DATA PROTECTION POLICY

POLICY DETAILS:

Date of approval	5 June 2018
Approving body	Executive Group
Supersedes	previous Data Protection Policy
Date of EIA	tbc
Date of next review	*See departmental schedule*
Author	Data Protection Officer
Responsible Executive Group area	Registrar and Secretary
Related policies and documents	IT Policies
Benchmarking	The General Data Protection Regulation Information Commissioner's Office University of Stirling IT Governance Policy Templates

THE GLASGOW SCHOOL OF ART

EXECUTIVE GROUP

DATA PROTECTION POLICY

CONTENTS

PART III: FORMS

The undernoted forms are available on GSA's Data Protection webpages at **www.gsa.ac.uk/about-gsa/key-information/general-data-protection-regulation/**

40. **Forms**
To be confirmed. Please contact the DPO in the meantime.

PART IV: REGISTERS

The undernoted registers, which are held centrally by the Data Protection Officer, are available, for information, on GSA's Data Protection webpages at
www.gsa.ac.uk/about-gsa/key-information/general-data-protection-regulation/

41. **Registers**
To be confirmed. Please contact the DPO in the meantime.

PART V: TEMPLATES

The undernoted templates are available on GSA's Data Protection webpages at **www.gsa.ac.uk/about-gsa/key-information/general-data-protection-regulation/**

42. **Templates**
To be confirmed. Please contact the DPO in the meantime.

KEY CONTACTS

1. GSA DATA PROTECTION OFFICER

GSA's Data Protection Officer (DPO) is Tom McDonnell.
DataProtection@gsa.ac.uk

2. LOCAL DATA PROTECTION CO-ORDINATORS

a) For areas reporting to Professor Ken Neil, Deputy Director (Academic), including all academic Schools and departments, Learning and Teaching, and Research and Enterprise.

Jane Stickley-Woods	**j.stickley-woods@gsa.ac.uk**
John Quinn	**j.quinn@gsa.ac.uk**

b) For areas reporting to Professor Irene McAra-McWilliam, Deputy Director (Innovation)

Tom McDonnell	**DataProtection@gsa.ac.uk**

c) For areas reporting to Dr Craig Williamson, Registrar and Secretary, including all the Academic Registry, Student Support and Development, Information Technology, Technical Support, Human Resources, Learning Resources, the Academic Quality Office, and the Corporate Governance Office.

Sheila Kay	**sh.kay@gsa.ac.uk**
Virginia Toyi	**v.toyi@gsa.ac.uk**

d) For areas reporting to Mr Alastair Milloy, Director of Finance and Resources, including Finance, Estates, Health and Safety, and Procurement.

Alistair Storey	**a.storey@gsa.ac.uk**

e) For areas reporting to Mr Alan Horn, Director of Development

Margaux Achard-Brown	**m.achardbrown@gsa.ac.uk**

f) For areas reporting to Mr Scott Parsons, Director of Strategy and Marketing, including Student Recruitment and International Office, International Academic Development, Marketing and Communications, Alumni and Events, and Open Studio.

Shona Paul	**s.paul@gsa.ac.uk**
Vanessa Johnson	**v.johnson@gsa.ac.uk**

3. OFFICE OF THE INFORMATION COMMISSIONER
www.ico.org.uk

PART I: GENERAL PRINCIPLES

1 INTRODUCTION

1) The General Data Protection Regulation (EU) 2016/679 (GDPR), formally approved by the European Parliament on 27 April 2016, is effective as of 25 May 2018.

2) As a Regulation, it is directly applicable throughout the UK without the need for domestic legislation, although it should be noted that the UK Parliament in Westminster has enacted a new Data Protection Act which is designed to supplement the GDPR and have the effect of ensuring GDPR remains applicable in the UK post-Brexit. Accordingly, the new Data Protection Act should be read alongside the GDPR.

3) The GDPR effectively repeals the current data protection regime under the Data Protection Act 1998, and introduces a new framework regulating the processing of personal data.

4) The main purpose of the GDPR is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, in accordance with their rights.

5) The GDPR applies to "personal data" which is all data relating to (directly or indirectly), and descriptive of, living individuals who are referred to as "data subjects". Definitions of the main terms used in this policy are set out in the Glossary in section 39 of this document.

6) The GDPR imposes obligations on the Glasgow School of Art (GSA) and the means by which it handles personal data. GSA, its staff, students and members of the Board of Governors are obliged to ensure that personal data is processed fairly, lawfully and securely.

7) Personal data should only be processed if GSA has a valid condition for processing (normally, through consent or contract), and GSA has provided information to the data subject about how and why their data is being processed (normally, through a privacy notice).

8) There are restrictions on what GSA is permitted to do with personal data, such as passing it on to third parties, transferring data outside the EU or using it for direct marketing.

9) The GDPR gives data subjects various rights including, *among others*, the rights:

   - to access the data held;
   - to prevent processing likely to cause damage or distress;
   - to take action to rectify or destroy inaccurate data, including the right to be forgotten; and
   - to sue for compensation following a contravention of any of the provisions of the GDPR.

10) In the UK, the responsibility for monitoring, auditing and enforcing all aspects of the GDPR rests with the Information Commissioner's Office (ICO). GSA may be required to satisfy the ICO at any time that GSA is fully compliant with all of the provisions of the GDPR, therefore it is important that all staff, students and members of the Board of Governors understand and comply with this Data Protection Policy.

2 PURPOSE OF THIS POLICY AND THE IMPACT OF NON-COMPLIANCE WITH GDPR

1) It is important to recognise that the data which GSA collects will be other peoples' personal and/or special category data including, *among others*, data relating to a data subject's racial or ethnic origin, political opinions and affiliations, religious beliefs, trade union activities, physical and/or mental health, and sexual life.

2) It is important that every member of GSA staff, its student body and members of the Board of Governors has an understanding of the main legal principles (including the six GDPR data protection principles, set out in section 5 below) relating to the gathering, storing and transmission of a wide range of personal data on a variety of data subjects including, *among others,* students (potential, current and former), staff (potential, current and former), members of the Board of Governors (potential, current and former), customers/suppliers, clients and members of the public.

3) It is important that every student, member of GSA staff and members of the Board of Governors recognises that compliance with the provisions of the GDPR is essential and that data protection is an integral part of GSA's overall data security and records management regimes.

4) This policy, together with its associated Forms, Registers and Templates sets out the responsibilities of GSA, its staff, members of the Board of Governors and its students to comply fully with the provisions of the GDPR, and together they form the framework from which GSA staff, members of the Board of Governors and students should operate to ensure compliance with the GDPR.

5) Any deliberate breach of the GDPR and this Policy, and/or failure to adhere to the six data protection principles, may lead to disciplinary action being taken and access to GSA facilities being withdrawn.

6) The GDPR authorises punitive action by the ICO, and criminal prosecution is also a possibility.

3 SCOPE

1) This policy applies to all staff, members of the Board of Governors and students, and all items of personal data that are created, collected, stored and/or processed through any activity of GSA, across all areas, including Schools and Professional Support areas.

4 ASSOCIATED POLICIES

1) The following associated policies should be consulted in conjunction with this Data Protection Policy as appropriate:

   a. Policy for Staff Electronic File backup
   b. Management of IT Business Systems
   c. IT Service Level Agreement
   d. Information Technology Security Policy
   e. IT Backup and Recovery Policy
   f. Staff Acceptable IT Use Policy
   g. Student Acceptable IT Use Policy
   h. Remote Working Policy – IT Acceptable Use
   i. Policy for Virtual Private Network Usage at GSA
   j. GSA Records Management Policy
   k. Procurement Policy
   l. CCTV Operational Policy

5 DATA PROTECTION PRINCIPLES

1) GSA, its staff, members of the Board of Governors and students must adhere to the six principles of data protection as laid down by the GDPR.

2) The six principles seek to ensure that data must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

3) The six principles are:

   i) Lawfulness, fairness and transparency.
   Personal data must be processed lawfully, fairly and in a transparent manner.

   a) **Lawful** means that GSA must identify a lawful basis, or "condition for processing" before data can be processed, for example, consent or contract.

   b) **Fairly** means that GSA must make certain information available to the data subject as practicable, irrespective of the source from which the data was obtained.

   c) **Transparency** means that GSA must give specific privacy information to data subjects, in an intelligible form and using clear and plain language. The GDPR sets out a minimum of nine elements on which information must be given to the data subject.

   ii) Purpose limitation.
   Personal data can only be collected for specific, explicit and legitimate purposes and must not be further processed in any manner incompatible with those purposes. Further processing for archiving, scientific or historical research is permissible if certain requirements are met, in line with Article 89(1) of the GDPR.

   iii) Data minimisation.
   Personal data must be adequate, relevant and limited to what is necessary for processing.

iv) Accuracy.

Personal data must be adequate and, where necessary, kept up to date. If necessary, it should be erased or rectified without delay.

v) Storage limitation.

Personal data processed for any purpose must not be kept longer than is necessary for that purpose. GSA can store personal data for longer periods for archiving, scientific or historical research purposes if certain requirements are met, in line with Article 89(1) of the GDPR.

vi) Security and confidentiality.

Personal data must be stored in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6 DEFINITION OF PERSONAL DATA

1) Personal data is information about a living individual, who is identifiable from that information, or who could be identified from that information when combined with other data which GSA holds or is likely to obtain.

2) Personal data includes, *among others*,
   - names,
   - contact details,
   - photographs,
   - salary,
   - attendance records,
   - student marks and assessment records,
   - sickness absence,
   - leave,
   - dates of birth,
   - marital status,
   - personal email addresses,
   - online identifiers,
   - IP addresses, and
   - any expression of opinion or any intentions regarding a person.

3) The GDPR covers all personal data processed by GSA, irrespective of the location of the data, irrespective of who holds the personal data, whether, for example, by individual members of staff in their own separate files (including those held anywhere outside the GSA campus) or in Schools/Professional Support areas records or centrally by GSA.

4) The GDPR also covers "special categories" of personal data. These include, *among others,* particularly sensitive personal information such as
   - health details,
   - racial or ethnic origin, and
   - religious beliefs.

5) There are also types of sensitive personal data, which while not deemed as 'special category', disclosure may cause significant harm or distress. Examples are
   - bank account details,
   - national insurance number,
   - identity documents,
   - criminal convictions or offences; and
   - date of birth.

6) Data relating to these special categories must only be processed under the limited conditions specified in the GDPR.

7 GENERAL

1) GSA is responsible for ensuring and demonstrating compliance with the GDPR in general and the six data protection principles (section 5 above) in particular. This is known as the *Accountability* obligation.

2) Compliance with the GDPR and adhering to the six principles is the responsibility of GSA, all of its staff, members of the Board of Governors and students.

3) GSA is required to keep a record of its data processing activities as a summary of the processing and sharing of personal information, and the retention protocols and security measures which are in place.

8 KEY CONSIDERATIONS

Before embarking on any processing of personal data, whether by way of sharing personal data with a third party, using a new online tool, marketing a new programme or any other action that involves the use of personal data, the following issues should be addressed.

1) Does GSA really need to record the information?

2) Could anonymised or pseudonymised data be used?

3) Does GSA have a valid justification for processing the data, i.e. is it required for a contract, or has the data subject given their consent?

4) Has the data subject been informed about the processing, i.e. has a privacy notice been issued?

5) Is GSA authorised to collect/store/process the personal data?

6) Has GSA checked with the data subject that the personal data is accurate?

7) Is GSA sure that the personal data will be secure during the process?

8) Is GSA planning to pass personal data on to a third party or transfer the personal data outside the EU? If so, does it have the necessary contract(s) in place to do this or can it otherwise transfer the personal data in compliance with GDPR?

9) If GSA is setting up new systems/processes, have the Data Protection by Design and the Data Protection Impact Assessment (DPIA) guidelines been followed?

10) Are there alternative means by which the same objective can be achieved without using or sharing personal data?

9 DATA SECURITY

1) GSA, its staff, members of the Board of Governors and students, must ensure that all personal data which is held is kept securely (either by using appropriate IT equipment/security measures or – exceptionally – by physical storage means).

