Algospark Data Classification and Handling Guidance

Version: 0.03
Last updated: 6 June 2019
By Darren Wilkinson

Purpose
A framework for classifying and handling data to ensure that the appropriate degree of protection is applied to all data held. The classification of data will help determine how the data should be accessed and handled and ensure that sensitive and confidential data remains secure. The correct classification of data is important to help ensure the prevention of data leaks and minimising the impact of such leaks if they do occur.

Scope
This guidance covers all data or information held, in physical or electronic format, including documents, spreadsheets and other paper and electronic data and should be applied by all staff. This guidance is also applicable to associates, agency staff, data processors, third parties and collaborators. They are responsible for assessing and classifying the information they work with and applying appropriate controls. Members of staff working with these types of associates and third parties have a responsibility to bring this guidance to their attention.

Categories
Data classification is based on the level of sensitivity and the impact on Algospark and clients should that data be disclosed, altered, lost or destroyed without authorisation. The classification of all data into different categories ensures that individuals who have a legitimate reason to access a piece of information are able to do so, whilst at the same time ensuring that data is protected from those who have no right to access the information. The classification will guide the appropriate security and technical controls required to be in place. All data owned, used, created or maintained within the University should be categorised into one of the following four categories: Public, Confidential, Sensitive or Secret.

Responsibility and Ownership
All data and information must be held in an information asset and therefore would be included in the Information Asset Register held by the Data Protection Officer. The Information Assets are the responsibility of the Information Asset Owner. Information security is everyone's responsibility and therefore all staff have a responsibility to protect data and information. All staff should have an awareness of the four data classifications and the way in which the data and information in each classification should be handled.

Removal of Information Assets
Staff must not remove sensitive information assets (Confidential/Strictly Confidential/Secret) from the Algospark or client premises without the prior agreement or consent from the appropriate authority. In the event of authorised removal of information assets, it is your responsibility to adequately protect the information assets at all times and to return them in the condition in which they were originally provided to you.

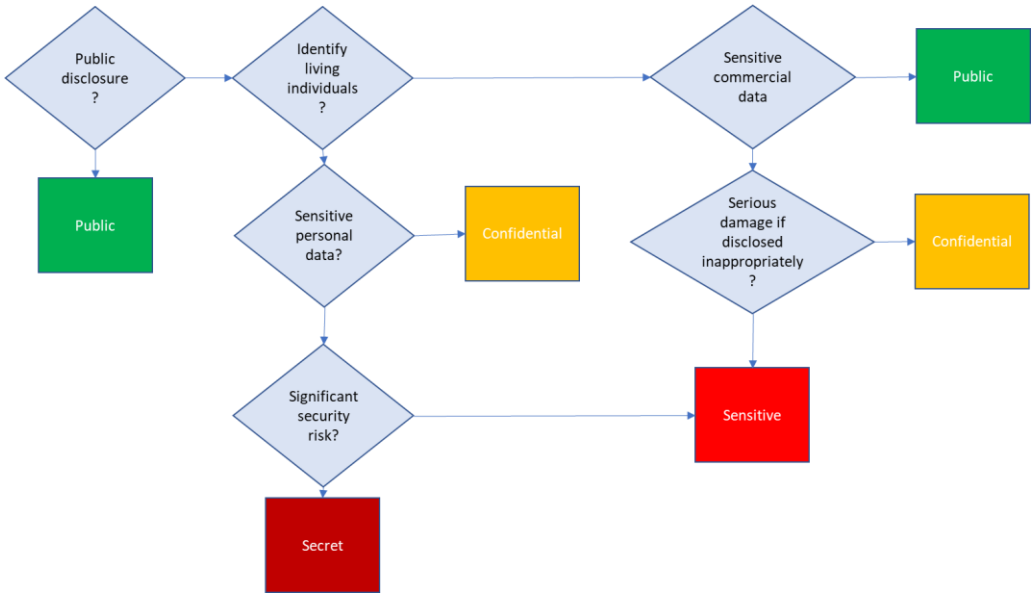
Secure Disposal
Information assets which are considered sensitive (i.e. Secret, Confidential or Restricted), and are no longer needed or are deemed to have reached "end of life" must be securely disposed of. There are several ways to dispose of information assets and equipment. These include:

- Secure shredding (Cross cut shredders)
- Confidential waste disposal bins (Paper based). Confidential waste bins are available within company premises and are an alternative to secure shredding.

Table 1: Types of information, access, storage, transmission and disposal

	Public Data	Confidential Data	Sensitive Data	Secret Data
Description	Info that requires no protection: open and unclassified; likely to already exist in public domain. Examples: ads, press releases, blog posts, published info.	Info only available to staff to carry out roles. Examples: non-sensitive personal data, policies & processes, tenders, bids, proposals	Personal data, commercial data, legally privileged or under embargo. Examples: personal data, research, usernames, passwords, payment details, financial data, medical info, info under embargo.	Official secrets or data with potential to cause catastrophic harm. Example: obtained under Official Secrets Act or equivalent obtained as part of project.
Impact if info made public	None	Low: minor reputational or financial damage; minor privacy breach for individual	Medium: substantial reputational or financial damage; substantial privacy breach for individual	High: significant reputational or financial damage; distressful privacy breach for individual
Security marking	Not required	Marked “Confidential”	Marked “Sensitive”	Marked “Secret”
Electronic Storage	Algospark authorised secure computers, Microsoft OneDrive. Azure storage, USB hard drive.	Algospark authorised secure computers, Microsoft OneDrive. Azure storage, USB hard drive.	Algospark authorised secure computers. Azure storage, not stored on Dropbox. Consider encrypting documents with passwords. Passwords stored in password vaults.	Only Algospark authorised secure computers.
Hardcopy Storage	No restrictions	Locked office or lockable cabinet / drawer	Restricted access room with lockable cabinet / drawer	No hard copy
Algospark Email	Yes	Internal email no encryption required, external encrypted files required.	Internal email no encryption required, external encrypted files required.	Not emailed.
Post	Yes	Marked Confidential	Marked Confidential & hand delivered	Not to be posted.
Personally owned mobile devices	Yes	Not be stored	Not permitted	Not permitted
Removable media	No restrictions	Encrypted storage with strong password	Encrypted storage with strong password	Encrypted storage with strong password
Hardcopy disposal	No restrictions, recycle where possible.	Shredding or confidential waste bags	Cross shredding then into confidential waste bags	Cross shredding then into confidential waste bags

Diagram 1: Data Classification Flow:



General Data Protection Regulations Definitions

- "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as: a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
- "Sensitive Personal Data" are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Data relating to criminal offences and convictions are addressed separately (as criminal law lies outside the EU's legislative competence).