party

4.2. Anyone with full mental capacity can authorise a representative/third party to help them make a data subject access request. Before disclosing any information, CAG must be satisfied that the third party has the authority to make the request on behalf of the requestor and that the appropriate authorisation to act on their behalf is included (see *Data Request Form*).

Complaints

4.3. If an individual is dissatisfied with the way CAG have dealt with their subject access request, they should be advised to invoke the CAG complaints process. If they are still dissatisfied, they can complain to the Data Protection Regulator.

5. RESPONSIBILITIES

Compliance, monitoring and review

5.1. The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing subject access rights at CAG rests with the Data Protection Officer.

5.2. All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant CAG policies and procedures.

Records management

5.3. Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised CAG recordkeeping system.

5.4. All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

6. TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

DSAR: data subject access request

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

7. RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Information Commissioners Office (ICO)
- The Canterbury Auction Galleries (CAG) Data Protection Policy

8. FEEDBACK AND SUGGESTIONS

CAG employees may provide feedback and suggestions about this document by consulting with their line manager.

9. APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	The Directors
Data Protection Officer	David Parker
Next Review Date	26/05/2024

Approval and Amendment History	Details
Original Approval Authority and Date	The Directors 26/05/2018
Amendment Authority and Date	

10. APPENDIX

Data Request Form