THE GLASGOW SCHOOL OF ART

Data Protection Policy

Policy control

Reference	GSA Data Protection Policy
Date approved	5th May 2015
Approving Bodies	Executive Group
Implementation Date	5th May 2015
Supporting policy	Information Security policy
Review date	December 2017
Author	Colin Watson
Date of completed Equality Impact Assessment	2nd April 2015

Table of Contents

Data Protection Policy

Introduction

The GSA needs to keep certain information about its employees, students and other users to allow it to monitor performance and achievements and, for example, to ensure health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, personal information must be collected and used fairly, stored securely and not disclosed to any other person unlawfully. To do this, the GSA must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The GSA and all staff or others who process or use any personal information must ensure that they follow these principles at all times.

Status of this Policy

This policy does not form part of the formal contract of employment for staff, or the formal offer of a place for study for students, but it is a condition of employment or study that employees and students will abide by the rules and policies made by GSA where required to do so. Any failure to follow this policy can therefore result in disciplinary proceedings.

Definitions

Data Subject

The Data Subject is the individual on whom data is being kept. e.g. a student, member of staff, customer, supplier, etc.

Personal data

Personal data is any information held on a living individual which contains a data item which will allow that individual to be identified. Data items that allow identification include: name, address, date of birth, National Insurance number, etc.

Personal data covers both facts and expressed opinions about the individual.

Personal data can take the form of text and images (pictures and photos). It can be held on a computer, on paper or on CCTV.

Sensitive personal data

Sensitive personal data includes racial or ethnic origin, gender, age, political opinions, religious beliefs, trade union membership, physical or mental health, sexual orientation, commission or alleged commission of an offence and any proceedings from it.

Since this information is considered sensitive, staff and students will be asked to give express consent for the GSA to do this.

Processing

Processing, in relation to personal information or data, means obtaining, recording or holding the information or data. This includes collection, recording, storage, organisation, adaptation, alteration, alignment, combination, blocking, erasure or destruction of the information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure of the information or data.

Relevant filing system

Relevant filing system (including information held on paper) is any set of information relating to an individual that is structured to allow that information to be readily accessible. For example ordered by name or programme or department, etc. This could include staff telephone lists, student application forms, student record cards.

Use of Personal Data

GSA collects, holds and uses personal data relating to individuals who have/have had a relationship with the institution. Individuals about whom GSA holds personal data will be informed at the outset as to the purposes for which their data was collected.

Data to be collected

Any personal data must be obtained and processed for specified purposes. It is illegal to use personal data that was collected for one purpose for another. For example the GSA keeps personal data about students that is collected via their Registration Form for appropriate GSA business and to satisfy legal requirements. It therefore cannot be used for projects and/or research unrelated to the purpose for which the data was originally collected.

The personal data that is collected must be adequate, relevant and not excessive. That is there must be a specific reason why we need a specific piece of data. It is unacceptable to collect data just in case it may be useful later on.

When obtaining personal data it is essential that the length of time for which it needs to be kept is determined. It should not be held longer than necessary.

Data Subjects rights

In many cases, the GSA can only process personal data with the consent of the individual. In all cases, where the data is sensitive, express consent must be obtained. Agreement to the GSA processing personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

All employees are bound by GSA's policies as stipulated by their contract; and all students are bound by GSA's policies as stipulated by their registration form. Consequently by signing their contract, or submitting their student registration form, all prospective staff and students acknowledge that personal data will be collected and processed to meet the business requirements and legal obligations of GSA. A refusal to sign such a form can result in the offer being withdrawn.

Notification

Notification is a statutory requirement and every organisation that processes personal information must notify the Information Commissioner's Office (ICO), unless they are exempt. Failure to notify is a criminal offence.

Notification is the process by which GSA gives the Information Commissioner details about their processing of personal information. The Information Commissioner publishes certain details in the register of data controllers, which is available to the public for inspection.

In order to ensure that GSA's notification is accurate, the institution's Data Protection Officer (Head of Policy and Governance) must be informed of any data sets used within the GSA.

