Status: Published
Classification: Restricted
Date Updated: 10/06/2020

Information Handling Policy

Version: 1.7

This document is classified as RESTRICTED

Revision history

Date	Version	Author	Summary of changes
11/01/2017	1.0	Rahim Hankin	Version 1 issued
16/07/2017	1.1	Rahim Hankin	Various clauses updated
18/05/2019	1.2	Rahim Hankin	Addition of decision tree diagram
17/06/2019	1.3	Rahim Hankin	Addition classification model
24/06/2019	1.4	Rahim Hankin	Changes to wording
26/06/2019	1.5	Rahim Hankin	Changes to the Decision Tree diagram
26/11/2019	1.6	Rahim Hankin	Updated graphic on cover page
10/06/2020	1.7	Rahim Hankin	Reviewed and updated

Approvals

Date	Version	Approver name	Approver title
16/07/2018	1.1	Rahim Hankin	Technical Director
16/07/2018	1.1	Mehul Kotecha	Commercial Director

IMPORTANT NOTE:
In the event of an inconsistency between this document and the FDM Technology Security Policy, the FDM Technology Security will take precedent and should always be used.

Table of contents

Revision history 2
Approvals 2
1 Purpose, scope and users 5
1.2 Reference documents 5
2. Information Handling Policy 6
2.1 Policy introduction 6
2.2 Management of information 6
2.3 Classification of information 7
2.4 Disposal of information 9
2.5 Removal of information 9
2.6 Information on screens, desks and printers 10
2.7 Storage of information 10
2.8 Back-ups of information 11
2.9 Dissemination and exchange of information 12
2.10 Information in application systems 14
2.11 Compliance 14
3. Handling Electronic Information 15
4. Classification Model 17
4. Validity and document management 18

1 Purpose, scope and users

The purpose of this document is to provide guidance on handling information; including how it should be protected and how it should be shared. FDM generates and holds a variety of information that must be protected against unauthorised access, disclosure, modification and/or other misuse. Different types of information require specific security controls requiring proper classification of information assets is therefore vital to ensure effective information security and management practices are adhered to.

This policy describes the expectations and principles relating to handling information. It is forms part of the FDM Information Security Management System. Adhering to this policy will help ensure correct information classification and handling methods are applied.

This policy applies to all FDM staff and to all information assets generated, processed or held by FDM. All FDM staff, and where applicable, suppliers and third parties associated with the FDM handling information/data on behalf of FDM, must comply with any 'explicit agreements', 'legal compliance requirements' or 'implicit expectations' when handling information. Such information may include information or data which is considered confidential, sensitive or has financial or reputational value, whether under Data Protection law or by virtue of FDM's classification of data as Secret, Confidential, Restricted or Public; personal data, including special category data, as defined by GDPR/Data Protection Act 2018; and information or data that is subject to a formal agreement with an external body that specifies secure handling requirements should be prioritised.

Individuals have a personal responsibility to ensure the correct management and protection of information and may be personally liable for any breaches in information security that arise from a failure to take appropriate measure to do so. In the event of doubt please contact your Manager or the Head of Information Security and refer to the FDM Staff Handbook and FDM Technology Security Policy.

1.2 Reference documents

Ref No	Control Statement
1.2.1	Documents referred to in this document are: • FDM Information Security Management System • FDM Supplier Security Standard • FDM Technology Security Policy • Data Protection Act 2018/GDPR • FDM Staff Handbook • Acceptable Use Policy

2. Information Handling Policy

2.1 Policy introduction

System Owners, Information Asset Owners and Managers should appropriately manage any security risks relating to the handling of information for which it has responsibility.

Ref No	Control Statement
2.1.1	Information Asset Owners and Data Processors should: • Identify information that must be protected and ensure that the responsibility for doing so is assigned. This should be done systematically by Managers and System Owners, groups and individual members of staff as applicable. • Ensure that those responsible for managing the security of information take into account confidentiality and value of the information they are managing when determining what security measures to use. • Ensure that both the information owners and those responsible for handling that information, where different, have the same understanding of the security requirements, expectations and limitations. • Ensure that those with responsibility for secure handling of information are offered training, guidance and support. • Ensure that staff are generally aware of the need to take a responsible approach to handling information and provide them with guidance. • Ensure that information is managed continuously until it is destroyed, or until that responsibility is transferred to another organisation.