2) They must attempt to ensure that personal data is not disclosed to any unauthorised party, internal or external, accidentally, carelessly, negligently or deliberately.

3) Personal data which is held within the GSA central Student Records System will be accessible to relevant staff to process on a regular basis. This personal data must only be processed in accordance with the provisions of this policy.

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

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

6) The responsibility for ensuring that personal data is securely protected rests with the individual handling the data. Further information and advice in relation to methods of secure IT storage/transfer can be obtained from GSA's IT Department.

7) Unauthorised disclosure of personal data constitutes a breach of the GDPR and may also lead to disciplinary proceedings. Individuals may also face criminal proceedings for a serious breach of the provisions of the GDPR or if they knowingly or recklessly obtain and/or disclose personal data without the GSA's consent i.e. for their own purposes, which are outside the legitimate purposes of GSA.

10 DATA RETENTION

1) Schools and Professional Support areas in GSA are responsible for ensuring the appropriate retention periods for the personal data they hold and manage, based on GSA's Records Management Policy, referred to in section 4 above.

2) Retention periods will be set based on legal and regulatory requirements, sector and good practice guidance.

3) Personal data must only be kept for the length of time necessary to perform the processing for which it was collected.

4) Once personal data is no longer required it should be disposed of securely.

5) Paper records should be shredded or disposed of in confidential waste.

6) Electronic records should be deleted permanently or, if this is not possible from a technical perspective, put beyond use. You should contact the IT Department if you have any queries on this point.

7) If personal data is fully anonymised there are no time limits on storage from a data protection perspective.

11 OVERVIEW OF ROLES, RESPONSIBILITIES, AND RELATIONSHIPS

GSA has defined a management responsibility structure regarding data protection in general, and within that GDPR in particular, that aligns with its institutional Strategic Plan, (current version 2015-2018) and to other important obligations, such as equality.

The core roles are set out below:

a. Board of Governors

The Board must assure itself that GSA is compliant with the GDPR. The Board will receive and consider independent reports from the Data Protection Officer (DPO) on this matter, and management reports from the Director of GSA (as part of the normal Board-Management relationship).

b. Director of GSA

The Director of GSA is responsible for providing leadership and ensuring institutional compliance with the GDPR. The Director is responsible for receiving and considering formal compliance reports from his direct reports regarding compliance within their respective remits.

c. Senior Officers

The following officers are responsible, on behalf of the Director, for compliance with the GDPR regarding their respective remits:

- Deputy Director (Academic)
- Deputy Director (Innovation)
- Director of Development
- Director of Finance and Resources
- Director of Strategy and Marketing
- Registrar and Secretary

d. Data Protection Officer

In summary, the purpose of the Data Protection Officer (DPO) role is to provide information, guidance, and advice to GSA, and to report independently to the Board of Governors on GSA's compliance with all aspects of the GDPR. The role of the DPO is not to undertake or ensure local delivery; that rests with the aforementioned senior staff who are line managed by the Director of GSA (see section 11c above).

GSA must:

i) ensure that the DPO reports directly to the highest management level of GSA (i.e. the Board of Governors).

ii) ensure that the DPO does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by GSA for performing his or her tasks.

iii) support the DPO in performing the tasks of the role by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

iv) ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

v) ensure that the tasks and duties of the DPO do not result in a conflict of interests.

The role of DPO does **not** include the provision of legal advice on GDPR issues – that responsibility rests with GSA's solicitors.

e. Data Protection Forum and Data Protection Co-ordinators

In order to facilitate the continuing mainstreaming of GDPR, and in line with a recent Internal Audit observation on this matter, GSA has established a Data Protection Forum. The main aims of this Forum are to cultivate local delivery and accountability, and also to promote effective communication, on GDPR issues.

By default, membership of the Data Protection Forum shall take the form of each of the responsible officers (i.e. those senior staff line managed by the Director, (see section 11 c above) and the Data Protection Officer. However, each responsible officer is encouraged to nominate, normally, up to two Data Protection Co-ordinators for their overall area of responsibility to attend on their behalf. The advantage of having two for each area is that it would provide absence or holiday cover and would also encourage local discussion of relevant aspects of GDPR outwith the Forum. Local Data Protection Co-ordinators would be expected to meet with their respective responsible officer regularly, as this would ensure senior ownership, engagement, and accountability.

Each local Data Protection Co-ordinator would support their respective responsible officer by undertaking the following duties:

a. Be the first point of contact on GDPR issues within the respective responsible officer's area of responsibility.

b. Liaise with, collaborate with and consult the DPO on all necessary GDPR issues, including training, guidance and assistance on GDPR issues (including potential breaches of the GDPR), all as provided for elsewhere in this policy.

c. Assist staff and students in the completion and delivery of necessary GDPR forms, requests etc., as provided for elsewhere in this policy.

d. Attend regular meetings of the Data Protection Forum to receive and consider, in the first instance, all Privacy Notices, and any proposed amendments (or not, as the case may be), before submitting them to the Executive Group for approval.

e. To attend regular meetings of the Data Protection Forum, to consider any issues arising from points a, b, c and d, above and any other relevant issues in relation to the routine operation of, and compliance with, the GDPR in general, and this policy in particular.

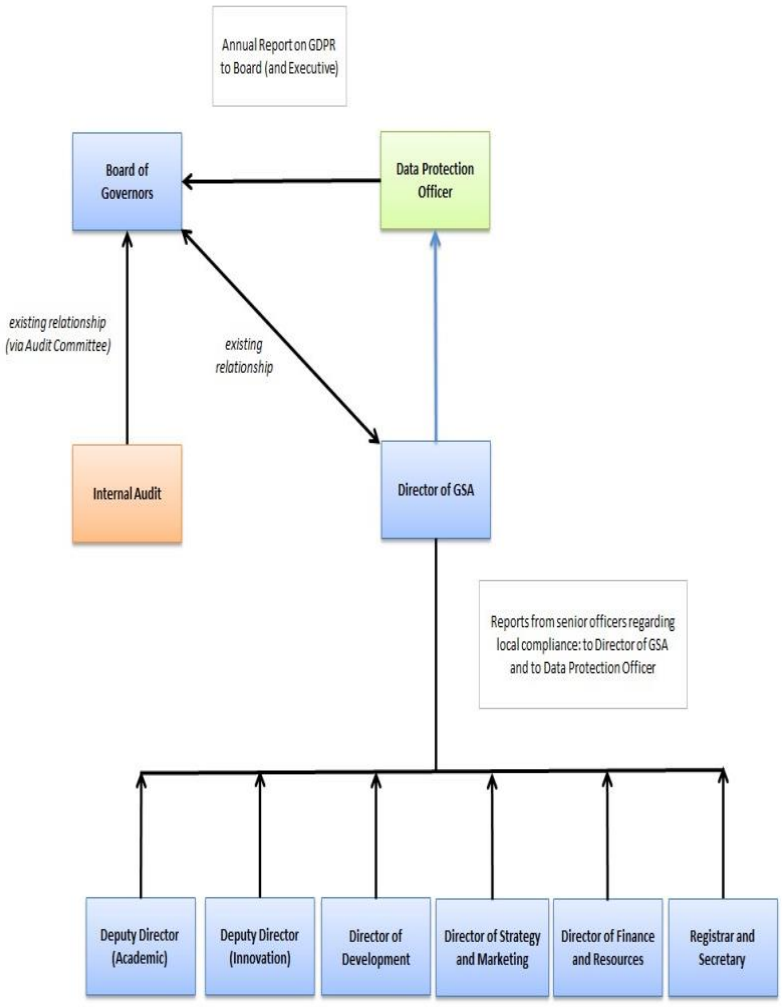
It is anticipated that the Data Protection Forum will meet monthly, in the first instance, progressing to quarterly meetings as GSA's approach to GDPR develops and matures.

f. Internal Audit

Acting in conjunction with the Director of GSA, the Registrar and Secretary set in place Internal Audit procedures for 2017/18. These were approved by the Audit Committee. Annual Internal Audit reviews of GDPR operation and compliance, at least for the period up to an including 2019/20, will be necessary in order to inform the DPO's report to the Board of Governors.

g. Reporting and Review Relationships

The diagram below illustrates the principal GDPR reporting and review relationships.



h. Annual Reporting Protocols

The nature and timing of the annual reporting shall be determined by the Board of Governors on the advice of the DPO but is likely to be considered at the December Board meeting. The basic sequence of the senior staff, line-managed by the Director submitting formal reports to the Director and the DPO, should be followed. The DPO would then provide an independent annual report to the Board of Governors. The report will also be submitted to the Executive Group.

i. DP Officer Annual Report

For the annual report in 2018 from the DPO, each senior officer with responsibility for a School or Professional Support area will submit to the DPO:

a. a formal statement confirming that the 2017/18 Audit, Gap Analysis and Treatment Plan Exercise has taken place,
b. a Record of Processing Activities from each area and together with a statement confirming that it is accurate,
c. a commentary and/or justification for any changes, proposed or implemented, and

d. if relevant, a statement that any Privacy Notices are being developed/reviewed.

For 2018 this formal statement should be submitted by 25 May. Post 2018 submissions should be made by 31 May each year.

12 GSA'S APPROACH TO GDPR AND EVIDENCE OF COMPLIANCE

1) GSA has adopted a mainstreaming approach to GDPR compliance, whereby both local and central ownership and compliance are regarded as equally important in enabling GSA to meet its obligations. Further, GSA has used the *accountability* requirement in the GDPR as a way of framing its preparations i.e. GSA must demonstrate that it is compliant. It is not enough simply to comply with the provisions of the GDPR – GSA must be able to demonstrate cross-institutional compliance.

2) GSA, and each of its constituent Schools and Professional Support areas, will ensure the prompt and timely provision of evidence, that, *among others*:

   a. GSA policy and guidance has been observed, centrally and in local areas.

   b. entry-level on-line training is available to all staff.

   c. legal advice has been adhered to, centrally and in local areas.

   d. regular training has taken place and guidance is provided and is being implemented.

   e. an up-to-date record of processing activities is in place in local areas and should be available, for example, to GSA's Internal Auditors upon request.

f. local-level audit, gap analysis and treatment plan exercises are undertaken and followed by appropriate action. This should be kept up-to-date and should be available to, for example, GSA's Internal Auditors upon request.

g. good record keeping is in place in central and local areas.

h. appropriate organisation and technological measures are in place to ensure the security and integrity of data.

i. Data Protection Impact Assessments/Privacy Impact Assessments are used appropriately.

j. due diligence with suppliers is undertaken.

k. appropriate internal policies are in place and are communicated to staff and students.

l. appropriate contractual arrangements are in place with third parties.

m. annual independent Internal Audits are undertaken and followed by appropriate action.

n. the DPO has direct engagement with senior levels of management.

o. the Board of Governors and Executive Group have received regular and relevant formal updates in the build up to the GDPR coming into place.

p. Responsible officers are up-to-date regarding compliance, and any challenges, within their areas, and engage with the Director of GSA or DPO as appropriate.

3) GSA must align with the accountability and privacy by design requirements of the GDPR (as described in section 31 below).

4) GSA has an obligation to implement technical and organisational measures to demonstrate that GSA has considered and integrated data protection into its processing activities.

5) Such measures are designed to minimise the risk of breaches and uphold the protection of personal data. Core elements include, *among others*,

a. Raising awareness across GSA and provision of ongoing GDPR training;

b. Monitoring of guidance from the ICO;

c. Keeping and maintain a record of its processing activities;

d. Revising relevant policy provisions;

e. Comprehensive data audits, both locally and centrally;

f. Adoption of and adherence to privacy by design principles;

g. Demonstrating that data usage content is freely given, specific, informed and unambiguous;

h. Provision of Privacy Notices explaining data use, retention, and the complaints model;

i. Utilising policy-embedded Data Protection Impact Assessments (or Privacy Impact Assessments) for certain key business decisions;

j. Ensuring that Data Sharing Agreements and international transfers must be reviewed to guarantee compliance;

k. Enabling the Right to be Forgotten of data subjects;

l. Enabling the Right to Restrict Process of data subjects;

m. Enabling the Right of Portability of Data for data subjects;

n. Providing special protection for the data of children, including obtaining parental consent;

o. Ensuring effective communication between the DPO and the DP Co-ordinators; and

p. Ensuring that the DPO reports to the highest levels of GSA.

