Information Classification Procedures

Effective Date: February 2025
Supersedes: Information Classification Procedures (May 2019 version)
Last Review: January 2025
Next Review: January 2026

1. Purpose and scope

1.1 The Information Classification Procedures have been developed to support King's information security, records management, and data governance policies. These procedures are intended to help creators, users and managers of University information to assess its sensitivity and apply an appropriate classification level.

1.2 There are two tiers of classification levels in use, these are King's standard classification levels (for most University information) and Government security classification levels (for Government contracts).

2. Classification levels

2.1 King's standard classification levels

2.1.1 The standard classification levels for routine University business are External, Internal, Restricted and Highly Restricted. Each level is described in detail below.

King's standard classification level	Description	Examples
External	Information intended to reach the widest possible audience. There are no restrictions on who can access the information. The information has a use for audiences outside King's. Release of the information will have no adverse effect on King's. There is a need to publicly disclose the information in accordance with legislative requirements for accountability and transparency, such as the Freedom of Information Act 2000.	Marketing and publicity materials. Press releases and information about public events. Course information and prospectuses. University policies, procedures, regulations, and strategies. General information about Faculties and Departments, including programmes, contact details, news and events. Annual reports and financial statements. Minutes of senior committees and other information that King's is

		required to make publicly available. Open access research publications, papers, articles and presentations.
Internal	Information intended for King's students and staff. Information of limited use or interest to external audiences. Release of the information will have no adverse effect on King's. There is no requirement for information to be publicly available.	Staff and departmental organisational charts. Timetabling and room booking information. Staff and student email directories. Internal emails, messages, notices and newsletters. Information about internal events. Internal procedures, guidance and forms.
Restricted	Information intended for use by a limited group of King's staff. Information of little use or interest to wider groups. Restricted information includes personal data and financial information but not highly confidential or sensitive material. Release of the information could have an adverse effect on King's.	Most information held on University servers or in student and staff personal storage (OneDrive). Most information held in Microsoft 365 storage, including SharePoint and Teams sites. Routine records relating to students and staff, including data held in SITS and on HR systems. Records of departmental committees and team meetings. Databases or spreadsheets used for logging enquiries or contact details. Routine financial information, such as purchase orders and invoices. Teaching materials and content on KEATS. Most research records and data.
Highly Restricted	Information strictly for use by a specified group of authorised University staff. Information that is of no use to wider members of the University or external audiences. Information that is personal, confidential, sensitive, or of financial or commercial value.	Special category personal data relating to staff and students as defined by the University Data Protection Policy. Disciplinary, complaint and misconduct investigations. Confidential financial information including personal bank account details. Note that cardholder data

	Release of the information would have an adverse effect on King’s.	(for any payment card type) is classified as highly restricted but must not be retained or processed on any King’s system. Information relating to security of University buildings and systems. Confidential, high-level planning and strategy documents. Information on controversial research. Information with commercial value. Sensitive information on research participants.

2.2 Government security classification levels

2.2.1 The Government security classification levels are Official, Official-Sensitive, Secret and Top Secret. Further information and guidance on application of government classifications is available in the Government Security Classifications Policy.

Government security classification level	Description	Examples
Official	Most information that is created, processed, sent or received in the public sector and by partner organisations. In some cases, there may be damaging consequences for individuals or organisations if data is lost, stolen or published. Release may breach undertakings to maintain confidentiality or statutory restrictions on information disclosure.	All routine day-to-day business, including, but not limited to, policy development, service delivery, legal advice, personal data, reports, statistics, administrative data, commercial information, financial data (including tenders, procurement, and contracts), and committee minutes and papers.
Official – Sensitive	Information which is particularly sensitive, but still classed as Official. Loss or compromise could have damaging consequences for individual and organisations. Information with an enhanced level of risk where additional controls are required.	Sensitive corporate or operational information including, but not limited to, organisational change, security, contentious issues, investigations or court proceedings, case files, commercially sensitive data, diplomatic or international business or negotiations, sensitive personal data.

Secret	Very sensitive information that requires heightened protective measures, including the use of secure networks on secured dedicated physical infrastructure, to defend against determined or highly capable threats. Disclosure of information may result in serious harm or risk.	Any information relating to national security. Intelligence and investigations relating to individuals of interests to security agencies. Security or vetting information. Details of high-level visits. Personal data or case files where there is a specific threat to the life or liberty of an individual such as protected witness scheme records.
Top Secret	Information of the highest sensitivity relating to national security and subject to highly capable threat sources. Information that requires an extremely high assurance of protection with the use of secure networks on highly secured dedicated physical infrastructure.	Any information relating to national security, counter-terrorism, cyber security or protected witnesses.

3. Managing classified information

3.1 The table below provides advice on securely handling and managing data in accordance with University processes for data storage, access, transfer and disposal.