2.2 Management of information

Ref No	Control Statement
2.2.1	All Information Assets and Data Processing activities should be recorded on FDM's Information Asset Register which records our Assets and Data Processing activities; supports the secure handling of information; compliance with GDPR/ Data Protection Act 2018; Information risk management and business continuity planning.
2.2.2	Each member of staff should review their Information Assets and Data Processing activities at least annually if not more frequently to keep the Information Asset Register up to date.

2.2.3	Each member of staff must ensure that they are aware of the items and classes of information they are responsible for handling.
2.2.4	The information asset list is a combination of specific information items, types of information, processes, computer systems, storage devices or locations where information is stored.
2.2.5	The information asset list should record useful information about each information asset identified including: description or descriptive name, location(s) of the information asset, staff member with responsibility for handling the information or managing the information asset, the type(s) of information stored or processed, origin or ownership of the information stored or processed, the importance of the information stored or processed, retention periods and any special or non-standard security measures required.
2.2.6	Information Assets should be reviewed and updated annually, and new assets and data processing activities recorded when received.
2.2.7	A basic non-technical review of how the information involved is handled should be performed to minimise problems that may to a security incident.
2.2.8	Information Asset Owners and Data Processors should: • Ensure that access rights to data (files, documents, web pages, etc.) are configured correctly. • Ensure that files of personal and special category data (both physical and electronic) are stored securely and access is well controlled. • Ensure that files of personal and special category data are retained in accordance with retention schedule requirements and are deleted when no longer in use. • Ensure that security and access control records are maintained following staffing change events (such as a resignation or change in role of an individual). Ensure that data is owned, and that ownership is transferred following staffing change events.

2.3 Classification of information

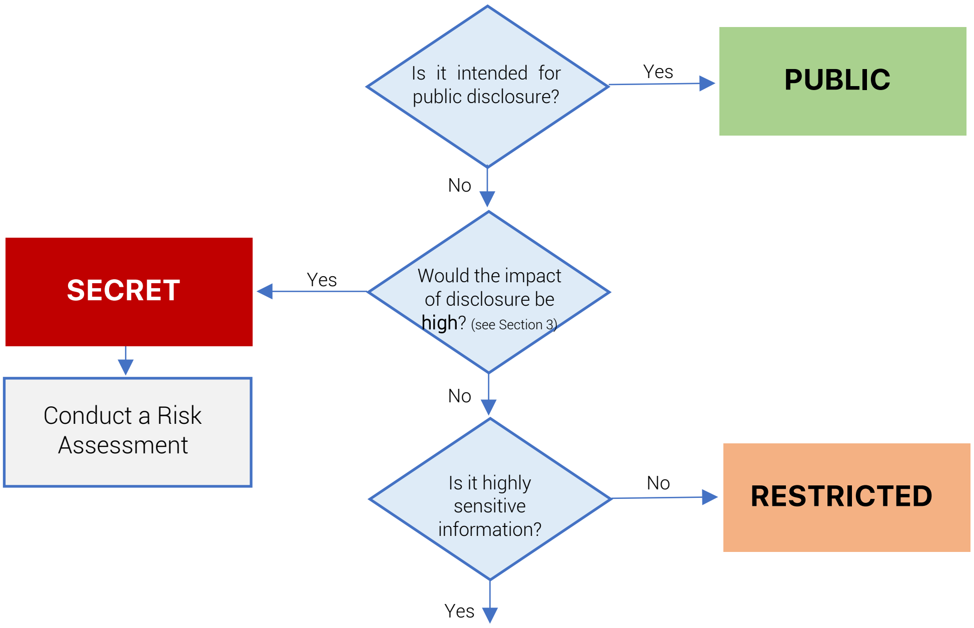
All information generated, processed or held by FDM is subject to classification. FDM follows its own Data Classification standards with four levels of data classification – Public, Restricted, Confidential and Secret. The table below is provided to assist Information Asset Owners to determine the different levels of security required (please also see Sections 3 & 4 below):