6) GSA's Schools and Professional Support areas must submit an initial action plan and supporting documentation (e.g. audits, gap analyses, treatment plans, Privacy Notices for GDPR compliance) to the DPO by 25 May 2018. Privacy Notices must be drafted in accordance with the advice received from GSA's solicitors. The above documentation should be submitted with the approval of their respective responsible officer.

7) GSA's Schools and Professional Support areas must review the above action plan and supporting documentation, annually, by submitting an annual return, to ensure that they continue to align with the accountability and privacy by design requirements of the GDPR. This should be submitted to the DPO with the approval of their respective responsible officer.

8) The documentation will be made available to GSA's internal auditors, GSA's DPO, and, if appropriate or necessary, the ICO.

9) All Schools and Professional Support areas will be reviewed against the submissions made by the local DP Co-ordinator and the respective responsible officer as part of the normal management structure.

10) The Director of GSA will review local GDPR progress with the respective responsible officers who report directly to him. This will normally take place through monthly, scheduled, update meetings and also as part of the annual Career Review process.

11) The DPO will review local GDPR compliance against each annual action plan and any request(s) for further training, so that a report can be made to the Director and the Board of Governors on the level of compliance, indicated by the returns, and on the training and guidance necessary to maintain or improve GSA's position.

13 DATA PROTECTION TRAINING AND GUIDANCE

1) As part of its preparations for GDPR, GSA commissioned three sets of briefing and development sessions from its solicitors. A series of *Stage One Briefing Sessions* for members of the Executive Group and their respective Senior Management Teams set out a detailed introduction to GDPR and its obligations.

2) A subsequent series of *Stage Two and Stage Three Development Sessions* for data protection teams in each of the Schools and Professional Support areas provided a detailed explanation of the Audit-Gap Treatment exercise that each team would be asked to address.

3) After Schools and Professional Support areas have completed their Audit-Gap-Treatment exercise, the Head of Department or Head of School will then discuss the outcomes with their respective senior officer who will review any training or guidance needs and sign-off an appropriate request to the DPO.

4) The DPO will use this information to assess the overall training and guidance needs of GSA and will prepare a plan to address this which will be informed by the feedback from the Data Protection Forum, on an annual basis.

5) Post 25 May 2018, it is anticipated that a series of *Enhancement Clinics* will be offered to the DPO and local Data Protection Co-ordinators. These will be delivered by GSA's solicitors. Following these sessions DPO and the local DP Co-ordinators will liaise in the rolling out of further training events and exercises for all staff.

6) On-line general-principles data protection training has also been made available to all staff from May 2018.

14 CONTACT WITH AUTHORITIES

1) The responsibility for communicating with any external authority, such as the ICO for example, in all matters relating to the GDPR rests with the DPO. Specifically, in GSA, the responsibility of reporting breaches of the GDPR rests with the DPO.

2) Any individual receiving any GDPR related communication from any external authority must report the communication to the DPO at the earliest available opportunity. Such an individual must not respond to that communication, beyond a brief acknowledgement, and/or confirmation that the communication has been passed to the DPO.

PART II: PROCESSES and PROCEDURES

15 PROCESSING

1) Under the GDPR, processing is any operation or set of operations carried out by GSA or others on personal data including:

   a) recording,
   b) organisation,
   c) storage,
   d) adaption or alteration,
   e) retrieval,
   f) consultation, disclosure by transmission,
   g) dissemination, and
   h) erasure or destruction.

16 LEGITIMATE INTEREST AND BALANCING TEST

1) GSA must be able to identify the legal basis on which it is relying on to process personal data for each purpose.

2) There are broadly 6 legal bases which GSA can seek to rely on to process personal data. These include:
   (a) consent
   (b) where it is necessary to perform a contract or for taking steps to enter into a contract with the data subject
   (c) where it is necessary to comply with a legal obligation
   (d) where it is necessary to protect vital interest of the data subject or another person
   (e) where it is necessary to carry out a task in the public interest or in the exercise of official authority vested in GSA or
   (f) where it is necessary for the purpose of the legitimate interests of GSA.

3) In terms of the GDPR, legitimate interest can be defined, as the "processing of personal data if this is necessary for legitimate interests pursued by an organisation or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".

4) Organisations wishing to rely on this "catch all" processing basis must establish and be able to demonstrate what this legitimate interest is and it must undertake what is known as the Legitimate Interest Test.

5) The "legitimate interest" basis for processing personal data is **not** usually available to GSA, as a public authority, in the performance of its core activities as public tasks.

6) Exceptionally, it may be possible for GSA to use legitimate interest for data processing that is undertaken outwith GSA's public tasks. Generally, public tasks are those that are imposed on GSA by an enactment or are part of its official authority – for such tasks GSA would normally look to rely on Art 6(1)(e) – tasks in the public interest/official authority base to legitimise such processing. Thus, if GSA is processing personal data for a purpose which is not a 'public task', it may consider the legitimate interest base to legitimise such processing activity. Before relying on this basis, a legitimate interest test must be undertaken and documented. This involves consideration of:

a. What is the legitimate interest pursued by GSA?

GDPR does not define what factors to take into account when deciding if a legitimate interest is being pursued. Legitimate interest means that either GSA or a third party has a clear, specific and legitimate benefit or outcome in mind. Organisations must demonstrate what they are trying to achieve with the particular processing operation and this can include commercial interests or broader societal benefits.

b. Is the processing necessary for that purpose?

This means the processing must be a targeted and proportionate way of achieving your purpose and there is no less intrusive alternative. If you can achieve your objective in a less intrusive way, the processing will not be deemed necessary.

c. Do the individual's interests override GSA's legitimate interest?

GSA must take into account 'the interests or fundamental rights and freedoms of the data subject which require the protection of personal data' and check that they do not override GSA's interests. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override GSA's legitimate interest.

GSA must be able to satisfy all three parts of the test prior to commencing the processing.

The basis for relying on the legitimate interest justification must be made out by the relevant esponsible officer (i.e. who reports to the Director) and must be entered in the relevant Record of Processing Activities.

7) Appropriate records must be kept and this "interest" must be evaluated and reviewed on an evolving basis by those relying on and applying the justification to ensure it continues to justify processing personal data.

8) Before GSA can rely on the exceptional legitimate interest basis, it must seek to identify whether processing can be justified under a different basis and this exercise must be evidenced and retained for review by the Internal Auditors.

17 PRIVACY NOTICES

1) Under the "fair and transparent" requirements of the first data protection principle, GSA is obliged to provide data subjects with a Privacy Notice to let them know what GSA is doing with their personal data.

2) If GSA is conducting an activity which is not covered by the respective Human Resources and Academic Registry Privacy Notices, a separate Privacy Notice will require to be provided when the personal data is collected.

3) A Privacy Notice should include the following information:

a) The identity and contact details of GSA or any other partner organisations and the contact details of the DPO, and the local DP Co-ordinator, the latter being noted as the first point of contact,

b) The purpose(s) for which the data will be used,

c) The legal basis for processing, i.e. fulfilment of student or staff contact. Where the basis is legitimate interests, the legitimate interest must be stated. Where it is based on contract or statutory requirements, GSA needs to confirm what would happen if the information is not provided,

d) The identity of other people or organisations who may have access to the data,

e) Details of any transfers of data outside the EU,

f) The retention period of the data or, if this is not possible, the criteria used to set this,

g) The right to access the data, ask us to rectify data, restrict processing of data, to object to processing, ask us to transfer or 'port' their data to the data subject or a third party, or to withdraw consent,

h) The right to complain to the ICO,

i) Details of automating decision-making or profiling where applicable, and

j) The source of the personal data if the data was not collected from the data subject.

4) A Privacy Notice template is published on GSA's GDPR website.

5) If a Privacy Notice is being prepared in respect of a new activity which could have an impact on the privacy of the individual(s) concerned, consideration should be given to carrying out a Data Protection Impact Assessment (DPIA) – see section 30 below.

6) All Privacy Notices, initiated locally with the consent of the relevant senior officer, must be submitted to the DPO for consideration and evaluation by the Data Protection Forum in the first instance, before referring them to GSA's solicitors for advice and then submitting them to the Executive Group for formal approval.

7) Privacy Notices must be reviewed, at least annually, or when circumstances change, and submitted to the Data Protection Forum, with the consent of the relevant senior officer, together with a statement for the rationale for any amendments or not, as the case may be. The Data Protection Forum will consider and evaluate any proposed amendments, before referring them to GSA's solicitors for advice, and submitting the amended Privacy Notice to the Executive Group for approval.

8) The DPO is responsible for ensuring that the Register of Privacy Notices is both accurate and current at all times.

18 RECORDS OF PROCESSING ACTIVITIES

1) For the purposes of the GDPR, GSA is a data controller.

2) A data controller is an organisation, person or other body, other than the data subject, which alone or jointly with others, determines the purpose and means of processing personal data.

3) As a data controller, GSA is required to maintain a record of processing activities which covers **all** the processing of personal data carried out by GSA. Each School of Professional Support area must have a record of individual processes which is confirmed annually, by 31 May, and identifies and justifies any substantial change(s) in its processing activities.

4) This record must contain details of:

   a) the reason(s) for processing the personal data,
   b) the types of individuals about whom data is held,
   c) the type of personal data being processed,
   d) with whom the personal data is shared,
   e) when personal data is transferred to countries outside the EU,
   f) how long GSA will retain the personal data for, and
   g) where possible, a general description of the technical and organisational security measures adopted to keep the personal data secure.

5) GSA's overall Records of Processing Activities (which is a collation of those submitted by Schools and Professional Support areas) covers three categories of data subjects:

   a) Staff data (including job applicants, previous staff, honorary, emeritus and visiting staff),

   b) Student data (including potential, current and former), and

   c) Data subjects other than staff, students (potential, current and former) and former employees. Members of the Board of Governors are included in this category.

6) Staff embarking on new activities involving the use of personal data which is not covered by one of the existing Records of Processing Activities should inform the local DP Co-ordinator before starting the new activity.

19 CONSENT AND CONSENT WITHDRAWAL

1) Under the GDPR, in order to process personal data, GSA must satisfy at least one of the following conditions:

   a) The data subject has given his or her consent,

   b) The processing is required under a contract with the individual, or is necessary to take steps at the request of the data subject prior to entering into the contract,

   c) It is necessary to fulfil a legal obligation,

d) It is necessary to protect someone's vital interests (i.e. a life or death situation),

e) It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller,

f) It is necessary for the legitimate interests of the data controller or a third party and does not interfere with the rights and freedoms of the data subject (this condition cannot be used by a public authority such as GSA in the performance of its public tasks – see section 16 above).

2) All processing of personal data carried out by GSA must meet one or more of the conditions in section 19.1 above.

3) In addition, the processing of "special categories" of personal data (section 6.4 above) requires extra more stringent conditions to be met.

4) Under the GDPR, GSA is classified as a public authority and as such GSA is not encouraged to use consent for core activities due to the imbalance in the relationship between the data controller and the data subject.

5) Consent can only be used where there is no other lawful basis for processing personal data.

6) Where possible, GSA should identify alternative justifications for processing personal data which would normally be contract (19.1.b above) or official authority (19.1.e above). The relevant part of the contract or the official authority should be clearly identified.

7) Consent is defined in the GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes, by which he or she, by statement or other clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

8) The GDPR specifically states that silence, pre-ticked boxes or inactivity do not constitute consent.

9) Consent that has been obtained must be documented to include details of what the data subjects were told and when and how they consented.

10) A data subject who has provided consent has the right to withdraw their consent at any time.

11) They must be told of their right to withdraw their consent and how to do this. It must be easy and straight-forward for a data subject to withdraw his or her consent.

20 CHILDREN

1) For the purposes of the GDPR, a child is defined as anyone under the age of 13 where the data controller provides an information society service (i.e. a paid for service online) aimed directly at children. For all other purposes, a child is deemed as anyone under the age of 12 in Scotland.