Consequently, all personal data or information held by the GSA, either centrally or by departments, must be notified to GSA's Data Protection Officer. The following information must be provided

- a description of the personal data being held
- a description of the purpose for which the data is being processed
- a description of the intended disclosure of the information
- the name of any countries outside the European Economic Area to which personal data may be transferred
- a description of the general security measures that are used to protect this data

All existing and new sets of information held (on paper or computer) that contain personal data must be notified to GSA's Data Protection Officer (the Head of Policy and Governance)

Responsibilities of Staff

All staff are responsible for:

- checking that any information that they provide to GSA in connection with their employment is accurate and up-to-date,
- informing GSA of any changes to the personal data which they have previously provided e.g. change of address,
- informing GSA of any errors or changes in their personal data.

When staff process information about other people (e.g. opinions about ability, references, details of personal circumstances etc.) they have a responsibility to ensure that they are doing so in accordance with the Act.

Staff who have a responsibility for mentoring/supervising students who are undertaking processing of personal data, e.g. as part of a research project or on a placement, have a responsibility to ensure that the student is informed as to his/her responsibilities under the Act, by reference to this policy and other relevant materials. In addition, departments must ensure that students complete the "Authorisation Form for Data Processing by Students" (ANNEX 1). This form must be retained in case of audit.

GSA's Data Protection Officer (Head of Policy and Governance) can provide additional guidance to assist staff in understanding and complying with data protection.

The Registrar is the institution's Senior Officer responsible for compliance with the Act.

Members of GSA's Executive Group are responsible for compliance with the Act within the areas of the institution over which they have management responsibility.

Heads of School/Department (academic and service) have responsibility for ensuring that arrangements in their area comply with the Act.

Heads of School/Department may nominate a Departmental Data Protection Contact to advise on issues and deal with day-to-day matters. The nomination of a Departmental Data Protection Contact must be notified by email (dataprotection@gsa.ac.uk) to GSA's Data Protection Officer by the Head of Department. A copy of the notification email must be retained by the department as evidence of this designation of responsibility.

Without such notification, or in the absence of the appointed member of staff, the Head of Department shall assume the duties of the Departmental Data Protection Contact.

Departmental Data Protection Contacts should advise colleagues on data protection issues where appropriate. Otherwise, they can refer issues to the Data Protection Officer. Departmental Contacts are also responsible for collating any personal data required from their area in relation to Subject Access Requests (SARs). They must treat such requests in the strictest confidence and handle them on a "need-to-know" basis. Only those staff whose input is required to respond to a SAR should be informed that a request has been received.

Use of Personally-owned Computers and Equipment for Data Processing

Personal Data must be processed only on equipment and systems controlled by GSA.

Members of staff are not normally permitted to use their own personal equipment (phones, tablets, laptops) for storing personal data on behalf of GSA, unless they have explicit written consent from their Head of Department. Such devices may be searched if required to comply with a Subject Access Request.

Responsibilities of Students

All students are responsible for:

- checking that any information that they provide to GSA is accurate and up-to-date,
- informing GSA of any changes to the personal data which they have previously provided e.g. change of address,
- checking the information that GSA sends out to them is correct, and informing GSA of any errors or changes in their personal data.

Students who are considering processing personal data as part of their studies must notify and seek approval from their supervisor/Head of Department before any processing takes place. Such students will be bound by the Act and by this policy and must ensure that they act in accordance with both. Departments must ensure that students complete the "Authorisation Form for Data Processing by Students" (ANNEX 1). This form must be retained in case of audit.

Responsibilities of Others Working for and on behalf of GSA

GSA is responsible for the use made of personal data by anyone working on its behalf. Heads of Departments/Schools, who employ third parties who will handle personal data on its behalf, i.e. contractors, external supervisors, external examiners, must ensure that these third parties:

- are made aware of this policy and adhere to its terms,
- do not have access to personal data beyond that required for the work to be carried out,
- return or destroy personal data on completion of the work.

Data Security

All staff and students are responsible for ensuring that:

- any personal data which they hold is kept securely (either by physical storage means or by using appropriate IT equipment/security measures), and
- personal information is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party.

Personal data or information held on paper should be kept in locked cupboards and/or drawers unless it is being worked on.