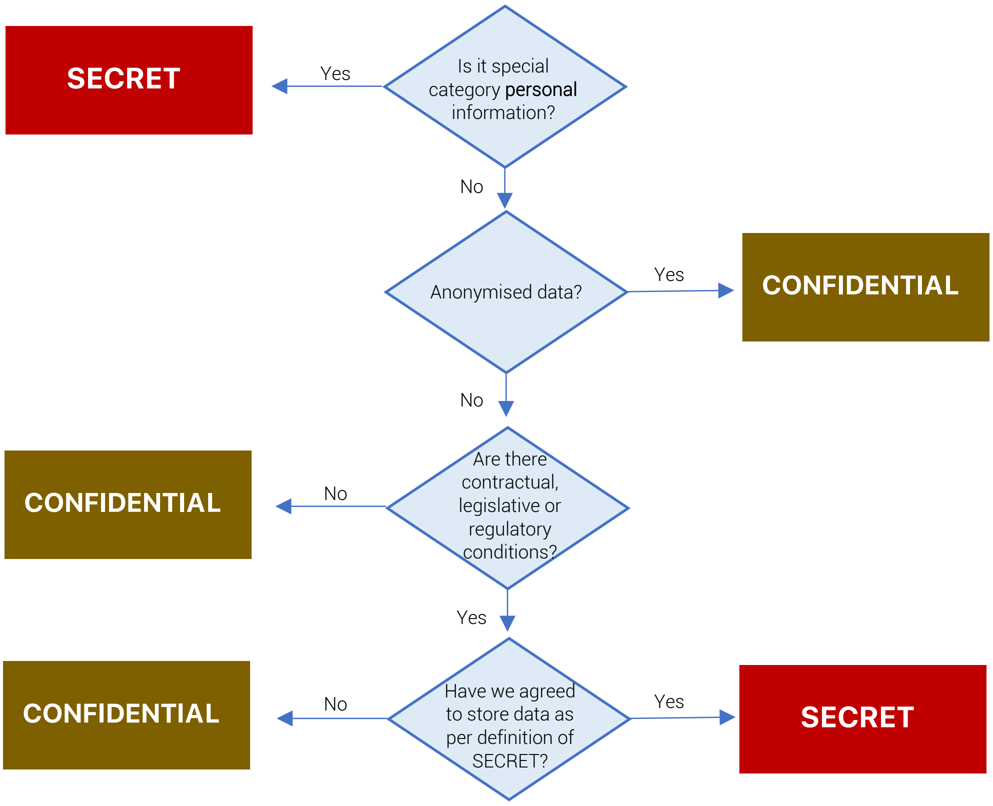
Ref No	Control Statement
2.3.1	To ensure risks are properly identified, and adequate controls are implemented all systems and information assets must have an assigned FDM owner and be classified (see Section 4).
2.3.2	**Public:** Information which is available to the public.
2.3.3	**Restricted:** Information which if lost or wrongly disclosed may cause limited negative effects for FDM.
2.3.4	**Confidential:** Information which if lost or wrongly disclosed could cause distress to our clients or people or damage the interests of FDM.
2.3.5	**Secret:** Information which if lost or wrongly disclosed could cause very serious damage to the interests of FDM, our clients, people, suppliers or business partners.

FDM's Information Security Management System details that information should be classified and labelled according to its sensitivity for all documents that are Restricted, Confidential or Secret in nature. This itself does not make the information secure, it assists appropriate information handling; it clearly indicates that such documents, or their contents, should not be distributed without due authorisation or consent from their owner.

Distribution of confidential or secret information must be controlled in accordance with authorisation.

Classification decision tree diagram:


Is it intended for public disclosure?
Yes
PUBLIC
No
Would the impact of disclosure be high? (see Section 3)
Yes
SECRET
Conduct a Risk Assessment
No
Is it highly sensitive information?
No
RESTRICTED
Yes


SECRET
Yes
Is it special category personal information?
No
Anonymised data?
Yes
CONFIDENTIAL
No
CONFIDENTIAL
No
Are there contractual, legislative or regulatory conditions?
Yes
CONFIDENTIAL
No
Have we agreed to store data as per definition of SECRET?
Yes
SECRET

2.4 Disposal of information

Ref No	Control Statement
2.4.1	Electronic data must be securely and irretrievably deleted. When disposing of removable media or computing equipment containing hard drives these must first be securely wiped of information. The Head of IT must be contacted for equipment disposal. Simple file deletion alone is inadequate for ensuring that files cannot be recovered and must not be relied on in and of itself. Further information is available in the FDM Technology Security Policy and Information Security Management System.
2.4.2	Retention periods of information held must be determined in advance by the Information Asset Owner, according to the business needs and other responsibilities such as legal, contractual, moral. Information should not be kept longer than it is required for business use unless required for archival or to satisfy contract or statutory obligations.

