

Section 3: Data Classification and Data Handling Responsibilities

Based on the Data Protection Acts 1988 and 2003, the FOI Act 2014, and the Data Protection Commissioner Code of Practice:

Data Classification	Description	Data Owner & Decision Maker	Data Handling Responsibilities				
			Collection	Storage	Transmission	Processing	Destruction
Public Non-Personal Data	DIT information which is not prohibited by law to publish.	Head of Function	N/A	N/A	By the appropriate Head of Function	N/A	N/A
Private Non-Personal Data	DIT information which is subject to a confidentiality agreement, or the concerns financial, commercial, or intellectual property matters the disclosure of which would cause material loss.	Head of Function	As authorised by the Appropriate Head of Function.	<ul style="list-style-type: none"> • Physical documents subject to physical security in locked storage. • Computer data subject to IS security password or encryption. 	<ul style="list-style-type: none"> • Physical documents transmitted with physical security measures, by informed employees, or courier firms with confidentiality agreements with DIT. • Computer data only emailed subject to IS security or encryption. 	<ul style="list-style-type: none"> • On the authority of the appropriate Head of Function. • By third parties on the authority of the appropriate Head of Function, and subject to a confidentiality agreement. 	<ul style="list-style-type: none"> • Data is destroyed on Authorisation of Head of Function. • Function's Data or Records Retention Schedule is updated on destruction.

Data Classification	Description	Data Owner & Decision Maker	Collection	Storage	Transmission	Processing	Destruction
Personal Data	DIT data relating to a living individual who may be identified from the data.	Head of Function	<ul style="list-style-type: none"> Collected with the consent of the Data Subject (relevant individual) for the specified lawful purpose intended. 	<ul style="list-style-type: none"> Subject to appropriate physical locked storage and IS security password or encryption. 	<ul style="list-style-type: none"> Data is transmitted only as necessary for the purpose it was collected. 	<ul style="list-style-type: none"> Data is processed only in ways compatible for the consented purpose for which it was initially given. 	<ul style="list-style-type: none"> Data is destroyed on Authorisation of Head of Function when its consented purpose is fulfilled.
Sensitive Personal Data	DIT data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership, personal data of a financial nature.	Head of Function	<ul style="list-style-type: none"> Ensure data collected is adequate, relevant, not excessive, and retained no longer than necessary for the specified purpose. 	<ul style="list-style-type: none"> Subject to Data Access Request from the Data Subject (relevant individual). Subject to being kept accurate and up to date. Subject to retention for no longer than is necessary for the consented specified purpose. 	<ul style="list-style-type: none"> Physical documents transmitted with physical security measures, by informed employees, or courier firms having confidentiality agreements with DIT. Computer data only emailed subject to IS security password or encryption. 	<ul style="list-style-type: none"> On the authority of the appropriate Head of Function. By third parties on the authority of the appropriate Head of Function, and subject to a confidentiality agreement. 	<ul style="list-style-type: none"> Function's Data or Records Retention Schedule is updated on destruction.