NATIONAL GALLERIES SCOTLAND

Data Protection Policy

Version	2.1
Date	30 April 2019
Owner	Data Protection Officer

Contents

1. Introduction

The National Galleries of Scotland (NGS) processes personal data on a daily basis to support our work and enable us to carry out our functions effectively.

The legislative framework protecting personal data was updated significantly on 25 May 2018 with the introduction of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). The NGS Data Protection Policy has been updated accordingly.

This policy sets out our commitment to complying with the data protection legislation, what this means for us in terms of our responsibilities as an organisation and the measures we must have in place to meet the legislative requirements.

2. NGS Data Protection Policy Statement

The National Galleries of Scotland is committed to protecting the rights and freedoms of individuals and, as such, processes all personal data under its control in accordance with applicable data protection legislation, including the General Data Protection Regulation and the Data Protection Act 2018.

3. Scope

Organisation, Employees and Third Parties
This Policy covers the activities of the NGS and the NGS Trading Company Ltd, a wholly-owned subsidiary. For ease of reference, 'NGS' refers to both when used in this policy document.

NGS is a data controller as defined in the GDPR but also operates as a joint controller and data processor for certain activities. NGS accepts the responsibilities which each role brings and implements the appropriate technical and organisational measures to ensure compliance in each case.

All NGS employees (permanent and temporary), trustees and volunteers are required to act in accordance with this policy and any other related policies and procedures that apply to them in place within NGS.

Any third parties (including freelancers) collecting, processing or with access to personal data on behalf of NGS will be required under contract to act in accordance with the data protection legislation, and where appropriate, this policy.

Protected Data
Any personal data which can be used to identify a living individual is protected and can only be processed in accordance with the GDPR and the DPA. This may include names and contact details, photographs, salary and pension details, bank account numbers, biographical information, online identifiers or even opinions written in emails, for example. Some data, such as trade union membership, religion or sexuality, falls into the 'special categories' defined in

the GDPR and requires additional protection. Personal data may be held in a variety of formats and on different systems.

4. Data Protection Officer

NGS is required, as a public body, to designate a Data Protection Officer (DPO) to fulfil the tasks set out in Article 39 of the GDPR, including:

- Informing and advising NGS and its employees of their data protection obligations
- Monitoring compliance with the data protection legislation and relevant policies
- Cooperating with the Information Commissioner's Office (ICO)

The DPO role at NGS sits within the remit of the Compliance Manager, based in the Director-General's Office. The current DPO, Kathryn Farrell, can be contacted for any NGS data protection matters as follows:

Data Protection Officer
National Galleries of Scotland
73 Belford Road
Edinburgh
EH4 3DS
Tel: 0131 624 6473
Email: dataprotection@nationalgalleries.org

5. Data Protection Principles

The GDPR sets out the principles to be followed when processing personal data (article 5), summarised as:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

To ensure compliance with the legislation, NGS is committed to embedding these principles in our activities in the following ways:

- We only collect and process personal data which is necessary and appropriate to fulfil our stated lawful purposes and in ways which do not harm the interests of the person(s) to whom the data relates.
- We do not process special categories or criminal convictions data unless a valid exemption applies under the GDPR and a relevant condition of the DPA is met where necessary.
- We consider using pseudonymised or anonymised data wherever possible.

- We are open about the data we collect, what we do with it, who it's shared with and what rights individuals have with regard to their data. To support this, we publish privacy notices for different groups/ processing purposes and make these easily accessible, unless an exemption applies.
- We have measures in place to maintain the accuracy and security of personal data.
- We provide guidance and training to employees to raise awareness of our data protection obligations and to ensure personal data is handled appropriately.
- We do not disclose data to third parties unless under contract with an individual, with their consent, or obliged to by law.
- We retain personal data only for as long as it is necessary for the fulfilment of our legitimate purposes and for no longer than it is required, at which point it will be securely deleted/ destroyed.
- We maintain a register of processing activity as required under Article 30 of the GDPR setting out the purposes for which data is processed, the lawful condition for processing, retention periods and ownership.

Our employment contract makes specific reference to this data protection policy and requires all NGS employees to abide by the employee code of conduct, which has been updated to reflect the new data protection requirements. Any failure to follow this policy may result in disciplinary proceedings.

6. Data Protection by Design and Default

Of fundamental importance for compliance with the data protection legislation is the concept of data protection by design and default. This requires NGS to implement appropriate measures to embed 'data protection' in all that we do, to ensure that implications for personal data are considered at the earliest stages of planning, and that the necessary safeguards are put in place to minimise privacy risks.

Data Protection Impact Assessment
An important tool for identifying and managing data privacy issues, a data protection impact assessment (DPIA) is a mandatory requirement for certain proposed processing activities. The ICO has provided detailed guidance on when a DPIA must be undertaken and when one should be considered. NGS' own process and forms take this into account.