2.5 Removal of information

Ref No	Control Statement

2.5.1	Individuals must be authorised, by the Head of Department, to remove confidential or valuable FDM information offsite or to insecure locations. (It should be determined locally whether or not repeated authorisation is required by those undertaking a specific routine activity.)
2.5.2	Whether information should be removed, and if so whether any particular security measures are required, should be determined by assessing the risks that the removal may introduce. (Advice about Data Protection and general information security is offered by the Head of Information Security.)
2.5.3	Specific policy relating to taking personal information out of secure FDM locations on mobile computing devices is given in the FDM Technology Security Policy and Acceptable Use Policy.

2.6 Information on screens, desks and printers

Ref No	Control Statement
2.6.1	FDM operate a clear desk policy; confidential and secret information must never be printed.
2.6.2.	Staff responsible for handling Restricted paper documents should take appropriate measures to avoid their unauthorised disclosure. Suitable procedures must be decided and employed based on the nature of the documents and assessment of the risks involved. This may involve locking the documents away when they are unattended. When restricted documents are being printed or copied, devices and documents must be either physically secure or else remain attended.
2.6.3	The possibility that sensitive information displayed on computer screens may be viewed by those without authorisation must be avoided. This must be considered especially when siting devices on which sensitive information is regularly displayed. For further details see the FDM Technology Security Policy and Information Security Management System.

2.7 Storage of information

Ref No	Control Statement
2.7.1	Information of any classification should not be stored locally on workstations or laptops. Instead information should be saved on the Cloud Folder.

	Procedures governing the storage of information must be in place based on the nature of the document.
2.7.2	For a better understanding of where and how data should be stored please see Sections 3 & 4 below.
2.7.3	The security of the FDM Cloud Drive and other data stores including FDM servers must be managed by a member of staff. Security management includes assessing and keeping under review risk levels associated with the data store. Where judged necessary and feasible risk mitigation measures should be implemented. Mitigation measures include storing information elsewhere that is more secure; improving the physical security of the location; backing-up the data to another location; encrypting the data. These measures should be proportionate to the value of the data –measured by the extent to which loss, corruption or disclosure of the data held could cause a significant negative impact on FDM's business and/or reputation.

2.8 Back-ups of information

Ref No	Control Statement
2.8.1	The member of staff with day-to-day responsibility for managing an information asset is by default responsible for ensuring that any necessary back-up procedures are in place, adequate and tested. This may be the information owner or the Manager of a system that stores or processes the information.
2.8.2	Information Asset Owners and Data Processors should: • Make back-ups of information, such as data and software, where the possibility of losing the live, working or master copy of the information is unacceptable; or where not having back-ups is potentially more costly than making them; or where there is any doubt, back-ups should be taken. This should take into account the type and frequency of the back-up, which should be appropriate to the medium. • Ensure that the backed-up data is stored appropriately and in resilient disk storage systems or secure locations. • Clearly establish who is taking responsibility for backup arrangements, especially where data is used across teams. • Ensure that staff or data processors responsible for archiving or making back-ups are aware of any FDM data retention policy relating to the type of data being handled. • Ensuring that all owners of information held in the asset are aware of the back-up arrangements. Where appropriate there should be liaison between the person responsible for managing backups and

	Information Asset Owners with the aim of ensuring that the arrangements are suitable. • Ensure that when potentially inadequate back-up arrangements are identified owners are notified and actions taken • Ensure that back-up media is securely disposed of, when no longer required, in a way that ensures that information will not be disclosed to unauthorised persons. • Periodically test the recoverability of backed-up data to ensure that the recovery procedure does not accidentally destroy more recent files.

2.9 Dissemination and exchange of information

When sharing information, the appropriate method of transfer must be decided, taking into account the nature and volume of the information being exchanged and the impact of inappropriate disclosure. Intended recipients of information must be authorised to receive such information and have sufficient security policies and procedures in place to assure the confidentiality and integrity of the information. Confidential and Secret information may only be transferred across external networks, or copied to other media, once it has been encrypted and password protected (see Section 3 below).