King's standard classification level	Storage	Access	Transfer	Disposal	Remote working
External	Digital – OneDrive or SharePoint sites. Paper – Office filing.	Public. Digital – External website or external SharePoint sites. Paper – Public dissemination.	Internal or external transfers with no restrictions.	Digital – Delete Paper – Recycle	No restrictions.
	Storage	Access	Transfer	Disposal	Remote working

Internal	Digital – OneDrive or SharePoint sites. Paper – Office filing.	King's authenticated login or ID. Digital – King's intranet, internal emails or newsletters. Paper – Internal dissemination.	Digital – King's email or link to internal OneDrive or SharePoint sites. Paper – Internal or external mail.	Digital – Delete Paper – Recycle	Digital – Use King's login to access intranet, email and storage. Paper – No restrictions.
	Storage	Access	Transfer	Disposal	Remote working
Restricted	Digital – Follow IT guidance and advice on the Digital Skills Hub. Paper – Local filing and office storage, lockable where personal data is involved.	Digital – Authenticated logins or permissions for relevant groups, password protection where applicable. Paper – Physical access to paper files restricted to relevant groups.	Digital – Follow King's guidance on sharing or transferring files. See advice on the Digital Skills Hub for sharing files via OneDrive and Sharepoint. Paper – Internal mail, clearly addressed and job number for delivery obtained from Estates, or registered external mail.	Digital – Delete or overwrite with updated version. Secure disposal of electronic media. Paper – Sealed confidential waste bin or shred.	Digital – Follow IT guidance and policies on accessing files remotely. Paper – Restrict unauthorised viewing or access. Do not leave unattended in a public place.
	Storage	Access	Transfer	Disposal	Remote working
Highly Restricted	Digital – Follow IT guidance and advice on the	Digital – Authenticated logins, passwords or permissions for	Digital – Follow King's guidance on sharing or	Digital – Overwrite and delete. Secure disposal of	Digital – Follow IT guidance and policies on

	Digital Skills Hub. Note that no storage of cardholder data is permissible. Paper – Locked filing areas.	protected documents. Note that no storage of cardholder data is permissible. Paper – Access only to key holders.	transferring files. See advice on the Digital Skills Hub for sharing files via OneDrive and Sharepoint. Note that no documents containing cardholder data may be transferred. Paper – By hand, secure courier or registered mail.	electronic media. Paper – Sealed confidential waste bin or shred to standard BS EN 15713. Check credentials of confidential waste contractor.	accessing files remotely. Avoid downloading documents to personal devices. Do not leave unattended and use encryption on personal devices. Paper – Avoid removal from King's premises. Avoid making unnecessary copies and do not leave unattended in a public place.
Government security classification levels	Storage	Access	Transfer	Disposal	Remote working
Official	Digital – Follow IT guidance and advice on the Digital Skills Hub. Portable digital media to be approved and encrypted. Laptops to be stored securely. Paper – Locked filing areas.	Digital – Controlled access. Permissions for relevant groups or password protection. Paper – Physical access to paper files restricted to relevant groups.	Digital – Email or follow King's guidance on sharing or transferring files. See advice on the Digital Skills Hub for sharing files via OneDrive and Sharepoint. Paper – By hand, post or courier.	Digital – Secure disposal of electronic media. Paper – Shred and recycle	Digital – Encrypted and Government approved laptops and portable media to be used. Ensure information cannot be overlooked.

	Storage	Access	Transfer	Disposal	Remote working
Official - Sensitive	Digital – Follow IT guidance and advice on the Digital Skills Hub. Portable digital media to be approved and encrypted. Documents should be marked *Official – Sensitive* and classification included in metadata. Paper – Locked filing areas.	Digital – Controlled access. Permissions for relevant groups or password protection. Paper – Physical access to paper files restricted to relevant groups.	Digital – By encrypted email only to known contacts on a need-to-know basis. Paper – By hand, registered mail or tracked courier.	Digital – All portable media to be shredded or destroyed by an approved contractor. Paper – Confidential waste or shred.	As Official, plus: Digital – Documents must not be opened in a public area. Papers or portable media must not be left unattended. Documents, laptops and portable media to be stored in a locked drawer or cabinet.
	Storage	Access	Transfer	Disposal	Remote working
Secret	Digital – Not suitable for storage on King's network. Paper – Secure locked storage with approved locks. All documents and movement of documents to be logged.	Digital – Access only via stand-alone Government Secret system. Paper – Access only to individuals with need-to-know and security clearance.	Digital – No email or digital transfer permitted. Paper – By hand by staff with appropriate security clearance and movement of document logged. Receipt obtained for delivery. For external mail use approved registered mail, approved	Digital – Contact IT Cyber Security Team for advice. Paper – Shred using approved contractor or approved office shredder. All shredding must be witnessed by another staff member. Record of document destruction	Risk assessment and only take what is necessary. Documents must be transported in a locked container. Remote location must have a Government security approved storage container.

			tracked courier or Government courier.	must be logged.	
	Storage	Access	Transfer	Disposal	Remote working
Top Secret	Not suitable for storage on King’s network. Paper – Two secure barriers (i.e. locks, combinations, alarms) and approved locks and cabinets. All documents and movement of documents to be logged.	Digital – Access only via stand-alone Government Top Secret system. Paper – Access only to individuals with need-to-know and security clearance.	Digital – No email or digital transfer permitted. Paper – By hand by staff with appropriate security clearance and movement of document logged. Receipt obtained for delivery. For external mail, risk assessment and special handing required.	Digital – Contact IT Cyber Security Team for advice. Paper – Shred using approved contractor or approved office shredder. Implement control measures to witness and record destructions.	Only permitted in exceptional circumstances with approval and guidance from Government security officers.

4. Further information

4.1 For queries regarding online storage, data security and technical issues, please contact IT Services; email 88888@kcl.ac.uk.

4.2 For advice on the Government information classification scheme or secure management of Government data, contact the Cyber Security Team; email 88888@kcl.ac.uk

4.3 For advice on management of personal data, contact Information Compliance; email info-compliance@kcl.ac.uk.

4.4 For advice on management of University records, contact Corporate Records Management, email records-management@kcl.ac.uk.

5. Approval and review

5.1 These procedures were approved by University Executive on 20 February 2025 and are subject to annual review.