2) The following restrictions apply to the processing of personal information relating to children:

   a. Online services offered directly to children require parental consent from those under the age of 13.

   b. Any information provided to a child in relation to their rights as a data subject has to be concise, transparent, intelligible and easily accessible, using clear and plain language.

   c. The use of child data for marketing or for profiling requires specific protection.

   The local Data Protection Co-ordinator must be consulted in the first instance, if any of the above activities are being contemplated. In any event, even where the processing does not involve a child under 12 or 13 but between the ages of 13 and 16, GSA's practice is to obtain parental consent as good practice.

21 RESEARCH

1) Before personal data is obtained or used, each research project or proposed project must have a written Data Protection Impact Assessment in place. This must be reviewed and signed-off, if the assessment is suitable, by the relevant Head of School or the Head of Research and Enterprise on behalf of the Deputy Director (Academic). This documentation must be retained locally and be made available to the Internal Auditors or other such authorised parties upon request. Initial guidance may be sought from the local Data Protection Co-ordinator.

2) The Head of Research may, in due course, design a standard template for the above.

3) Personal Data used for research purposes by GSA staff must be dealt with in accordance with GDPR and its Data Protection Principles. This is subject to the limited exemptions discussed in more detail below. This section outlines the considerations and responsibilities of those conducting research involving personal data in the context of the six Data Protection Principles.

4) The GDPR clarifies that scientific research should be interpreted in a broad manner including privately funded research as well as studies carried out in the public interest. In order for processing to be considered statistical in nature the result of processing should not be "personal data but aggregate data" and should not be used to support measures or decisions regarding a particular individual. For information about what is defined as personal data or 'special categories' of personal data see section 6 of this policy on Personal Data.

5) In addition to meeting GDPR requirements, research that involves personal data must still meet the relevant ethical approval procedures.

6) When using personal data in research it is always best to use anonymised data if possible. However, the level of anonymisation must be such that it is impossible to identify any living individual from the information concerned or in combination with any other information that GSA holds or is likely to hold – something which is difficult to achieve. If personal data is suitably anonymised, then it is outwith the scope of the GDPR.

7) Where full anonymisation is not possible then another option is pseudonymisation where the identity of an individual is disguised for instance by replacing identifying fields with artificial identifiers or pseudonyms. When data has been pseudonymised it still retains a level of detail which allows tracking back of the data to its original state. This is in contrast to anonymised data where reverse compilation should be impossible.

8) The GDPR emphasises that anonymisation or pseudonymisation should be used where ever possible particularly in relation to historical or scientific research or for statistical purposes.

The next few paragraphs lay out the research considerations in relation to the data protection principles.

9) Principle 1: Personal data shall be processed lawfully, fairly and in a transparent manner.

Lawfully

Certain conditions as set out in Article 6 of the regulations must be met before personal data can be processed lawfully. As far as GSA research is concerned the most likely legal basis for processing personal data will be that it is 'necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'. Whilst many research participants will be asked to consent to participating in the research from an ethical/confidentiality perspective, it is unlikely that consent will be an appropriate legal basis in relation to GDPR. This is because consent has to be capable of being withdrawn. In most research projects, once the analysis of data is underway and results are published it would not be feasible to extract the personal data relating to an individual following the withdrawal of consent. In addition, research data often gets reused for subsequent research and it is unlikely that consent would be obtainable for this.

When the research involves the use of special categories/sensitive personal data a justification under Article 9 of the GDPR needs to be identified. For research purposes it is likely that Article 9(2)(j) 'public interest, scientific or historical research purposes or statistical purposes' can be used. However, for special categories/sensitive personal data further restrictions apply and additional safeguards should be in place to ensure respect for the principle of data minimisation such as pseudonymisation. For further information about the types of safeguards that can be used see section 12 on Data Protection by Design and Default.

Fair and Transparent

Under the "fair and transparent processing" requirements of the GDPR, researchers also need to provide a project-specific Privacy Notice to research participants at the time their personal information is initially collected from them. This Privacy Notice can be combined with a consent form for participating in the research but it should be clear that once they have agreed to participate in the research, consent will not be the legal basis for processing their personal data. For information about what should be included in a Privacy Notice please see sections 17 and 19 of this policy on Privacy Notices and Consent.

In some cases, the researcher may be using personal data obtained from a third party, rather than directly from the data subject. In such cases a Privacy Notice should still be provided, unless it has been provided by another party (e.g. a research partner) or it can be proved that providing such would be impossible, involve disproportionate effort on the part of the researcher, or that providing the notice would likely render the research impossible or seriously impair the achievement of the research objectives.

In deciding whether the disproportionate effort argument applies, researchers should evaluate the time, cost and ease of providing the subject with the notice against the benefit to the subject of receiving the notice (or prejudice in not receiving it). Factors to consider in this assessment would include the size of the sample, whether up-to date contact details are available and if not, how easy or practical it would be to obtain them, the purpose of the research and its likely effect on the individuals concerned.

10) Principle 2: Purpose limitation.
Personal data shall be collected for specific, explicit and legitimate purposes, and not further processed in any manner incompatible with those purposes.

This principle goes on to state that further processing for archiving, scientific or historical research or statistical purposes is permissible. This is on the basis that the personal data is not used to support measures or decisions regarding any individual and that suitable safeguards have been put in place to keep the information secure.

11) Principle 3: Data Minimisation.
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which they are processed.

Researchers should only collect and process personal details which are necessary to conduct their research. For example, if personal identifiers such as names and addresses are not required in order to carry out the research, the respondent should not be asked for such information.

12) Principle 4: Accuracy.
Personal data shall be accurate and, where necessary, kept up to date.

Efforts should be made to ensure that personal data gathered for research purposes is accurate. In most research situations it will not be necessary to keep the personal information updated as the research will be based on information representing a situation at a particular moment in time.

13) Principle 5: Storage Limitation.
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary.

Personal information must be kept in a form which permits identification of data subjects for no longer than is necessary. However, there is an exemption for personal data stored for research purposes, provided adequate safeguards are put in place e.g. pseudonymisation, and appropriate technical and organisational measures are in place, e.g. the information is stored securely.

14) Principle 6: Integrity and Confidentiality.
Appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures.

Researchers must employ measures appropriate to the sensitivity of the data held to ensure that personal data is kept securely. They should ensure that:

- Personal data held on computer is protected through appropriate access restriction and password protection controls. Digitised personal data should only be stored on shared network drives or GSA authorised, secure offsite storage (such as Box) and not offline or on local drives.

- Personal data held manually is stored in locked cabinets and offices to prevent accidental or deliberate access by third parties.

- Personal data held off site (e.g. at home or travelling) receives the same level of security protection as it would in the office.

- Personal data is disposed of appropriately once research has been completed. For paper files this will mean disposal in confidential waste sacks for low level personal data, or cross shredding for sensitive personal data. For data held electronically steps should be taken to ensure data is permanently deleted or destroyed.

15) Transfers outside the EU

Transfers of personal data to recipients in countries outside the EU are regulated and restricted in certain circumstances. This needs to be taken into account where research involves international collaboration and, in the course of that collaboration, personal data will be transferred to a country outside of the EU. In most cases explicit consent for the data transfer will be required from participants. There are some occasions when personal data can be transferred to countries which do not offer an adequate level of protection which include public health research. For more information, see section 27 of this policy on Transfers of Personal Data outside the EU.

16) Data Subject Rights

Research participants generally have the same rights as other data subjects; for more information about these rights - see section 36 of this policy, however, there are some exemptions relating to research. There is an exemption from the right to erasure if it would render impossible or seriously impair the achievement of the research objectives. Likewise, there is an exemption from the right to object to processing if the processing is being carried out in the public interest.

17) Data Protection Impact Assessment

Researchers will need to carry out a Data Protection Impact Assessment if the research could result in a high risk to the rights and freedoms of individuals. This is particularly relevant where research involves a systematic and extensive evaluation of personal aspects relating to individuals and which is based on automated processing, including profiling and which could involve a legal or significant effect on the individual. For further information about when and how to do a DPIA, see section 28 of this policy on Data Protection Impact Assessments.

22 DATA SHARING

1) Prior to any data sharing proposal being considered, the DPO and the owner of the original data must be consulted with a view to obtaining their approval to the proposal being taken forward in the first instance.

2) Once the above consultation has taken place, the data sharing proposal must be signed-off by the relevant responsible officer, who must be a direct report of the Director of GSA.

3) Certain conditions need to be met before personal data can be shared with a third party or before an external data processor is used to process data on behalf of GSA.

4) As a general rule personal data should not be passed on to third parties, particularly if it involves special categories of personal data but there are certain circumstances when it is permissible.

5) Any transfer of personal data must meet the six data processing principles, in particular it must be lawful and fair to the data subjects concerned.

6) It must meet one of the conditions of processing. Legitimate reasons for transferring data would include:
   a) That it was a legal requirement
   b) It is necessary for the official core business of GSA.

7) If no other conditions are met, then consent must be obtained from the individuals concerned and appropriate privacy notices provided.

8) GSA must be satisfied that the third party will meet all the requirements of GDPR particularly in terms of holding the information securely.

9) Where a third party is processing personal data on behalf of GSA, a written contract **must** be in place.

10) A contract is also advisable when data is being shared for reasons other than data processing so GSA is assured that GDPR requirements are being honoured.

23 PERSONAL DATA FOR FIELD TRIPS

1) Please refer to the GSA's policy "Health and Safety in Fieldwork Procedure" approved by the Occupational Health and Safety Committee on 11 May 2016. Further advice may be available from GSA's Health and Safety Team.

24 REQUESTS FOR PERSONAL INFORMATION FROM THIRD PARTIES

1) GSA often receives requests for the personal information on its students and staff from third parties. This section is intended to provide advice to staff on how such requests should be handled to ensure compliance with GDPR.

2) GSA informs students and staff how their information will be used, and in what circumstances and to whom it may be disclosed, through the relevant student and staff privacy notices.

3) There are some third parties that can require disclosure of personal data, examples of these are:

   UK Funding Councils e.g. HEFCE HEFCW, SFC and their agents e.g. QAA, HESA, HEFCE auditors. Further and Higher Education Act, 1992 s.79

   Electoral registration officers
   Representation of the People Act 2000; The Representation of the People (Scotland) & (England and Wales) Regulations 2001

Officers of the Department of Works and Pensions, and Local Authorities

Health and Safety Executive
Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 1995 s.3

Audit Commission and related auditing bodies Audit Commission Act 1998 s.6

Environmental Health Officers
Public Health (Control of Disease) Act 1984 and the Public Health (Infectious Diseases) Regulations 1988

Child Support Agency (CSA) Child Support (Information, Evidence and Disclosure) Regulations 1992.

Inland Revenue
Taxes Management Act 1970

Police Officers
With a Court Order/warrant

Other third parties
With a Court Order

4) GSA should **not** process personal information of individuals in ways that are not covered by GSA privacy notices, without establishing a lawful basis.

5) As a general rule, personal data should **never** be disclosed to anyone other than a GSA employee with a legitimate work interest in the information, without written consent from the data subject.

6) Requests from parents, friends or relatives

There must be no release of personal data without the explicit consent of the student. It is acceptable to advise them that GSA will accept a message and, if having checked GSA records and such a person exists, will pass it on. This avoids disclosing any information about the student, including whether or not they are at GSA.

7) Requests from organisations providing financial support.

GSA routinely notifies public funding bodies and the Student Loans Company of changes to a student's status. These disclosures are covered in GSA's privacy notices and records of processing activities. Records should not be disclosed to organisations that are not covered in GSA's privacy notices (e.g. private funders) without written evidence of student consent.

8) Requests from Home Office/Immigration and Nationality Directorate/UK Visas.

GSA often receives requests for information on attendance and other details relating to international students. Information should only be disclosed where GSA is satisfied there is a legal requirement to provide the requested information or the individual concerned has given their consent.

9) Requests from the police or law enforcement officials.