Ref No	Control Statement
2.9.1	The Data Protection Act 2018 requires that personal data is securely handled and imposes special conditions relating to transfer of personal data abroad. For further details see the FDM Technology Security Policy.
2.9.2	Any request for information about FDM, data FDM handles or stores or information which a member of staff would not normally handle as part of their job, should be referred to HQ Requests and no further action should be taken.
2.9.3	Exchanges of significant amounts of personal data or other sensitive information with other organisations should be covered by suitable formal agreements. The security specification of the agreement should reflect any legal compliance requirements and the sensitivity of the information involved. It is the responsibility of the Manager involved to ensure that there is a valid and complete legal agreement. The Manager will need to seek confirmation from Legal Services that this is complete.
2.9.4	The drafting and completing of formal agreements for the exchange or transfer of data or information should be undertaken by Legal Services.

2.9.5	Non-disclosure agreements with other organisations must only be made with due regard for provisions of the Freedom of Information Act. Advice should be obtained from Legal Services.
2.9.6	Where confidential information must be sent via physical mail it should be in a sealed and taped envelope and marked "personal and confidential" and "for addressee only" and must be sent Royal Mail Special Delivery. For particularly sensitive information delivery by hand should be considered.
2.9.7	The limited security of email should always be taken into account when undertaking critical business activities. FDM email is not generally encrypted, although FDM devices and therefore access to FDM email accounts are (a limited number of individuals will have physical security keys which are required for two-step login authentication).
2.9.8	Network transactions or connections between FDM computer systems and systems operated by other organisations should as far as possible utilise technology that assures confidentiality, authentication, nonrepudiation and integrity. (An assessment of the risk should be undertaken when deciding whether to undertake electronic transactions that cannot be fully secured.)
2.9.9	Physical digital media in transit must be protected by security measures appropriate to the risks involved. For further information see the FDM Technology Security Policy
2.9.10	Information that may be associated with FDM or any of FDM's clients must not be distributed, published or otherwise made available unless it is legally compliant, appropriate and approved by management. (Inappropriate content includes material, which is obscene, violent, illegal, damaging to the University or otherwise in breach of FDM policy.) For further information see Acceptable Use Policy and FDM Technology Security Policy
2.9.11	Unsolicited email, faxes and other electronic messages should not be replied to, forwarded or acted upon until and unless the sender's identity and authenticity of the message have been verified. For further policy relating to protecting against malicious code and inappropriate material sent via email and other forms of electronic messaging see the FDM Technology Security Policy
2.9.12	FDM Staff must not disclose, modify, copy or disseminate to others any privileged information which may become available to them. Where they have been given access to information in error, they should advise the owner that the information may be inadequately protected or incorrectly distributed. For further details please see the FDM Staff Handbook and FDM Security Technology Policy

2.10 Information in application systems

Ref No	Control Statement
2.10.1	Where information is being processed by an application system, quality controls should be used to help ensure its accuracy and integrity. Where applicable the following measures should be implemented: • Ensure that a member of staff with responsibility and knowledge for ensuring secure operation of the application is nominated. • Ensure correct levels of access to inputs, outputs and to administrative functions of the application system. • Generate and review regularly transaction and processing reports to help identify integrity problems. • Validate input and output data. For application systems, where the consequences of doing otherwise could be serious, input and output data should be validated to at least ensure it is of the correct type and within a reasonable range.

2.11 Compliance

Ref No	Control Statement
2.11.1	Internal and external audits may carry out reviews relating to compliance with this policy.
2.11.2	Individuals have a personal responsibility to ensure the correct management and protection of information and may be personally liable for any breaches in information security that arise from a failure to take appropriate measure to do so. In the event of doubt please contact your Manager or the Head of Information Security
2.11.3	It is the Information Asset Owner's responsibility to control classified information from conception to destruction including the distribution and any copies of the information that may have been created.
2.11.3	Failure of an individual to comply with this policy may lead to disciplinary procedures and, in some circumstances, legal action. Failure of a Supplier to comply may lead to immediate termination of a contract. Where appropriate, breaches of the law will be reported to the authorities.