Compliance Checklist
All reports to the Senior Management Team and the Board of Trustees require completion of a cover sheet with a compliance checklist, which includes confirming if a DPIA has been carried out or is still required.

7. Data Subjects' Rights

The new data protection regime provides individuals with important and enhanced rights in relation to their personal data. Subject to some legal exceptions, individuals have the right:

- To access the data held about them and to know what is done with it
- To have any inaccuracies corrected
- To have their personal data erased
- To place a restriction on the processing of their data
- To object to processing of their data
- To request that their data is provided in a portable format

If data is processed on the basis of consent, individuals can withdraw their consent at any time. There are also rights relating to automated decision-making and profiling, and to object to direct marketing.

NGS wants to make it as easy as possible for people to exercise their rights:

- All NGS privacy notices contain a guide to the relevant rights in each instance of processing and how individuals should make a request to exercise their rights.
- As well as a dedicated data protection email address, people can submit requests through an online form on the website.
- A detailed internal procedure for responding to requests is available to staff on the NGS intranet.
- NGS employees are made aware that they may receive a request for any of the above, by any means, and know to pass these to the Data Protection Officer as soon as possible.

We are required to respond within one month and will ensure the appropriate measures are in place to enable compliance with this time limit.

A record will be kept of all requests for access to personal data by the Data Protection Officer.

8. Data Sharing

NGS will not disclose personal data to any third party unless one of the data processing conditions is met, such as with the consent of the individual, and the principles of data protection are satisfied, including integrity and confidentiality of the data.

Transfers outside the European Economic Area (EEA)
With the exception of the data published on our website which may be seen anywhere in the world, we do not transmit data outside the EEA without adequate safeguards in place.

9. Third Party Processors

If NGS uses a third party to process data on our behalf, this will be on the basis of documented instructions from NGS to ensure appropriate safeguards are in place.

This requirement covers the use of online as-a-service providers such as email distribution, survey and event booking tools. A list of online service providers with data processing agreements in place is maintained by the Data Protection Officer.

10. Direct Marketing

NGS undertakes marketing for many reasons including advertising products for sale, publicising our public programme of exhibitions, displays and events, running fundraising campaigns, and promoting our vision and aims as an organisation.

We use multiple channels to convey our marketing messages. Our direct marketing is usually by post or email.

Any postal marketing we undertake will be on the lawful basis of consent or legitimate interest. Recipients will always be offered a way to withdraw consent or otherwise opt-out of such mailings.

Email and other electronic means of direct marketing are governed by the Privacy and Electronic Communications Regulations 2003 (PECR) and require specific, informed consent from recipients.

NGS complies with PECR and other relevant legislation when conducting direct marketing campaigns and will immediately stop direct marketing to an individual at their request.

11. Personal Data Breaches

NGS is required to report personal data breaches to the ICO within 72 hours of becoming aware of the breach. Breaches are security incidents which compromise personal data and pose a risk to individuals.

If there is a high risk to the affected individuals, NGS will notify those individuals. This may be through direct communication or a notice on our website, depending on the scale and severity of the breach.

NGS has a breach notification procedure in place within the organisation. This is designed to alert appropriate individuals to security incidents so that the incidents can be assessed and, if found to constitute a breach, be reported to the ICO.

12. Further Information

This document is available to staff on the NGS intranet, and available to the public on www.nationalgalleries.org or on request.

Detailed procedures and training for specific systems in use within NGS are available separately for staff.

A set of useful definitions and terminology is included at Appendix 1.

Further information on Data Protection and this policy can be obtained from the Data Protection Officer (contact details provided at section 4 above).

Useful guidance on the application of current data protection legislation is available on the UK Information Commissioner's website at www.ico.gov.uk.

13. Complaints

As well as contacting the Data Protection Officer using the details above, you can use our Feedback procedure to make a complaint about the way we process your personal information, including using the online contact form at https://www.nationalgalleries.org/content/contact-us.

You also have the right to lodge a complaint directly with the UK Information Commissioner's Office (ICO), the data protection supervisory authority in the UK by visiting www.ico.org.uk.

Appendix 1: Definitions and Terminology

Definitions used in this document

- NGS: National Galleries of Scotland & Trading Company
- GDPR: General Data Protection Regulation (EU) 2016/679
- DPA: Data Protection Act 2018
- PECR: Privacy and Electronic Communications (EC Directive) Regulations 2003
- ICO: The UK Information Commissioner's Office

Terms defined under the GDPR

Personal data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Categories: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Processing of data: any operation or set or operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Controller: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (in this case, NGS).

Terms defined under the DPA

Public authority and *public body:* a Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002.

NGS is therefore a 'public authority' or 'public body' for the purposes of the data protection legislation. This definition only applies when performing a task carried out in the public interest or exercising official authority.