GSA is not legally obliged to provide information to the police, unless presented with a court order or warrant. However, GSA may choose to release information where the police, or other law enforcement agencies, can demonstrate to GSA's satisfaction that non-release would be likely to prejudice the prevention/detection of crime or apprehension/prosecution of offenders. GSA aims to support police investigations where possible. However, GSA is obliged to manage personal information in accordance with the GDPR.

Requests from the police should:

- be in writing,
- be signed and counter signed, the latter by a senior officer
- be for specific information about a specific individual. While this may not always be the case, the information requested should be relevant and limited, state that the personal data requested is required for the stated purposes and that failure to provide the information will, in their opinion, be likely to prejudice the investigation.

The local Data Protection Co-ordinator should be informed when such requests have been received and they may wish, in some circumstances, to consult the DP Officer.

Documentation relating to the request, and the release of information (should that follow), should be retained locally and be made available to the Internal Auditors or other such authorised parties upon request. A copy should be sent to the DPO.

10) Disclosures required by law

There are circumstances where GSA is legally obliged to disclose information about an individual to a third party if this is required by statute or court order. GSA must ensure that any legal obligation (details of legislation and relevant section) is correctly described by the requestor in writing.

All such requests should be referred to the local Data Protection Co-ordinator for advice and validation, in the first instance. The Data Protection Co-ordinator may wish, in some circumstances, to consult the DPO.

Documentation relating to the request, and the release of information (should that follow), should be retained locally and be made available to the Internal Auditors or other such authorised parties upon request. A copy should be sent to the DP Officer.

11) Information provided for Council Tax purposes

GSA routinely provides the local Councils with details of current students for Council Tax exemption purposes. Students living outwith such Council areas may ask for certification for this purpose and GSA is legally obliged to provide them with this. Occasionally, students object to this processing and request that their details are not passed to the Council. They are entitled to do so under the GDPR, and GSA would be required to stop processing the information in this way unless it can be demonstrated that there are compelling legitimate grounds for processing which override the interests, rights and freedoms of the data subject.

Any objections to Council Tax related processing should be referred to the Academic Registry, who will take the matter forward.

Documentation relating to such a request must be lodged with the Academic Registry where it shall be retained and will be made available to the Internal Auditors or other such authorised parties upon request.

12) Information about deceased staff or students

The GDPR only applies to living individuals, thus a deceased staff or student's personal information may potentially be disclosed under the Freedom of Information (Scotland) Act 2002 (FOISA). However, in doing so GSA must ensure that the individual whose information is sought is in fact deceased and that disclosure does not infringe the data protection rights of any third parties (e.g. parents). There may also be an ongoing duty of confidentiality. No information should be released unless sufficient evidence of death is provided. Such evidence may include:

- Death certificate,
- Student or staff member already recorded as deceased on the records system,
- Notification of death in writing by next of kin,
- Obituary or confirmed newspaper report of death (but not if there are insufficient details to conclusively identify the student or staff member on the records system).

Details of relatives of a deceased student or staff member should not be disclosed.

Consideration should be given to the sensitivities of the deceased individual's family where a request for disclosure is sought in the immediate aftermath of a death (e.g. by the media). Advice should be sought from the local Data Protection Co-ordinator in such cases.

13) If it appears that the information may fall within the scope of one of the exemptions under the FOISA, please refer the matter to the local Data Protection Co-ordinator, in the first instance. The Data Protection Co-ordinator may, in some circumstances, wish to discuss the matters with the Academic Quality Office, which centrally receives and co-ordinates Freedom of Information requests at GSA.

25 REFERENCES FOR STAFF AND STUDENTS

1) GSA should not process personal information of individuals in ways that are not covered by GSA privacy notices, or without having a legal basis to do so.

2) As a general rule, personal data should **never** be disclosed to anyone other than a GSA employee with a legitimate work interest in the information, without consent.

3) Requests for references or confirming qualifications

The requestor should be advised that GSA requires explicit consent from the individual concerned before information can be released (in relation to students it is important not to confirm whether or not the student has attended GSA prior to consent being obtained). The consent must be in writing (letter or email) and include sufficient information (full name, address, date of birth, dates and subjects of study/areas or work) to allow GSA to identify them, and be satisfied as to their identity. A letter should be signed or, for a current student or member of staff, an email from their GSA email account will be sufficient evidence of identity. A qualification awarded by GSA and validated by the University of Glasgow should only be confirmed by the GSA Academic Registry.

4) In instances where the third party seeking information suspects an individual has falsely claimed to have a qualification from GSA, the matter should be referred to the GSA Academic Registry.

26 TRANSFERS OF PERSONAL DATA OUTSIDE OF THE EU

1) Personal data can only be transferred outside the EU if one of the following applies:

a) The EU has assessed the third country to have an adequate level of protection. The countries (or other entities) that currently fall into this category are Andorra, Argentina, Canada, Faroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay;

b) Appropriate safeguards are in place such as a legally-binding enforcement instrument, binding corporate rules are in place or the EU Commission standard data protection clauses are in place;

c) A court or tribunal requires the transfer;

d) The data subject has consented to the transfer having been informed of the possible risks of such transfers due to the absence of an adequacy decision and appropriate safeguards;

e) The transfer is necessary for the performance of a contract between the data subject and GSA, or the implementation of pre-contractual measures taken at the data subject's request;

f) The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between GSA and another organisation;

g) The transfer is necessary for important reasons of public interest;

h) The transfer is necessary for the establishment, exercise or defence of legal claims;

i) The transfer is necessary to protect the vital interests of an individual i.e. a life or death situation, where the data subject is physically or legally incapable of giving consent;

j) The transfer is made from a register which is open to the public.

2) Options (d), (e) and (f) are not available to GSA to legitimise the international transfer of personal data carried out by GSA in the exercise of its 'public powers'. GDPR does not define 'public powers', however it is likely that it involves the exercise of any powers provided to GSA under enactment.

3) Staff authorising transfers of personal data outside the EU are responsible for ensuring that one of the above requirements is met and ensuring that a record is kept of which condition has been met.

4) Where transfers are done on the basis of consent, evidence of the consent and when it was obtained should be kept.

5) For more advice on transfers of personal data outside the EU, the local Data Protection Co-ordinator should be consulted, in the first instance**.** The Data Protection Co-ordinator may, in some circumstances, wish to consult the DPO.

6) Once the above consultation has taken place, the data sharing proposal must be signed-off by the relevant responsible officer, who must be a direct report of the Director of GSA.

27 MANAGING SUB-CONTRACTED PROCESSING

1) Scope

All external suppliers (if any) who process personal data on behalf of GSA fall within the scope of this procedure.

2) Responsibilities

a) Responsible Officers (i.e. those senior staff reporting to the Director of GSA), in consultation with the DPO, are responsible for approving the selection of all sub-contracted processors of personal data in line with the requirements of this policy.

b) Responsible Officers, in consultation with the DPO, are responsible for ensuring that all external data processing is contracted out in line with this policy.

c) The Director of IT is responsible for ensuring that adequate technical support and other resources that might be required are made available to support GSA, as the relationship owner, in the monitoring and management of the relationship.

d) Responsible Officers, in consultation with the DPO, are responsible for carrying out regular audits of third party compliance.

3) Procedure.

The following general principles apply. Further information is available from the Procurement Office or in associated GSA Procurement policies.

1) GSA selects only suppliers who can provide the technical, physical and organisational security which meets all of GSA's requirements in terms of all of the personal data they will process on behalf of GSA.

2) GSA must have in place appropriate checks, to ensure that all contracts are reviewed, on a regular basis, to see if personal data is processed. These checks must be carried out even if the data processing activities are not the primary reason for the contract.

3) GSA must ensure that all the security arrangements are outlined in the contract with the external processor.

4) Suppliers from outside the EU (if none are available within the EU), will only be selected under the following conditions, in addition to any other conditions set out elsewhere in this policy:

   i. If the supplier or the state in which it is domiciled has been positively identified in an adequacy decision by the EU Commission, or

   ii. Where there are legally binding corporate rules or approved contractual clauses in place, and organisational and technical safeguards established between GSA and the supplier to secure the rights and freedoms of data subjects at least equal to those afforded in the EU, or

   iii. Where the arrangement has been approved by the ICO.

5) An information security risk assessment must be carried out before a supplier is engaged, or if the DPO considers it necessary because of the nature of the personal data to be processed or because of the particular circumstances of the processing an audit of the supplier's security arrangements may also be necessary before entering into the contract.

6) GSA must enter into a written contract with the supplier which complies with Article 28 of the GDPR and which require the supplier to provide appropriate security for the personal data it will process.

7) All data processing contracts must allow GSA to conduct regular audits of the supplier's security arrangements during the period which the supplier has access to the personal data.

8) All data processing contracts must forbid suppliers from using further subcontractors without GSA's written authorisation for the processing of personal data.

9) Where GSA permits a supplier to subcontract processing of personal data, the immediate supplier must prohibit the second-level contractor (or further down the chain) from subcontracting these processing operations without GSA's written permission.

10) Contracts with second-level subcontractors will only be approved if they require the subcontractors to comply with at least the same security and other provisions as the primary subcontracting organisation (the supplier) if they specify that when the contract is terminated, related personal data will either be destroyed or returned to GSA, and so on down the chain of sub-contracting.

28 DATA PROTECTION IMPACT ASSESSMENTS/PRIVACY IMPACT ASSESSMENTS

1) A Data Protection Impact Assessment (DPIA) is a process whereby potential privacy issues and risks are identified and examined from the perspective of all stakeholders and allows GSA to anticipate and address the likely impacts of new initiatives and put in place measures to minimise or reduce the risks. As the use of technology and the collection and storage of personal data grows, the need to ensure that it is properly managed and maintained increases.

2) It is a requirement of GDPR that a Data Protection Impact Assessment (DPIA) is carried out in certain circumstances. This section will explain when a DPIA has to be done, how it should be carried out, and what should be taken into consideration as part of the process.

3) The impact assessment covers not only the protection of personal data but broader privacy of individuals and therefore could also be referred to as a Privacy Impact Assessment (PIA).

4) The procedures in this section are designed to minimise the risk of harm that can be caused by the use or misuse of personal information by addressing data protection and privacy concerns at the design and development stage of a project.

5) Conducting a DPIA should benefit GSA by managing risks, avoiding unnecessary costs, avoiding damage to reputation, ensuring legal obligations are met and improving the relationship with stakeholders.

6) The term project is used in a broad and flexible way and means any plan or proposal. Examples of the types of projects that need a DPIA are:

    a) A new research project that involves data subjects.

    b) A new IT system storing and accessing personal data.

    c) A data sharing initiative where two or more organisations seek to pool or link sets of personal data.

    d) A proposal to identify people in a particular group or demographic and initiate a course of action (e.g. identifying students believed to be at risk).

    e) A new surveillance system such as CCTV.

    f) A new database which consolidates information held by separate parts of an organisation like GSA.

7) When does a DPIA need to be undertaken? A DPIA should be undertaken as part of the initial phase of a project and before any processing to ensure that risks are identified and taken into account before the problems become embedded in the design and causes higher costs due to making changes at a later stage. Also, if there is a change to the risk of processing for an existing project a review should be carried out. In the context of this guidance a project could include the development or enhancement of any activity, function or processing such as a system, database, programme, application, service or scheme. The time and effort put into carrying out the DPIA should be proportionate to the risks.

8) A DPIA does not have to be conducted as a completely separate exercise and it can be useful to consider privacy issues in a broader policy context such as information security. The DPIA does not necessarily need to start and finish before a project can progress further but it can run alongside the project development process provided it is carried out prior to processing.

9) The GDPR requires that a DPIA is carried out in the following cases:

   a) When the processing involves systematic and extensive evaluation of personal information particularly in cases of automatic processing or profiling where decisions are made that could have a significant or legal impact on an individual. Profiling is the processing of data to evaluate, analyse or predict behaviour or any feature of behaviour, preferences or identity.

   b) When processing on a large scale of special categories of data or data relating to criminal convictions and offences.

   c) The monitoring of a publicly accessible area on a large scale.

   d) Any other cases specified by the ICO (none currently specified).

   e) It is the responsibility of the person leading the project to carry out a DPIA and attain sign-off, through appropriate channels from the respective responsible officer (who reports directly to the Director of GSA). As part of the process the DPO must be consulted but it is not the DPO who carries out the DPIA.

   f) If the project includes the use of any personal data, then it should be started by completing the screening questions on the DPIA form (section 42e). If the answer to all these questions is 'No' then the remainder of the assessment does not need to be completed but the results from the screening questions should be sent to the DPO for recording.

   g) If the response to any of the screening questions is 'Yes', the remainder of the impact assessment form should be completed. Guidance notes are included at the end of the form to help the user ensure that the assessment is properly completed.