3. Handling Electronic Information

Activity	PUBLIC	RESTRICTED	CONFIDENTIAL	SECRET
Creation	n/a	n/a	Visibly marked 'CONFIDENTIAL'	Visibly marked 'SECRET' To be created (and stored) only in a secure environment and copies be limited and recorded
Can Email	Yes	Only to @fdm.uk or other internal domains e.g. @futuredigitalmedia.net (take care to check recipient(s) addresses) or when password protected to external users	Only as encrypted/password protected attachment (take care to check recipient(s) addresses)	Only as encrypted/password protected attachment (take care to check recipient(s) addresses)
Need to password protect file in transit	n/a	Password to meet FDM standard (see FDM Technology Security Policy)	Password to meet FDM standard (see FDM Technology Security Policy)	Password to meet FDM standard (see FDM Technology Security Policy). Consider using PGP encryption (AES-256)
Can access remotely	Using Cloud Drive	Using FDM laptop and password via Cloud Drive	Using FDM laptop, physical security key and password via Cloud Drive	Using FDM laptop, physical security key and password via Cloud Drive
Access controls	May be viewed by anyone, anywhere in the world	Available only to specified authorised FDM staff (e.g. secured behind a login screen, requires authorisation to gain access)	Access is controlled and restricted to a small number of FDM staff (e.g. secured behind a login screen, requires authorisation to gain access)	Access is controlled and restricted to a small number of FDM staff (e.g. secured behind a login screen, requires authorisation to gain access)
Can share via Shared/Individual Cloud Drive	Yes	Only to @fdm.uk or other internal domains e.g. @futuredigitalmedia.net (take care to check recipient(s) addresses)	Only when encrypted/password protected (take care to check recipient(s) addresses)	Only when encrypted/password protected (take care to check recipient(s) addresses)
Can share via Instant Communication	Yes	Only to @fdm.uk or other internal domains e.g. @futuredigitalmedia.net (take care to check recipient(s) addresses) or when password protected to external users	Only when encrypted/password protected (take care to check recipient(s) addresses)	Only when encrypted/password protected (take care to check recipient(s) addresses)
Can keep on FDM laptops or other portable media	Yes	Only on a temporary basis, taking care to avoid loss or theft and if	Only on a temporary basis and if encrypted/password protected, taking care to avoid loss or theft	Only on a temporary basis and if encrypted/password protected, taking care to avoid loss or theft

Can keep on personally owned devices	Yes	No	No	No
Store on FDM servers	Preferably stored in the Cloud Drive	Only in the Cloud Drive with access restricted to only those with a valid right to access the information (either by adding a password to the document, encrypting it or apply permissions to a folder)	Only in the Cloud Drive with access restricted to only those with a valid right to access the information (either by adding a password to the document, encrypting it or apply permissions to a folder)	Only in the Cloud Drive with access restricted to only those with a valid right to access the information (either by adding a password to the document, encrypting it or apply permissions to a folder)

4. Classification Model

Classification	Description	Impact of unauthorised disclosure	Types of data
PUBLIC	Information which is available to the public.	None: • No confidentiality issues • Must still be accurate and protected from unauthorised change	• Website/internet content • Marketing/publicity • Research activity details • Information published in public forums
RESTRICTED	Information which if lost or wrongly disclosed could cause limited negative effects for FDM.	Low: • No sensitive data • No compliance restrictions • Disclosure might be inappropriate but of little significance	• Internal correspondence • Data which would be released as part of Freedom of Information request • Data which is not subject to legal, regulatory, commercial, contractual embargo • Data not yet prepared for formal publication • Policies and procedures
CONFIDENTIAL	Information which if lost or wrongly disclosed could cause distress to our clients or people or damage the interests of FDM.	Medium: • Distress or embarassment to small numbers of individuals • A degree of damage to FDM's reputation or operations • Breach of legislative, regulation or contract with possible financial penalties • Potential to damage future work and projects	• Data subject to legal, regulatory, contractual embargo (unless a higher degree of restriction is specified) • Data with ethical/moral implications e.g. identifiable deceased data subjects
SECRET	Information which if lost or wrongly disclosed could cause very serious damage to the interests of FDM, our clients, people, suppliers or business partners.	High: • Risk to safety or well-being of individuals • Significant distress to individuals • Substantial legal consequence to individuals or FDMy • Substantial financial penalties • Substantial damage to FDM's reputation or operations • Loss of major contracts, work and projects	• Data which poses risk to personal safety • Sensitive personal data (subject to DPA) • Protected characteristics • Data subject to legal, regulatory, contractual embargo for which highest degree of restriction is specified

4. Validity and document management

Ref No	Control Statement
4.1.1	This document is valid as of 26th June 2019.
4.1.2	The owner of this document is the CTO, who must check and, if necessary, update the document at least once a year.
4.1.3	When evaluating the effectiveness and adequacy of this document, the following criteria should be considered: • the number of incidents which occurred, but were not included in risk assessment • the number of errors in misclassification of information by FDM staff • the number of complaints made regarding the classification or handling of data by FDM staff