INFORMATION CLASSIFICATION

Manchester Metropolitan University

PUBLIC

Intended for public distribution with no specific security handling.

- Minimal or no risk
- No discomfort to individuals
- No breach of statutory obligation

INTERNAL

Relating to routine business operations and services.

- Minor reputational risk
- Short-term disruption
- Short term discomfort to individuals
- Commercial disadvantage or loss
- Possible breach of statutory obligation

SENSITIVE

Clear elevated sensitivity due to its legal, contractual or business value.

- Serious reputational risk
- Danger to personal safety
- Major breach of a statutory obligation
- Prolonged distress, discomfort or embarrassment to an individual
- Serious commercial disadvantage or loss
- Long-term disruption

Access

Available to users who have a legitimate business need to see the information

Labelling

All copies should be visibly marked 'SENSITIVE'

Destruction

Information should be destroyed in a way that makes reconstitution difficult

Remote Access

Should only be held on systems requiring VPN access and two-factor authentication

Storage

- Data should remain in the appropriate University systems
- Can be kept on University portable devices temporarily if encrypted/ password protected
- Cannot be kept on personal devices

Communication

- Not to be communicated externally
- Exercise discretion when discussing in public or by telephone
- Keep details to a minimum

Off-Site Working

- Removal of physical assets should be confirmed with the asset owner
- Physical assets should be protected in transit, not left unattended, and stored securely
- Precautions should be taken when working remotely or in public places

Sharing

- Internal distribution should follow the need-to-know principle
- Not to be shared via OneDrive
- Can use iCRED and shared MMU drive if access is appropriately restricted
- Take care when sharing information with external partners or the public