THE GLASGOW SCHOOL OF ART

Information and data classification policy

POLICY DETAILS:

Date of approval	7th February 2017
Approving body	GSA Executive Group
Supersedes	n/a
Date of EIA	23rd January 2017
Date of next review	*See departmental schedule*
Authors	Nicola Siminson
Responsible Executive Group area	Deputy Director (Academic)
Related policies and documents	GSA Information Technology Security Policy GSA Policy for Staff Electronic File Backup GSA Records Management Policy GSA Research Data Management Policy GSA Research Ethics Policy GSA Data Protection Policy
Benchmarking	http://www.stir.ac.uk/media/services/registry/planning/legalcompliance/DataClassificationPolicy.pdf https://www.hw.ac.uk/services/docs/WhatInformation2016.pdf https://www.st-andrews.ac.uk/media/restricted/it-services/security/Information-classification-policy-v1-1(Approved).pdf

1. What is information and data classification?

Data classification enables information to be appropriately managed throughout the Glasgow School of Art (GSA), and ensures that individuals who have a legitimate reason to access a piece of information are able to do so, whilst protecting data from those who have no right to access it.
The classification of data helps to:

- determine how information should be accessed and handled;
- ensure that sensitive and confidential data remains secure;
- prevent data leaks/breaches, and minimise the impact of such leaks if they do occur.

There are good reasons to protect some information and data, especially data that carries a high degree of sensitivity. Managing information appropriately reduces the likelihood of:

- harm or distress to individuals or groups;
- disruption to the GSA's business activities, and/or substantial financial loss;
- damage to the GSA's reputation and standing;
- legal action against the GSA, or investigations by regulatory bodies.

Within this policy, **classifying** information means allocating one of four **categories** to all information or data held by the GSA, based on the level of sensitivity and the impact on the GSA if this data was lost or stolen, altered or destroyed without authorisation, or accidentally disclosed to others. This includes documents, spreadsheets, and other print and electronic data; **Appendix A** includes a more detailed definition of data.

All data or information should have an owner; this could be the author of a document, or the School or Department responsible for the data or information. All data owned, used, created or maintained within the GSA should be categorised as either:

- public
- internal
- restricted
- highly sensitive

It is likely to be obvious which category most information should fall within, and the majority of the GSA's information will come under the **public** and **internal** categories, such as information on the GSA website, or internal correspondence.
A smaller amount of information will need to be categorised as **restricted** (for example student data, or reserved committee business). The **highly sensitive** classification should only be applied in exceptional circumstances, to confidential commercial contracts or legally privileged information, for instance.

The data classification framework in **Appendix B** includes further information and examples of the types of information and data which fall under each of these four categories; who should have access to this information; the level of risk in releasing the information inappropriately; and how the information should be disposed of when no longer needed. **Appendix C** provides a decision support flow chart, which can help to determine which category should be used for different pieces of information.

A single document may contain information or data with different classifications, and one piece of information can have different classifications throughout its lifetime. For example, a student record may consist of both sensitive and personal data, *and* information that is publicly available (for example, degree awards and prizes); and commercially sensitive information may become less sensitive over time. This also affects whether and when information can be disclosed, for instance in response to a Freedom of Information (FoI) request.

Classifying information and data appropriately helps the GSA to remain compliant with the requirements of both the Data Protection Act (1998), and to handle requests under the Freedom of Information (Scotland) Act (2002) effectively; any information that we record or receive in the course of our work could have to be disclosed under these pieces of legislation. Further information on both can be found in **Appendix A**.

2. Who does this policy apply to?

This policy applies to all GSA staff, both working on campus and when working remotely. It also applies to associates working with the GSA, including agency staff, data processors, third parties and collaborators working with the GSA. Members of GSA staff working with these types of associates and third parties have a responsibility to bring this policy to their attention.

All members of the GSA community need to know what steps we each need to take to:

- protect confidential information;
- communicate it safely;
- retain information only as long as needed [1] by the GSA;
- destroy it securely when no longer needed.

3. Roles and responsibilities

Data classification and handling bestows a number of obligations on individual members of staff, associates working with the GSA, and the School itself.

