UNIVERSITY OF BIRMINGHAM

Unstructured Personal Data – Guidance

Background

This guidance concerns unstructured personal information (PII) in documents, messages and other file types stored in shared network drives, Sharepoint libraries, email accounts and other repositories and services both on-site and in the cloud. It covers the management of personal data that is within scope for privacy laws such as the Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR).

Enterprise applications that process structured data in databases can automate the retention and disposal of data without manual intervention but shared file stores, email accounts, web content management systems, cloud storage services holding 'unstructured' data generally do not. Therefore it is up to individuals to manage their own unstructured data in a way that complies with the law.

Where little automation is currently available, each member of staff is responsible for managing their own documents, email messages, web pages and other artefacts containing personal data. Content management applications such as Sharepoint offer automated retention and disposal processing and these should be used where available. IT Services are investigating other potentially useful tools such as Data Loss Protection (DLP) software but these are not available yet.

Purpose

To provide basic guidance on managing personal data held in documents, email messages, web pages and other file types on shared network drives, content and document management applications.

Best Practice

	Practice	Rationale
1.	Collect only personal data for which there is a real business need and a valid legal justification (e.g. legal or contractual obligations, public interest, legitimate interest, consent).	GDPR requires us to have a valid legal basis for processing and storing personal information. Refer to Legal Services' Privacy Notices [3] for appropriate legal justification.
2.	Restrict the data items collected to what is strictly necessary for the purpose in hand.	Data that is not strictly required for the purpose in hand may not be justifiable under GDPR.
3.	Do not reuse data for purposes other than that for which it was collected.	Unforeseen reuse could be a breach of the GDPR.
4.	Each member of staff is responsible for managing, including disposal when no longer needed, the personal data in their own documents, email accounts etc.	Where no automated facilities exist, the user must dispose of data manually. Refer to Privacy Notices [3] for retention periods of various types of personal data.
	Examples: • CVs of job applicants should be deleted as soon as they are no longer needed or 7 months after the recruitment exercise ends. Unless anonymized, in which case GDPR does not apply and there is no specific time limit. • Emails and documents containing staff data such as salaries, email addresses should be deleted when no longer needed but there is no defined upper time limit at the time of writing.	
5.	Shared email accounts, Sharepoint sites and network drives are the responsibility of the Head of Section or designated owner or data steward.	The same rules apply to shared facilities as for personal accounts.
6.	Identify files and documents containing personal data and assign them the 'Confidential' classification as documented in the Information Classification Standard [2]	Personal data is confidential and must be clearly marked and managed accordingly. Documents should be marked 'Confidential' on every page.

	Practice	Rationale
7.	Encrypt personal data in transit over data communications networks. For email, use message encryption [4].	Personal, and other confidential, data must be encrypted in transit if technically feasible. This means using email encryption, uploading to and downloading from, secure websites using the HTTPS protocol not HTTP.
8.	Avoid storing personal data on desktops, laptops, tablets or smartphones.	All types of confidential data should be kept in central data stores, although working or cached copies may be downloaded to personal devices provided access is protected by user authentication and data encryption. University standard laptops and mobile devices have full disk encryption by default.
9.	Avoid storing personal data in cloud-based services that are not hosted in the UK or EU/EEA.	The GDPR states that personal data must not be exported unless 'equivalent protection' is provided. Many US-based services rely on the US/EU Privacy Shield, which is valid for now but could be challenged in court.

Further Information

Contact Legal Services (https://www.birmingham.ac.uk/privacy) or IT Security (https://itsecurity.bham.ac.uk).

Glossary

DLP	Data Loss Prevention software identifies and tracks data such as credit card numbers, bank details or personal data.
GDPR	European Union General Data Protection Regulation.
HTTP	Hypertext transfer protocol.
HTTPS	HTTP with encryption (usually indicated by padlock symbol in web browsers).
PII	Personal information or data.

References

[1]. Information Security and Management Policy
https://intranet.birmingham.ac.uk/it/documents/public/Information-Security-Policy.pdf

[2]. Information Classification Standard
https://collaborate.bham.ac.uk/it/itas/Published/Standards/Information%20Classification%20Standard.pdf

[3]. Privacy Notices
https://www.birmingham.ac.uk/privacy

[4]. Secure Email Information
https://collaborate.bham.ac.uk/it/itas/Published/Guidelines/Secure%20E-mail%20Information.pdf