10) The assessment template is split into 8 sections:

   i. Project details – providing a broad overview of the project.

   ii. Details of personal data – providing details of the types of personal data that will be processed and the justification for this.

   iii. Description of information flows – how the data will be collected, used, stored and deleted.

   iv. Consultation requirements – detailing consultation with data subjects or other stakeholders.

   v. Identification of privacy and related risks – detailing potential risks.

   vi. Identification of privacy solutions – what will be done to mitigate the risks.

   vii. Sign off and record of outcomes – an authorised record of the proposed outcomes.

   viii. Integration of outcomes back into the project plan – detailing of timing and responsibility for each outcome.

11) For further information about building privacy into a project during the design stage please see section 29 below on Data Protection by Design and by Default.

12) Once the risks are identified, and outcomes and actions agreed, it is important that the project leader ensures that the necessary actions are implemented. As the project develops and is embedded the privacy risks should continue to be assessed to ensure that adequate protections remain in place.

13) Once the DPIA process has been completed the outcomes will be recorded in a register maintained by the DPO. The register will record each risk, explain what action has been taken or will be taken, and identify who is responsible for approving and implementing the solution.

29 DATA PROTECTION BY DESIGN AND DEFAULT

1) Data Protection by Design (also called Privacy by Design) is an approach to handling personal data that promotes privacy and data protection compliance from the start rather than considered as an afterthought.

2) All staff, members of the Board of Governors and agents of GSA are required to apply the data protection by design principles when developing a new project or reviewing existing projects that involves the use or storage of personal data.

3) The guidelines below explain the types of project where this might be relevant, what data protection by design is, and what measures can be put in place to protect personal data.

4) Under GDPR GSA has an obligation to consider data privacy during the initial design stages of a project as well as throughout the lifecycle of the relevant data processing. By imposing a specific 'privacy by design' requirement, the GDPR emphasises the need to implement appropriate technical and organisational measures to ensure that privacy and the protection of data is not an afterthought.

5) Examples of the types of projects where privacy should be considered include:

   a) Building new IT systems for storing or accessing personal data
   b) Developing policies or strategies that have privacy implications
   c) Embarking on a data sharing initiative
   d) Using data for new purposes
   e) Research Projects

6) This section explains the concept of 'data protection by design' and suggests factors that can be taken into consideration to ensure that the privacy of individuals is protected. This should be read in conjunction with section 28 on Data Protection Impact Assessments.

7) In addition to meeting legal requirements taking a proactive approach to privacy will reduce the likelihood of fines or financial losses due to data protection breaches and help build reputation and stakeholder confidence.

8) What is Privacy by Design? Privacy by Design is an approach to protecting privacy by embedding it into the design specifications of technologies, business practices and physical infrastructure. This means building in privacy during the design phase of any project.

9) Seven foundation principles of Privacy by Design were first developed by Dr Ann Cavoukian, Academic and Privacy Commissioner in Canada, in the 1990s. These can be summarised as:

a) Use proactive rather than reactive measures. Anticipate, identify and prevent privacy invasive events before they happen.

b) Privacy should be the default position. Personal data must be automatically protected in any system of business practice, with no action required by the individual to protect their privacy.

c) Privacy must be embedded and integrated into the design of systems and business practices.

d) All legitimate interests and objectives are accommodated in a positive-sum manner. Both privacy and security are important, and no unnecessary trade-offs need to be made to achieve both.

e) Security should be end-to-end throughout the entire lifecycle of the data. Data should be securely retained as needed and destroyed when no longer needed.

f) Visibility and transparency are maintained. Stakeholders should be assured that business practices and technologies are operating according to objectives and subject to independent verification.

g) Respect user privacy by keeping the interests of the individual uppermost with strong privacy defaults, appropriate notice and user-friendly options.

10) A Data Protection Impact Assessment (DPIA) (see section 28) should be carried out as part of the initial phase of a project or when an existing project is being reviewed. If data protection or privacy implications are identified, then measures should be built into the project during the early stages to ensure that risks to privacy are minimised or eliminated.

11) Below are some examples of measures that can be taken during the project development or review to protect the personal data of individuals, not all these examples will be applicable in all circumstances:

Data minimisation – this includes retention minimisation i.e. only keeping personal data for as long as it is required, and, only using personal data when it is absolutely required therefore reducing the chance of individuals being identified

Collection minimisation **-** only collecting the personal information that is needed

Deletion – Having automated deletion processes for particular personal data to ensure it is flagged for deletion after a particular period

Anonymisation – The data is held in a form where the individuals are no longer identifiable and it is unlikely that any individuals can be re-identified by combining the data with other data e.g. data matching. The GDPR emphasises that anonymization or pseudonymisation should be used wherever possible particularly in relation to historical or scientific research or for statistical purposes.

Pseudonymisation – The identity of an individual is disguised for instance by replacing identifying fields with artificial identifiers or pseudonyms. When data has been pseudonymised it still retains a level of detail which allows tracking back of the data to its original state. This is in contrast to anonymised data where reverse compilation should be impossible.

Differential privacy – Random 'noise' is injected into the results of dataset queries to provide a mathematical guarantee that the presence of any one individual in a dataset will be masked. This technique may be useful for research data. Software evaluates the privacy risks or a query and determines the level of noise to introduce into the result before releasing it.

Synthetic data – As long as the number of individuals in the dataset is large enough, it is possible to generate a dataset composed entirely of 'fictional' individuals or altered identities that retain the statistical properties of the original dataset.

Privacy by Default – The system is set up so the default settings are the ones that provide maximum protection against privacy risks i.e. technical and organisational measures are put in place to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This may mean that the default position would not allow full functionality of the project, unless, the user explicitly chooses it.

User Access controls – The amount of personal data that authorised users have access to should be limited to the information they need to know to fulfil their roles.

Data Subject Access - Individuals should be able to access their own personal data and be informed of its use and disclosures. If individual users can't access the systems directly themselves, it should be set up in a way that allows data to be collated with ease in order to comply with subject assess requests.

User friendly systems – Privacy related functions should be user friendly. For instance, users should be able to easily update their details or extract information that relates to them.

Accuracy – The design should incorporate checks to ensure accuracy and completeness of data and that it is as up-to-date as is necessary to fulfil the specified purposes.

Compliance – The design should include processes to monitor, evaluate, and verify compliance (e.g. with legal requirements, policies and procedures).

State of the art – State of the art technology and organisation measures should be used, where possible, however this needs to be balanced against reasonable costs. Old technology should be replaced where possible and software and patches kept up-to-date. In deciding what measures are appropriate, account should be taken of the nature, scope, context and purposes of processing as well as the risks, likelihood and severity for the rights and freedoms of individuals.

Security – Security measures should include processes for secure destruction, appropriate encryption, and strong access control and logging methods.

Suppression of data – The system should be set up to allow the suppression of data of individuals who have objected to receiving direct marketing or those who want to object to decisions being made about them based on automated processing including profiling. Where appropriate the system should also allow data portability in accordance with the GDPR and the right of individuals to request the transmission of their personal data to another data controller in a machine-readable format.

Data processors – Contracts with data processors need to set out how risk/liability will be apportioned between the parties in relation to implementation of 'privacy by design' and 'privacy by default' requirements.

Tenders – Privacy issues should be considered as part of public tenders.

Transfers outside EEA – Particular consideration should be given to protecting personal data when data is likely to be transferred outside the EEA.

These are some example measures that can be taken and not all of them will be appropriate for every project or system, however, it is likely that most projects will benefit from taking some of the steps outlined above.

The DPIA should be used to record the privacy measures that are designed into the project.

30 PERSONAL DATA PROCESSED BY STUDENTS

1) Students use personal data for three main reasons:

   i. to maintain a personal life; for example, to communicate with family and friends,

   ii. to pursue a course of study with GSA; for example, to research and write an essay, report or thesis, and

   iii. to carry out research as a member of a GSA established research group.

2) Students may use many different methods to process personal data, such as maintaining an electronic address book, a computer database, or an email account.

3) When is GSA responsible for the personal data processed by students?

   GSA is only responsible for personal data when it is the data controller for that data. A data controller is the person who determines the purposes for which and the manner in which any personal data is or is not to be processed. Therefore, GSA is only responsible for the personal data processed by students when students process data for GSA's purposes.

   The following are some scenarios that involve students processing personal data.

   Scenario One

   A student processes personal data in the course of his or her personal life, for example writing an email (using his or her GSA provided email account) to his or her family about a friend's recent birthday.

   GSA is not the data controller for personal data processed by the student in the course of his or her personal life, as GSA does not determine the purpose of the processing. The fact that the student may choose to use the GSA provided email account to pursue his or her personal life does not make GSA responsible for the processing of personal data for that purpose. GSA did not determine the purpose so the institution cannot be the data controller. The student is the data controller and may claim the domestic purposes exemption.

Scenario Two

A student processes personal data in order to pursue a course of study with GSA; for example, as part of her degree course dissertation, the student's supervisor suggests carrying out interviews.

GSA is not the data controller for personal data processed by a student to pursue a course of study with GSA. Students undertake a course of study with GSA for their own personal purposes, most obviously to obtain a qualification. The student is not an employee or agent of GSA, and neither does she act on behalf of GSA. The student decides what work she will do, the way in which she will do it and what she will include in her final submission. She must make these decisions herself in order to prove that she is capable of degree-level work. She works on behalf of herself and not GSA. Thus, GSA cannot be the data controller for the personal data processed by the student in the course of her studies.

The fact that the student was recommended to undertake interviews by her supervisor does not make GSA responsible for the processing of the interviewees' personal data. The role of the supervisor is to advise and teach the student, which includes giving advice on data protection issues as part of the student's training in good research practice, but it was for the student's own purposes that the interviews took place.

Scenario Three

A student submits a piece of work (e.g. an essay, report or thesis) in which there is personal data, to GSA for assessment.

GSA is the data controller for the personal data contained within the submitted piece of work from the point at which it is submitted. Once the work has been submitted GSA is responsible for the personal data within the document, for example the member of staff who marks the work is processing the personal data contained within it (by reading it) for the purpose of determining what grade the GSA should award the student - this is GSA's purpose.

Scenario Four

A research student processes personal data whilst working on a project led by a GSA research group.

GSA is the data controller for personal data processed by a student working on a research project led by a GSA research group. The student processes personal data for the purposes laid down by the project, the remit of which has been decided by GSA (or the GSA employed principal investigator), not the student. The purposes for processing are the GSA's and not the student's, therefore GSA is the data controller and the student is an agent of the institution.

This is the case whether the student is funded by the research project or whether the student is self-funding. Normally only postgraduate research students would fall under this scenario but not all postgraduate research; in many cases the postgraduate themselves determines the scope of the research and where this is the case the processing is like that described in scenario two.

4) Therefore, GSA is the data controller for personal data processed by students in only very limited circumstances.

31 PHOTOGRAPHS AND RECORDED IMAGES OF PEOPLE

1) Still and moving images of individuals in small groups can be defined as personal data as they feature identifiable individuals and, as a result, they have to be processed in accordance with the GDPR principles.

2) All processing of personal information is required to meet a legal justification in GDPR. In relation to photographs and recorded images this will often mean that consent is required. The sections below explain what is normally required and gives examples of particular circumstances which involve the use of images and recordings.

3) Not following the guidance below or not obtaining appropriate consent can expose GSA to the risk of a legal claim or damage of reputation. If the consent of the subject has not been obtained, consideration should be given to using a different image where it is known that appropriate consent has been obtained.