3.1 The Glasgow School of Art

The GSA is committed to establishing and modelling good information and data classification, which protects sensitive data (and the individuals associated with it), enables GSA staff to carry out their work in an assured way, and prevents risks to the GSA.
Responsibility for information and data classification sits with the GSA's Executive Group, with the Deputy Director (Academic) having overall strategic responsibility.

The GSA's Executive Group and its individual members are responsible for:

- disseminating and promoting this policy to relevant staff within their areas;
- ensuring that staff within their areas are aware of and are undertaking the necessary processes;
- advising on strategic developments that are likely to impact on information and data classification.

3.2 All GSA staff

All GSA staff are responsible for:

- adhering to this policy;
- having an awareness of the four data classification categories (public; internal; restricted; highly sensitive), and the way information within each category should be managed;
- handling, classifying and protecting the GSA's information and data appropriately;

[1] You can find out more about what information needs to be kept, and for how long, within the Glasgow School of Art's **Records Retention Schedules**: http://www.gsa.ac.uk/about-gsa/key-information/records-management/

- promptly referring any requests for **restricted** or **highly sensitive** information from someone who is not already authorised to see it to foicoor@gsa.ac.uk for action;
- bringing this policy to the attention of any associates and third parties they are working with.

3.3 Associates working with the Glasgow School of Art, including agency staff, data processors, third parties and collaborators, where a Service Level Agreement (SLA) is not already in place

Associates and third parties are responsible for:

- adhering to this policy;
- handling, classifying and protecting the information they work with appropriately.

4. Further information and support

This policy should be read in conjunction with the related GSA policies listed below, especially the **GSA Information Technology Security Policy**, and the **GSA Policy for Staff Electronic File Backup**.

GSA policy	Link to web page
GSA Information Technology Security Policy	http://www.gsa.ac.uk/about-gsa/key-information/it-policies/
GSA Policy for Staff Electronic File Backup	http://www.gsa.ac.uk/about-gsa/key-information/it-policies/
GSA Records Management Policy	http://www.gsa.ac.uk/about-gsa/key-information/records-management/
GSA Research Data Management Policy	http://www.gsa.ac.uk/about-gsa/key-information/institutional-policies/
GSA Research Ethics Policy	https://vle.gsa.ac.uk/ → Research & Knowledge Exchange → Policy → GSA Research Ethics
GSA Data Protection Policy	http://www.gsa.ac.uk/about-gsa/key-information/it-policies/

In addition, the following GSA staff can provide further information and support:

- the **FoI Co-ordinator** can advise on how to determine whether information is disclosable, and should always be contacted when a FoI request is received: foicoor@gsa.ac.uk
- the **Institutional Repository and Records Manager** can advise on policy and practice relating to information handling and records management. Further information and contact details can be found on this web page: http://www.gsa.ac.uk/about-gsa/key-information/records-management/
- The **IT Helpdesk** can be contacted with any queries relating to the appropriate security and technical controls required to store and protect information: gsaitservicedesk@gsa.ac.uk

5. Acknowledgements

This document draws on policies and guides kindly shared with the GSA by the University of Stirling, Heriot-Watt University and the University of St Andrews, and the assistance of these institutions is gratefully acknowledged.

Appendix A: Definitions and legislation

- **Definition of data**

This covers all data, including research data, or information held by the Glasgow School of Art, on paper or in electronic format, including documents, spreadsheets and other data. It includes data held inside systems and databases, produced by systems and data to be keyed in/loaded into systems, as well as email content.

Further definitions of administrative data are available from the **Administrative Data Liaison Service (ADLS)** at the following link: http://www.adls.ac.uk/adls-resources/guidance/introduction/

In addition, the Glasgow School of Art's definition of ***research data*** is included in its policy, which is available at the following link: http://www.gsa.ac.uk/about-gsa/key-information/institutional-policies/

- **The Data Protection Act (1998)**

The Data Protection Act places obligations on the Glasgow School of Art to process personal information securely, and to ensure that the appropriate technical and organisational measures are taken to prevent unlawful processing of personal data, and to protect against accidental loss, destruction or damage to personal data.