Where personal information is held digitally on a device which is taken outside the GSA, suitable security precautions must be taken to ensure that the data is protected if the device is lost or stolen. This will generally necessitate the use of encryption of drives or files.

Similar precautions must be considered where data is to be transferred across the network e.g. via email, especially if it is sent outside GSA's network.

It is the responsibility of individuals handling the data to ensure that it is securely protected.

Further information and advice in relation to methods of secure IT storage/ transfer can be obtained from GSA's IT Department.

Unauthorised disclosure of personal data is a breach of the Act and may also be a disciplinary matter, and could be considered gross misconduct in some cases. Staff may also incur criminal liability if they knowingly or recklessly obtain and/or disclose personal information without the consent of GSA i.e. for their own purposes, which are outside the legitimate purposes of GSA.

Data storage

All personal data whether held on a computer or in a relevant filing system must

- be kept accurate
- be kept up to date
- be kept secure, and
- not be held longer than necessary.

This reflects not just central administrative systems but department based systems whether held on computer or paper. The holding of duplicate information leads to inaccuracies and extra care must be taken to ensure that all copies of personal data are updated.

Destruction of personal data

When obtaining personal data the length of time for which it needs to be kept should already have been determined according to a Retention Schedule. At this point personal data must be treated as confidential information and destroyed in an appropriate manner. If it is held on a computer appropriate data must be deleted from all files and archives. If held in another form it should be shredded. Further information on GSA's retention schedules can be found on the Records Management page on GSA's website[1]

Disclosure of personal data

The collection and notification of personal data indicates what disclosures can legally be made and to whom.

[1] http://www.gsa.ac.uk/about-gsa/key-information/records-management/

- We are not allowed to disclose information about staff or students without their consent. This includes confirming that they are students or members of staff of the GSA.
- External requests for information about staff or students must be properly checked. This should preferably be on appropriate headed notepaper containing telephone and/or fax numbers that could be checked out. We are allowed to disclose personal information to meet the GSA's legal requirements – e.g. HESA, Inland Revenue, etc. Again, unless it is someone from these Agencies that you have regular dealings with ask for the request in writing. Most requests within this area are likely to be addressed to either the Registry or Human Resources who should be familiar with legal exemptions under the Act.
- If staff or students are undertaking a period of study and/or placement abroad in countries outwith the European Economic Area then only personal information required to allow this to go ahead should be disclosed. In these circumstances express consent in the form of a signed agreement must be given by the individual(s) concerned.

Rights to Access Information

Staff, students and other users of the GSA have the right to access any personal data that is being kept about them either on computer or in a relevant filing system. This is known as a 'Subject Access Request' (SAR). The Data Subject has the right to

- request a copy of data held
- have it corrected
- prevent certain types of processing (e.g. automated decision taking, direct marketing, processing likely to cause substantial damage or substantial stress)

The Act however, requires the Data Subject to put the request in writing providing sufficient information to allow the data to be readily retrieved and to pay an administrative fee.

The Act also stipulates the time (starting from receipt of the fee) within which the Data Subject must be provided with a copy of their personal data. In most instances this will be 40 days.

Hence all requests must be made in writing and accompanied by a cheque for £10 made payable to The Glasgow School of Art. Requests can be made by email via the following email address: dataprotection@gsa.ac.uk

GSA has produced a document entitled "*Data Protection Subject Access Request Protocol*" which provides further guidance which must be followed by staff when dealing with SARs.

Other Rights under the Act

GSA recognises that under the Act an individual can request that the GSA does not process information about him/her if that processing causes substantial unwarranted damage or distress. The GSA is not always bound to comply with the request. Individuals should be aware that, in some cases, by exercising this right they may disadvantage themselves or, in extreme cases, may be unable to begin/continue studying or employment with GSA. The GSA will consider every request and will inform the individual of its decision within 21 days, as required by law. If an individual

chooses to exercise this right to "prevent processing of information" it in no way affects his/her other rights under the Act.