4) These procedures apply to still and moving images and recordings created or commissioned by GSA employees, contractors or volunteers in the course of their work for GSA. GSA is the data controller for all such images and recordings that feature people, regardless of where the recordings take place. GSA determines the purpose of recording and is legally responsible and accountable for its use.

5) These procedures do not apply to images or audio-visual recordings created by members of the GSA community or visitors for their own private use on their own personally-owned equipment. GSA is not the data controller for such recordings. However, personal use of images or audio-visual recordings which harass or cause distress to others may be subject to disciplinary sanctions in accordance with other GSA regulations and policies governing the conduct of staff or students and may also be in breach of criminal law.

6) When is an image personal data? Where an individual is the focus of an image, the image is likely to be personal data. Examples of images that are personal data:

   - photographs of individuals particularly those that are stored with personal details, for example, for identity passes

   - photographs of staff or students published on notice boards or websites along with some biographical details

   - individual images published in a newsletter or marketing material

7) Where individuals are incidentally included in an image or are not the focus, the image is unlikely to contain personal data. Examples include:

   - where people are incidentally included in an image or are not the focus, for example at a busy open day, the image is unlikely to classed as personal data

   - images of people who are no longer alive; the GDPR only applies to living people so these images are not personal data.

8) Small Groups

Small groups where photographs or videos are being taken of individuals or small groups of people then consent should be obtained. This is the easiest and safest way of proving that the image has been obtained fairly and in accordance with the individuals' rights. There are only a small number of exceptions to this when there is an alternative legal basis for processing, such as graduation ceremonies where official photographs and filming are done on the basis of contract (see below).

9) Large Groups

It will usually be enough for the photographer to ask permission verbally to take the photograph to ensure compliance with the GDPR. Anyone not wishing to appear on a group photograph will then have the opportunity to opt-out. This approach can be used when photographing, for instance, a seminar. However, if images will be posted on a website, explicit consent should be sought as the image will be disclosed outside the EU.

10) Consent

If a consent form is being used, it must include details of what the images will be used for, any third parties the images will be share with, whether they will be transferred outside the EU (including posting on websites), how the information will be held securely and for how long, details of the individual rights (e.g. the right to withdraw consent, the right to lodge a complaint with the ICO) and GSA's contact details (including contact details of the DPO). Copies of consent forms should be retained locally for as long as the image is retained.

11) Special Categories of Personal Data

The GDPR makes it clear that photographs are not normally considered to be processing of special categories of personal data (e.g. health information, ethnicity) unless they are being processed by technical means that enables the unique identification of an individual. However, care should be taken if images reveal sensitive personal information such as those taken in a medical context. Explicit written consent should be obtained in these circumstances and retained locally.

12) Graduation

All students and guests who attend a graduation ceremony are informed in advance that photographs and recordings will be taken at the ceremony and that official photographers are likely to be in and around the graduation venue taking photographs and video recording. As part of accepting the invitation to attend the graduation ceremony and agreeing to the graduation terms and conditions students are entering into a contract with GSA. The contract makes it clear that there is a possibility that they will be photographed and videoed and for these images to go on the GSA's website. Students who do not wish to be photographed or videoed have the option to graduate in absentia. Notices should be placed prominently at the graduation venue so people are aware of the recordings. The notification should advise that official photographs and video recordings are likely to be put on the GSA's website which means the images are transferred outside the EU.

Photographs taken for purely personal use are exempt from the GDPR requirements so photographs and videos taken by family members at a graduation ceremony are not covered by GDPR.

13) ID Cards

Photographs of staff and students are included on ID cards. This is for security purposes and consent is not required. The use of images in this way is covered in GSA's Academic Registry Privacy Notice and Human Resources Privacy Notice.

14) CCTV

CCTV cameras are located around campus for the purposes of security and preventing and detecting crime. Notices should be placed by the Estates Department around campus advising people of the presence of these cameras. The Head of Estates may wish to publish a fuller policy on this matter. The Head of Estates should also check whether the cameras overlook areas which people would assume are private (for example, a neighbouring residential property) and should nominate an individual with responsibility to ensure CCTVs are used appropriately.

15) Research

Images used for research should follow the guidelines on Research in section 21 of this policy. A Data Protection Impact Assessment should be conducted as part of the project approval process.

32 DIRECT MARKETING

1) Direct marketing is the communication to a particular individual of any advertising or marketing material.

2) It is not confined to the advertising or marketing of commercial products or services and includes messages trying to sell goods or services and those promoting an organisation or its values or beliefs.

3) Information promoting GSA events or opportunities for students could constitute direct marketing and therefore it is important that GSA is aware of these definitions and regulations, particularly when sending out mass communications. This covers all forms of communication including by post, telephone, email and other forms of electronic messages.

4) It can be difficult to tell the difference between a marketing email and a 'service' email. A service email is a communication that is sent to an individual that facilitates or completes a transaction, whether that is for the sale of goods or services.

5) When trying to identify a service email the following questions should be asked:
   - Is GSA under a legal obligation to send the email?
   - Is the email part of the performance of a contract?
   - Would the individual be at a disadvantage if they did not receive the email?

   If the answer to any of these questions is 'yes' then the email is likely to be more of a services email than a marketing email. For instance, an email to a student about an offer of a place on a course, paying fees or how to register would all be examples of service emails.

6) Marketing emails are those that promote the aims and objectives of GSA such as sale of goods, services or organisational ideals. Examples would be details of how to join student clubs which is not essential information for a student to study at GSA.

7) Any personal details collected and held for direct marketing purposes **must** comply with the data protection principles e.g. it is fair and lawful, the information is only used for the purpose it is collected for, the information is kept up-to-date, it is not kept for longer than necessary and is held securely.

8) In addition to GDPR the Privacy and Electronic Communications Regulations 2003 (PECR) regulate in detail the use of electronic communications (e.g. email, SMS text, recorded message) as a form of marketing. PECR is due to be replaced shortly by a new ePrivacy Regulation (ePR).

9) There are some minor exceptions but in order to comply with the GDPR and PECR requirements governing direct marketing it is safest to assume that consent is required. Consent should normally be obtained when contact details are collected and providing an appropriate privacy notice (see sections 17 and 19 of this policy).

10) The consent must be 'opt-in' and any direct marketing messages should only be sent to those people who have opted in.

11) All subsequent marketing communications that are sent should also contain an option to opt-out with details of how the individual can request not to receive any further messages. If GSA receives an opt-out request it must comply as soon as possible; there are no exceptions to this.

12) When requesting consent, it is good practice to request consent separately for different forms of communication i.e. whether individuals agree to be contacted via post, telephone or email. This is because the different forms of communication are covered by different legislation.

13) Where direct marketing is communicated by telephone, staff must identify themselves and if requested, provide an address or telephone number on which they can be reached.

14) Where cold-calling for fundraising takes place, details should first be checked against the Telephone Preference Service (TPS). Those receiving calls should be made aware of their right to object to the calls.

15) There is a minor exception to the general opt-in consent rule which is known as the 'soft opt-in' exception. This is where personal data has been collected in the context of an existing relationship with an individual and GSA limits marketing to providing information on similar services/goods. In this case, the soft opt-in allows GSA to market to these individuals via electronic means without having opt-in consent. However, this can only be relied on if the individual was informed at the point of data collection that the information would be used for marketing purposes and they are given the opportunity to opt-out at that stage and in each subsequent piece of communication. Please note that this 'soft opt-in' is only available to commercial marketing. Therefore, it is not available to not-for-profit organisations or charities (e.g. GSA) when promoting their aims or ideals or trying to fundraise. GSA should be careful about relying on the soft opt-in and seek consent as the preferred option.

33 REPORTING WEAKNESSES, EVENTS AND PERSONAL DATA BREACHES: PROCEDURE

1) A personal data breach is defined in GDPR to mean: "a breach of security leading to the accidental or unlawful destruction, loss, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

2) GSA must make every effort to avoid personal data breaches, however, it is possible that mistakes will occur on occasions or things will happen that are beyond GSA's control. In these cases, it is important that the GSA responds appropriately. GSA has a responsibility to deal with the breach immediately and appropriately in order to minimise the impact and prevent recurrence.

3) **The GDPR also imposes a requirement that most personal data breaches are reported to the ICO as soon as possible and at the latest within 72 hours of GSA becoming aware of the breach.**

4) This section of the policy sets out the procedures to follow if a personal data breach is identified. All individuals who access, use or manage GSA's information are responsible for following these procedures and for reporting any data protection breaches that come to their attention.

5) A personal data breach can occur for a number of reasons some examples of these include:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Unauthorised disclosure (e.g. email sent to incorrect recipient or document posted to the wrong address or personal information posted onto the website without consent);
- Human error;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack;
- 'Blagging' offences where information is obtained from an organisation by deception.

6) The consequences of a personal data breach could be physical, material or moral damage to individuals such as loss of control over their personal data, identity theft or fraud, financial loss, damage to the reputation, or any other economic or social disadvantage to the individual concerned.

7) **Reporting an incident.**
Reporting an incident is the responsibility of any member of staff, student or other individual who discovers a personal data breach to report it immediately to the local Data Protection Co-ordinator, in the first instance.

On initial contact the reporter should provide details of:

- The exact nature of the breach
- An indication of the seriousness of the breach (the sensitivity of the data breached, the number of individuals whose data may be involved, who may have access to the data)
- If possible, what action needs to be taken immediately to mitigate the breach.

The local Data Protection Co-ordinator will ask the reporter to provide more detailed follow-up information within 24 hours of the discovery of the breach, which the local Data Protection Co-ordinator will pass on to the DPO.

8) The DPO must contact other parties as required, such as the Registrar and Secretary and the police, if there has been any illegal activity, and the Director of Strategy and Marketing if there is likely to be press interest. Other Schools and Professional Support areas may be notified as appropriate, in particular if the breach involves IT security, the Director of IT will also be notified. There may also be other parties to notify as a result of legal/contractual requirements.

9) **Data Subjects**
After a personal data breach is identified, GSA will assess whether the breach will result in a high risk to the rights and freedoms of individuals and, if so, let the data subject know about the breach as soon as possible.

The local Data Protection Co-ordinator will communicate immediately with the relevant GSA area responsible for the data that has been breached and, in conjunction with the DPO, discuss the best way of contacting the data subjects concerned and what information the data subjects should be given.

When individuals are notified they should be given specific and clear advice on what they can do to protect themselves and what support and advice is available from GSA. They should be provided with details of who they can contact for further information or to ask questions.

10) **Containment and Recovery**
Steps should be taken as soon as possible to recover any losses and limit the damage. Steps might include:

- Attempts to recover lost equipment
- Use of backups to recover lost, damaged or stolen data
- Change relevant passwords as soon as possible
- If bank details have been lost/stolen, contacting banks directly for advice on preventing fraudulent use
- Attempts to retrieve personal data, e.g. recall emails, remove from websites etc.

11) **Evaluation and Response**
Once the incident is contained the DPO, in conjunction with the local Data Protection Co-ordinator, should conduct a review into the causes of the breach and the effectiveness of the response. The review should consider the type of data, what protections were in place (e.g. encryption), what happened to the data, and whether there could be wider consequences of the breach. If ongoing problems are identified, then an action plan should be drawn up to address these.

In the case of the most serious breaches a report will be submitted to the Audit Committee.
If the breach warrants a staff disciplinary investigation the Human Resources department will be contacted for advice and guidance.

The DPO will keep a record of all data breaches including the actions taken to mitigate the breach and the lessons learnt.

12) In the event that GSA is responsible for causing a personal data breach, or not taking appropriate action to prevent a breach, then there could be financial consequences. It is therefore important to make every effort to prevent breaches occurring and. if breaches do occur. take required actions. More information about the impact of non-compliance can be found in section 12 of this policy.

34 DATA SUBJECT RIGHTS

1) The GDPR gives data subjects the right to access personal information held about them by GSA. The purpose of a subject access request is to allow individuals to confirm the accuracy of personal data and check the legality of processing to allow them to exercise rights of correction or objection if necessary. However, individuals can request to see any information that GSA holds about them, which includes copies of email correspondence referring to them or opinions expressed about them.

2) GSA must respond to all requests for personal information and information will normally be provided free of charge.