The Data Protection Act also defines ***Sensitive Personal data,*** which relates to racial or ethnic origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of criminal offences. The processing of ***Sensitive Personal data*** is subject to additional, more stringent conditions, as detailed in Schedule 3 of the Act.

For further information about Data Protection, please see the GSA's Data Protection Policy at the following link: http://www.gsa.ac.uk/about-gsa/key-information/it-policies/

- **The Freedom of Information (Scotland) Act 2002**

The Freedom of Information (Scotland) Act (FOISA) requires the Glasgow School of Art to make information it holds publically available. Some information is made available as a matter of course, through the GSA's Publication Scheme (http://www.gsa.ac.uk/about-gsa/contact-us/foi-requests/). Other information would be available on request, and most of the information categorised as ***internal*** would be released to the public if a written request for the information were received by the Glasgow School of Art.
There are exemptions within FOISA which mean that there is some information which the Glasgow School of Art is not required to release. Examples of exemptions include information that contains personal information, confidential information, commercially sensitive information, information which could endanger the health and safety of an individual, etc.

For further information about Freedom of Information, please see the GSA's Freedom of Information web page at the following link: http://www.gsa.ac.uk/about-gsa/contact-us/foi-requests/

Appendix B: Data classification framework

	Data classification			
	Public	**Internal**	**Restricted**	**Highly sensitive**
Description	May be viewed by all members of the public	May be seen by all members of the GSA, but would not normally be available to people outwith the institution	Accessible by restricted members of staff or students, on a "need to know" basis. Often containing sensitive personal data	Accessible only to designated or relevant members of staff, due to its potential impact on the GSA (including financial or reputational damage), or its potential to have an adverse effect on the safety or wellbeing of individuals
Level of risk if released inappropriately	none	low	medium	high
Transmission of data	No restrictions	Information may be placed in shared folders, and sent via internal email	Should only be placed in folders with restricted access. Care should be taken when emailing, and acceptable encryption used if appropriate. Items sent by internal mail should be placed in sealed envelopes	Should only be transmitted electronically in an acceptably encrypted format. Hard copies of documents should be hand delivered internally. External postage should be signed for
Disposal ***See also RRS where available***	No restrictions. Recycle where possible	Most paper documents can be placed in paper recycling. Delete electronic media when no longer required	Shred or use confidential waste bags for paper documents. Ensure electronic media is wiped clean	Shred paper documents and permanently destroy electronic media
Examples of information and data	• Any information on the GSA website and related websites • Information contained within the GSA's Publication Scheme [2] • Information for prospective and current students • Publications • Press releases • Published research	• Internal correspondence • Committee papers • Internal policies and procedures	• Documents containing sensitive personal data • HR data • Student data • Reserved committee business • Draft reports, papers, policies • Financial information (not disclosed in Financial Statements) • databases and spreadsheets containing personal data • data on research participants	• Confidential commercial contracts • Passwords • Disciplinary proceedings • Security information • Legally privileged information • Medical records

