IG01: NDORMS Information Security Policy

Purpose: This document provides a management framework for managing information security within NDORMS and is supported by policies and guidelines on specific areas.

1 Management Framework

1.1 The NDORMS Board are committed to preserving the confidentiality, integrity and availability of the information assets required for the work of the department.

1.2 The information security requirements are aligned with the organisational goal of enabling medical and scientific research. All members of the NDORMS are required to comply with this policy, with departmental, divisional and university policies and guidelines, and with external regulatory and legislative requirements including the Data Protection Act 1998 or statutory requirements that replace it.

1.3 Revisions to this policy and related documents will be discussed by the NDORMS IT, Informatics and Communications Committee, which reports directly to the NDORMS Board.

1.4 The Head of Department bears final responsibility and will be informed immediately of data breaches.

1.5 The Information Governance Manager (infogov@ndorms.ox.ac.uk) will oversee development and maintenance of departmental information security, reporting to the Head of Department when required, supporting members of the department by investigating reports of risks and data breaches and providing advice to colleagues. The Information Governance Manager will sit on the NDORMS IT, Informatics and Communications Committee.

1.6 The NDORMS Information Security policy will be reviewed when necessary and at least annually to provide continued relevance and improvement.

1.7 Committees reporting to the Board will include a standing item on Information Governance to communicate information up and down through the organisation.

2 Management of Risk

2.1 Information assets will be recorded and monitored including appropriate and timely reporting of identified breaches.

2.2 Appropriate controls will be identified, implemented and monitored to mitigate risks, in proportion to their likelihood and potential impact.

2.3 Individual projects may adopt more stringent controls to provide for specific risks and external requirements but must not fall below the departmental baseline standards.

3 Management of Awareness

3.1 All members of NDORMS will be informed of major revisions of this policy.

3.2 All members of NDORMS must undertake locally mandated training on information security and data protection at least annually. Training will be recorded and monitored by the Information Governance Manager. This will include a declaration of current knowledge of relevant policies and guidelines.

3.3 Recruitment processes will include suitable mention of information security to ensure those joining NDORMS are ready to work in an environment that handles significant levels of sensitive information. New starters will meet with the Information Governance Manager as part of their induction period for an information security briefing.

Document History

Version	Authorship	Key Changes	Date	Review By
3.0	Wulf Forrester-Barker NDORMS Information Governance Manager	Minor changes to wording	14 September 2017	September 2018
2.0	Wulf Forrester-Barker NDORMS Information Governance Manager	Rewritten as management policy, supported by IG02	2 February 2017	April 2018
1.0	Wulf Forrester-Barker NDORMS NIHR BRU IT Manager	First published version	14 January 2015	May 2015

Authorisation by Head of Department

Signed:.....

Professor Andrew Carr

Date: .....

Signed by Professor Andrew Carr following NDORMS Board Meeting, 10 October 2017. Hardcopy held on file by Head of Administration.