The Tavistock and Portman NHS
NHS Foundation Trust

Secure Storage of Doctoral Students Electronic Research Data Procedure

Version:	2
Bodies consulted:	Academic Governance and Quality Assurance Committee
Approved by:	EMT
Date Approved:	12.1.16
Lead Manager:	Head of Technology Enhanced Learning
Lead Director:	Director of Education & Training
Date issued:	Jan 16
Review date:	Dec 20

Contents

Secure Storage of Doctoral Students Electronic Research Data Procedure

1 Introduction

This procedure sets out how students' research data that includes personal identifiable information shall be stored securely.

2 Purpose

The purpose of this procedure is to describe the manner in which the Trust will meet its legal obligations under the Data Protection Act by:

- detailing a practical procedure for secure storage, access and security of the Trust's doctoral students' electronic research data.
- describing the respective responsibilities in the secure storage, access and security of students' electronic research data.

3 Scope

This procedure covers the storage, access and security of doctoral students' electronic data that is collected as part of the student's supervised research at the Trust. This procedure applies to all Doctoral Students undertaking supervised research at the Trust and the Trust's staff and research supervisors.

4 Definitions

Moodle – an externally-hosted virtual learning environment containing resources for student and staff relevant to training and education in the Trust.

My Private Files – a facility available to each Moodle user where private files can be uploaded and stored. The files are accessible only to the individual user and the Moodle Administrators in the TEL Unit.

Shibboleth – an authentication system for registered students at the Trust that allows access to Moodle and Library resource.

Electronic research data – a piece of research for which an individual is registered with a recognised awarding body and upon successful completion leads to a designated award.

5 Procedures

5.1 The procedure for secure storage of Doctoral Students Electronic Research Data is as follows:

5.1.1 The Doctoral Research Student submits their research application to Postgraduate Research Degrees Sub-Committee for recommendation to Research Degrees Sub-Committee. No application can be accepted without an IG training certificate (see section 7).

5.1.2 The Doctoral student is issued with a Postgraduate Research Handbook which includes the postgraduate code of practice for data protection.

5.1.3 The Doctoral Student is issued with guidance for using the My Private Files facility within Moodle, a user-restricted area within the platform for storing electronic research data that is managed by the Trust's TEL Unit, with access permission for the student and TEL's Moodle Administrators only.

5.1.4 The respective Course Administrator will instruct the TEL Unit to delete the student's research folder one year after the student has been awarded, or one year after studies have been terminated for any other reason.

6 Duties and responsibilities

6.1 It will be the responsibility of:

6.1.1 the Director of Education and Training to ensure that this procedure is followed correctly.

6.1.2 The Trust's TEL Unit to ensure that

- adequate space is available for the student to store their electronic research data on the Moodle platform
- students are issued with instructions and training on using the My Private Files facility on the Moodle platform

6.1.3 The Postgraduate Research Degrees Sub-Committee secretary to ensure that:

- the student has been issued with instructions on using the My Private Files facility by making the request to the TEL Unit
- the student is issued with a Postgraduate Research Handbook, which includes the postgraduate code of practice for data protection
- TEL are informed when a Moodle user account including data stored under the My Private Files facility needs to be deleted

- the IT Department is instructed to terminate the Doctoral Student's IT user account
- the Registry is instructed to terminate the Doctoral Student's Shibboleth user account to prevent further access to Moodle
- the TEL Unit is instructed to delete the Doctoral Student's folder on the Moodle platform

6.1.4 the Doctoral Student's research supervisor to report any issues of non-compliance to the relevant course team lead, who in turn should report to the respective Portfolio Manager and the Director of Education and Training/Dean of Postgraduate Studies.

6.1.5 The Student to keep all person-identifiable data relating to their doctoral research in the secure folder and to keep data secure once collected but before it is uploaded. Once uploaded, copies of data must not be stored on student devices (unless the student is a member of staff with a Trust device).

7 Training Requirements

Doctoral students and research supervisors will need to complete the Trust's mandatory Information Governance Training.

Doctoral students will be issued with guidance and where necessary training on using the My Private Files facility within Moodle.

8 Process for monitoring compliance with this Procedure

8.1 The following criteria will be used by the Postgraduate Research Degrees Sub-Committee secretary for auditing this procedure:

8.1.1 Was the student issued with guidance on using the My Private Files facility?

8.1.2 Did the student access the My Private Files facility?

8.1.3 Is there electronic data stored in the folder?

8.1.4 Was the student's IT user access and Shibboleth account terminated on completion of studies?

8.1.5 Were the student's research files within the My Private Files facility in Moodle deleted one year after the student had finished their Doctoral studies?

8.2 In addition to the audit above the Doctoral Student's research supervisor will also report to the Associate Dean (Academic Governance and Quality Assurance) and the Head of the Academic Governance and Quality Assurance Unit if the student has not complied with this procedure and

stored their electronic research data in the My Private Files facility. The issue of non-compliance will be dealt with under the Trust's Student Conduct policy.

8.3 The Director of Education and Training will report IG training compliance (as set by the Senior Information Risk Owner) to the Governance Manager.

8.4 The Postgraduate Research Degrees Sub-Committee secretary will audit compliance and present their findings in an annual report to the Academic Governance and Quality Assurance Committee which will in turn report to the Dean of Postgraduate Studies.

9 References and Associated documents

Student Conduct Policy

Information Governance Policy

Data Protection Procedure

Postgraduate code of practice for data protection

Moodle Site Policy

10 Equality Impact assessment

1. Does this Procedure, function or service development affect patients, staff and/or the public?

YES

2. Is there reason to believe that the Procedure, function or service development could have an adverse impact on a particular group or groups?

NO

*3. If you answered **YES in section 2,** how have you reached that conclusion? (Please refer to the information you collected e.g., relevant research and reports, local monitoring data, results of consultations exercises, demographic data, professional knowledge and experience)*

4. Based on the initial screening process, now rate the level of impact on equality groups of the Procedure, function or service development:

Negative / Adverse impact:

Low…….does not have negative impact
(i.e. minimal risk of having, or does not have negative impact on equality)

Positive impact:

Low……not likely to contribute to promoting…
(i.e. not likely to promote, or does not promote, equality of opportunity)

Date completed: 10 August 2015

Name: Simon Kear

Job Title: Head of Technology Enhanced Learning

Manager: Brian Rock