[2] http://www.gsa.ac.uk/about-gsa/contact-us/foi-requests/

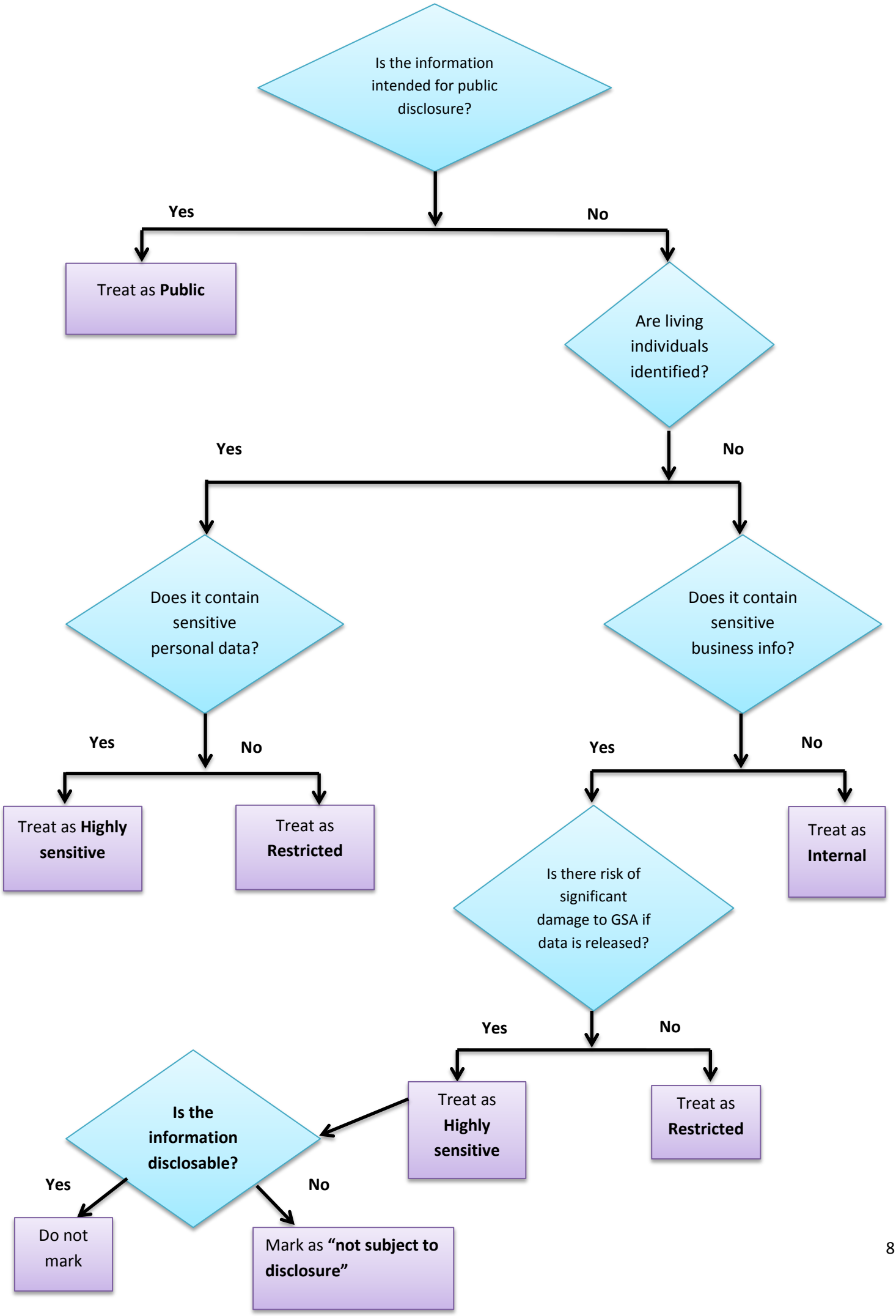
Appendix C: Data classification decision support flow chart

The data classification decision support flow chart on the following page can be used to help determine which of the following data classification categories should be applied to each piece of information:

- public
- internal
- restricted
- highly sensitive

Please note that it is possible for one piece of information or document to have different classifications throughout its lifetime; for example, commercially sensitive information may become less sensitive over time.

Where there is a possibility of ambiguity over the status of a piece of information, it is the responsibility of the owner of that information or document to ensure that they make anyone who has access to it aware of its status. This is particularly the case for **restricted** and **highly sensitive** information; and whilst there is no requirement to mark every single document with a data classification category, **highly sensitive** data should, where practicable, be marked as "**not subject to disclosure**". Whilst this in itself does not make the information secure, it assists with appropriate information handling.


Is the information intended for public disclosure?
Yes
No
Treat as **Public**
Are living individuals identified?
Yes
No
Does it contain sensitive personal data?
Does it contain sensitive business info?
Yes
No
Yes
No
Treat as **Highly sensitive**
Treat as **Restricted**
Is there risk of significant damage to GSA if data is released?
Treat as **Internal**
Yes
No
Treat as **Highly sensitive**
Treat as **Restricted**
Is the information disclosable?
Yes
No
Do not mark
Mark as **"not subject to disclosure"**