Transmission of personal data abroad

Under the provisions of the Data Protection Act 1998 personal data may only be transferred abroad to

- the European Economic Area (EEA) which consists of the EU States, Iceland, Norway, Liechtenstein; or
- other countries that have similar data protection legislation, or
- elsewhere, only with the consent of the Data Subject (a caveat should be included indicating that the information may only be used for the purposes it was provided)

Research, history and statistics

Where personal data is used for the purposes of research, history and statistics it

- must have been obtained fairly and lawfully
- is exempt from subject access so long as it is not used to support measures or decisions with respect to a specific individual
- may be held indefinitely
- must not be processed in a way that is likely to cause substantial damage or substantial stress to the Data Subject

Examination scripts and marks

Personal information recorded by candidates during an examination are exempt from subject access.

Students will be entitled to information about their marks for both coursework and examinations. Prior to the publishing of examination marks Data Subjects may make a request for access to their examination marks. In this particular situation the time within which a response has to be made is extended to 5 months from receipt of the request or 40 days after the publication of the examination results, whichever is earlier.

Coursework containing personal information

Where possible information used by students in coursework should be anonymous. Where this is impossible it must be collected within the auspices of the Data Protection Act 1998. Such coursework should not be kept longer than necessary and should then be shredded.

Confidential references

Confidential references given by members of the GSA for specific purposes (e.g. employment, training) are exempt from access by the data subject. However they can be disclosed to the data subject by the recipient of the reference. Hence a data subject can ask to see a reference that we have received.

Direct marketing

Direct marketing relates to communication (regardless of media) with respect to advertising and or marketing material that is directed to individuals. e.g. mail shots for fund raising, short courses, etc. Such uses of personal data must be registered. However under the auspices of the Data Protection Act 1998 the Data Subject has the right to be removed from such lists (free of charge). Direct Marketing must also meet the regulations of the Telecommunications (Data Protection and Privacy)(Direct Marketing) Regulations 1998.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 altered the consent requirement for most electronic marketing to "positive consent" such as an “opt in” box. Exemptions remain for the marketing of "similar products and services" to existing customers and enquirers, which can still be permitted on an opt-out basis.

Implementation

The GSA will implement these Data Protection Guidelines by:

- Ensuring that there is a general awareness of Data Protection issues
- Delegating specific responsibilities for Data Protection

Breaches of the Data Protection Act

Where a breach of the Act occurs, any possible actions to mitigate the breach should be taken by the relevant area immediately upon discovery of the breach i.e. removing personal data from a publicly-accessible website etc. The Data Protection Officer should be informed of the breach at the earliest possible opportunity.

The breach will be investigated by the Data Protection Officer in line with current guidance from the Information Commissioner’s Office www.ico.gov.uk.

Where appropriate the Information Commissioner’s Office will be informed of a breach. The Data Protection Officer will act as the main point of contact for any subsequent investigation.

Conclusion

Compliance with the Act is the responsibility of all members of GSA. Any deliberate breach of the Data Protection Policy may lead to: disciplinary action being taken, access to GSA’s facilities being withdrawn, or even a criminal prosecution

Any questions or concerns about the interpretation or operation of this policy should be addressed to the Data Protection Officer. Further guidance can be found on the Information Commissioner’s Office www.ico.gov.uk.

Review

This policy will be subject to review every three years, or as required, in order to comply with any changes in UK/EU guidance or legislation.

ANNEX 1: AUTHORISATION FORM FOR DATA PROCESSING BY STUDENTS

I confirm that my department has provided me with copies of GSA's Data Protection Policy and any other relevant information which I have read and understood. The data processing to be undertaken is part of my research/studies, as discussed with the departmental contact for Data Protection and Head of Department. My processing shall conform to the requirements the Data Protection Act 1998, and specifically GSA's Data Protection Policy, the Data Protection Principles, and GSA's Data Protection Notification to the ICO.

Student's Name	
Registration Number	
Department	
Programme	
Signature	
Date	

To be completed by the Head of Department

I confirm that the department has complied with the requirements of GSA's Data Protection Policy regarding granting the above student authorisation to process personal data under the GSA's Data Protection Notification to the ICO.

Name	
Title	*Head of Department*
Department	
Signature	
Date	

A copy of this form must be held by the department for audit purposes.