3) References

References may be disclosed to the person about whom they are written under the subject access provisions of the GDPR. This includes references received by the GSA from external sources and confidential references given and received internally e.g. as part of advancement and promotions procedures. There is an exemption from disclosure for references written by GSA staff and sent externally, however, these references would still be accessible to the applicant from the organisation to which the reference was sent. In order to maintain confidentiality and to prevent the unauthorised disclosure of information, staff should not provide references without a prior request from the student concerned.

4) Examination scripts

GSA is not required to disclose examination scripts however students are entitled to access any marks or comments annotated on the script. Students are entitled to their marks for both coursework and examinations. Unpublished marks must be disclosed within 5 months of a subject access request. Information about submitting subject access requests can be found in section 41e of this policy.

5) Data subjects have a number of other rights under the GDPR. These include:

Right to Object – Data subjects have the right to object to specific types of processing which includes processing for direct marketing. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right (see section 32 of this policy on direct marketing). Online services must offer an automated method of objecting. In some cases, there may be an exemption to this right for research or statistical purposes done in the public interest.

Right to be forgotten (erasure) – Individuals have the right to have their data erased in certain situations such as where the data are no longer required for the purpose for which they were collected, the individual withdraws consent, the individual has objected to processing based on legitimate interests or the information is being processed unlawfully.

There is an exemption to this for scientific or historical research purposes or statistical purposes if the erasure would render impossible or seriously impair the achievement of the objectives of the research. Individuals can ask the data controller to 'restrict' processing of the data whilst complaints (for example, about accuracy) are resolved or the processing is unlawful.

Rights in relation to automated decision-making and profiling

The right relates to automated decisions or profiling that could result in significant affects to an individual. Profiling is the processing of data to evaluate, analyse or predict behaviour or any feature of their behaviour, preferences or identity. Individuals have the right not to be subject to decisions based solely on automated processing in certain circumstances. When profiling is used, measures must be put in place to ensure security and reliability of services. Automated decision-making based on special category of data can only be done with explicit consent.

Right to Rectification - The right of individuals to require a data controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data is not complete, an individual can require the controller to complete the data, or to record a supplementary statement.

Right to Portability – the data subject has the right to request information about them is provided in a structured, commonly used and machine-readable form so it can be sent to another data controller. This only applies to personal data that is processed by automated means (not paper records); to personal data which the data subject has provided to the controller, and only when it is being processed on the basis of consent or a contract.

6) Any requests made to invoke any of the rights above must be dealt with promptly and in any case within one month of receiving the request. There may be some circumstances where GSA can take longer than one month to fulfil the request, however, these are limited and GSA should always strive to meet the stipulated timeframe of one month wherever possible. Members of staff should consult their local Data Protection Co-ordinator if any requests like these are received.

35 RIGHT TO BE FORGOTTEN PROCEDURE

1) Data subjects have the right to be forgotten (erasure) and, consequently, are entitled to have their personal data erased in certain situations such as where the personal data is no longer required for the purpose(s) for which it was collected, the individual withdraws consent, the individual has objected to processing based on legitimate interests or the information is being processed unlawfully.

2) There is an exemption to this for scientific or historical research purposes or statistical purposes if the erasure would render impossible or seriously impair the achievement of the objectives of the research. Individuals can ask the data controller to 'restrict' processing of the data whilst complaints (for example, about accuracy) are resolved or the processing is unlawful.

3) Data subjects wishing to exercise their right to be forgotten should contact their local Data Protection Co-ordinator in the first instance**.**

36 DATA PORTABILITY PROCEDURE

1) Under the GDPR, the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

2) It allows them to move, copy or transfer personal data from one IT environment to another in a safe and secure manner, without hindrance as to usability.

3) The right to data portability only applies:
- to personal data which an individual has provided to a data controller (GSA),
- where the processing is based on the individual's consent or the performance of a contract, and
- when processing is carried out by automated means.

4) GSA must comply with a data portability request by providing the personal data in a structured, commonly used and machine-readable form.

5) The information must be provided free of charge.

6) If the individual requests it, GSA may be required to transfer the data directly to another organisation if this is technically feasible.

7) If the personal data concerns more than one individual, consideration must be given as to whether providing the information would prejudice the rights of any other individual.

8) GSA must respond to the request without undue delay and in any event within one month. This can be extended to two months if the request is complex or a number of requests are received.

9) Where GSA is not taking action in response to a request, an explanation must be provided to the individual, informing them of their right to complain to the ICO and their right to seek a judicial remedy.

37 DATA SUBJECT ACCESS RIGHTS AND RIGHTS IN GENERAL

1) Any member of staff receiving a request from an individual for or about their own personal information should forward this to their local Data Protection Co-ordinator as soon as possible. The Data Protection Coordinator will refer the request to the Academic Quality Office for processing in accordance with normal procedure.

2) The purpose of the Subject Access Right is to allow individuals to confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary.

3) GSA must respond to all requests for personal information. Requests should be sent by the Academic Quality Office to the local Data Protection Co-ordinator(s) for a response. The following important points are relevant:

- The request can be in any format provided it is clear. The information provided needs to be sufficient to identify the person making the request.

- Proof of identity can be requested if required

- The scope of the request is clear. If the scope of the request is not clear, the requester can be asked to be more specific about the activities and areas to which the request relates. The requester can be asked to provide time periods, names of members of staff who may have dealt with them or Schools/ areas that are most likely to hold the information they are seeking.

- Information must be provided in a concise, transparent, intelligible and easily accessible format using clear language.

- The response should be provided in a commonly used electronic format, particularly if the request was submitted electronically, unless the requester has asked for another format.

- When requested by the data subject the information may be provided orally as long the identity of the data subject is not in any doubt.

4) There is a requirement that information should be provided within one month. If the information requested is particularly complex, this period can be extended by a further two months but the requester must be informed about the extension within one month and the reasons for the delay explained.

5) Information must be provided free of charge unless additional copies are requested when a reasonable fee can be charged based on administrative costs.

6) Where a request is manifestly unfounded or excessive, in particular because of the repetitive character, the request may be refused. In this case, GSA will have to demonstrate how the request is manifestly unfounded or excessive in character.

7) The data subject has the right to obtain the following information:

- Confirmation that personal data about them is being processed

- A copy of that personal data

- Details of the purpose of the processing

- Categories of the personal data concerned e.g. does it include any special categories or sensitive personal information

- Any recipients or categories of recipients the personal information has been shared with, particularly if these are situated or domiciled outside the EU.

- What safeguards are in place for transfers outwith the EU

- The period the personal information will be stored for or what the criteria are for determining the period of storage

- The existence of the right to request from the data controller the correction or deletion of personal data or to restrict or object to the processing of personal data concerning them

- The right to lodge a complaint with the Information Commissioner's Office (ICO)

- The source of the personal data if it has not been collected directly from the data subject

- Details of any automated decision-making, including profiling, and meaningful information about the logic involved and the envisaged consequences of such processing for the data subject.

8) The following information should be redacted or otherwise removed from a response before it is sent:

- Personal information relating to other individuals (unless their permission has been obtained to release it)

- Trade secrets or commercially sensitive information

- Intellectual property in particular the copyright protection of the software.

38 COMPLAINTS PROCEDURE

1) The GDPR requires that GSA must have a procedure which addresses complaints from data subjects about:

- the processing of their personal data,
- GSA's handling of requests from data subjects, and,
- appeals from data subjects on how complaints have been handled/resolved.

2) Procedure

The GSA Complaints Handling Procedures and HR and SPSO policies (together with supporting documentation and guidelines), comply with the Scottish Public Service Ombudsman's (SPSO) recommendations on the handling of complaints, and this policy should be read and applied in conjunction with the GSA Complaints Handling Procedures and HR and SPSO policies.

39 GLOSSARY

This glossary outlines briefly the meanings of particular words and phrases as used in this policy. Detailed definitions and explanations can be found in the relevant sections of the policy.

GDPR
The EU General Data Protection Regulation, effective as of 25 May 2018.

ICO
The Information Commissioner's Office - the UK Government supervisory body which oversees the implementation of, and compliance with, the GDPR.

Personal data
Any information relating to a living individual and by which that living individual can be identified either directly or indirectly.

Processing
Any operation or set of operations carried out on personal data.

Profiling
Any processing of data to evaluate, analyse or predict behaviour.

Data subject
Any identifiable living person.

Data controller
Any legal entity that determines the purpose and means of processing personal data.

Data processor
Any legal entity, other than the data subject, that processes personal data on behalf of the data controller.

Third party
Any legal entity, other than the data subject, the data controller or the data processor.

Consent
Legally binding assent given by one party.

Contract
A legally binding agreement entered into by two or more parties.

Legal obligation
A legally binding requirement imposed by law.

Privacy Notice
A formal document setting out information regarding the purposes for and uses of personal data**.**

Data security
The safe and secure collection, storage and protection of personal data

Personal data breach
A breach of security leading to the accidental or unlawful destruction, loss, unauthorised disclosure of, or access to personal data.

Subject access request
A request to allow individuals to confirm the accuracy of their personal data, check the legality of processing, and, exercise the rights of objection or correction**.**

Data sharing
Sharing personal data with a third party or an external processor.

Data Protection Impact Assessment/Privacy Impact Assessment
A process whereby potential privacy issues and risks are identified and examined.

Data protection by design and default/Privacy by design
An approach to handling personal data that promotes privacy and data protection compliance from the start.

Direct marketing
The communication to a particular individual of any advertising or marketing material(s).

Right to object
The right of a data subject to object to specific types of processing, including direct marketing.

Right of rectification
The right of a data subject to require a data controller to rectify inaccuracies in personal data held about them.

Right of destruction/Right to be forgotten
The right of a data subject to have their data removed, erased or destroyed in certain situations.

Right to portability
The right of a data subject to request that their personal data is provided in a structured, commonly used and machine-readable form so that it can be sent to another data controller.

Anonymisation
Personal data is held in a form whereby the data subject cannot be identified**.**

Pseudonymisation
Personal data is held in a form whereby the identity of the data subject is disguised.

Data minimisation
Only keeping personal data for as long as it is required.

Collection minimisation
Only collecting personal information that is needed.

Use minimisation
Only using personal data when it is absolutely required therefore reducing the chance of individuals being identified.

Deletion
Having automated deletion processes for particular personal data to ensure it is flagged for deletion after a particular period.

Differential privacy
Random 'noise' is injected into the results of dataset queries to provide a mathematical guarantee that the presence of any one individual in a dataset will be masked.

Synthetic data
The possibility of generating a dataset composed entirely of 'fictional' individuals or altered identities that retain the statistical properties of the original dataset.

Privacy by Default
A system is set up so the default settings are the ones that provide maximum protection against privacy risks.

User Access controls
The amount of personal data that authorised users have access to should be limited to the information they need to know to fulfil their roles.

Data Subject Access
Individuals should be able to access their own personal data and be informed of its use and disclosures.

User friendly systems
Privacy related functions should allow easy updating of details or the extraction of relevant information.

Accuracy
The system design should incorporate checks to ensure accuracy and completeness of data and that it is as up-to-date as is necessary to fulfil the specified purposes.

Compliance
The system design should include processes to monitor, evaluate, and verify compliance (e.g. with legal requirements, policies and procedures).

State of the art
State of the art technology and organisation measures should be used, where possible, however this needs to be balanced against reasonable costs.

Security
Security measures should include processes for data protection, secure destruction, appropriate encryption, and strong access control and logging methods.

Suppression of data
The system should be set up to allow the suppression of data of individuals who have objected to receiving direct marketing or those who want to object to decisions being made about them based on automated processing including profiling.

Tenders
Privacy issues should be considered as part of public tenders.

Transfers outside EEA
Particular consideration should be given to protecting personal data when data is likely to be transferred outside the EEA.

Legitimate interest
The processing of personal data which is necessary for the legitimate interests pursued by an organisation.

Children
Anyone under the age of 16 (or, possibly 13 when providing an online service directed at children but for all other purposes 12 in Scotland).

Sub-contracted processing
The processing of personal data by an external supplier/third party on behalf of a data controller.