

Undertaking to the Joint Committee on Legal Deposit

on the security of deposited non-print publications

Date:	21 st June 2013
Version:	1.0
Author(s):	Richard Gibby

1. Introduction

- 1.1. A Memorandum of Understanding, dated 1st January 2012, between the six Deposit Libraries commits them to implementing the Legal Deposit Libraries (Non-Print Works) Regulations 2013 on a shared basis. For this purpose a shared technical infrastructure, including a secure storage and preservation system for digital content assets designed and developed by the British Library (the 'Digital Library System'), is being put into effect. Copies of the digital content assets are stored in four connected nodes hosted by the British Library, National Library of Scotland and National Library of Wales. The British Library will also provide secure network access to the Digital Library System for users in the Bodleian Libraries, Cambridge University Library and the Library of Trinity College Dublin, and the National Library of Scotland will provide secure network access for users in the Library of the Faculty of Advocates.
- 1.2. The Deposit Libraries recognise the importance of managing deposited material securely, and the potential risks to a publisher's or other rights holder's interests if deposited material is used in ways that are not permitted by the Regulations. In this undertaking, the Deposit Libraries make a number of commitments to the Joint Committee on Legal Deposit, as a body containing representatives of the publishing industry and other stakeholder interests, for the secure management of deposited material.

2. Parties to this Undertaking

- 2.1. The parties to this Undertaking are:
 - The British Library, 96 Euston Road, London NW1 2DB.
 - The National Library of Scotland, Edinburgh, Scotland, EH1 1EW.
 - The Board of the National Library of Wales, Aberystwyth, Ceredigion SY23 3BU.
 - The Bodleian Libraries, Broad Street, Oxford OX1 3BG.
 - The Cambridge University Library, West Road, Cambridge CB3 9DR.
 - The Library of Trinity College, College Street, Dublin 2, Ireland.

Each a 'Library' and collectively 'the Deposit Libraries'.
- 2.2. This undertaking is authorised by the principal executive officers of the Deposit Libraries, and is effective from the commencement of Regulations.
- 2.3. Amendments to this undertaking must be authorised by the principal executive officers of the Deposit Libraries after consulting the Joint Committee on Legal Deposit.

3. Definitions

the Act	The Legal Deposit Libraries Act 2003
Deposited material	Offline or online works that are delivered to, harvested by or copied from the internet by a Party pursuant to the Regulations
Digital Library System	An electronic system developed by the British Library and hosted by the National Libraries in London, Boston Spa, Aberystwyth and Edinburgh, for storing digital content assets including (but not limited to) deposited material
the National Libraries	Collectively the British Library, the National Library of Scotland and the National Library of Wales
the Regulations	The Legal Deposit Libraries (Non-Print Works) Regulations 2013

4. Information Security: Governance

- 4.1. Each Library will establish, implement and maintain an information security policy and appropriate information security procedures within the Library's own organisation.
- 4.2. Each Library or its parent institution will charge a committee with overall responsibility for coordinating information governance, including information security, with a remit to direct, monitor and control the implementation of information security within the Library's own organisation.
- 4.3. Each Library or its parent institution will assign overall responsibility for information security within the Library's own organisation to a senior member of staff.
- 4.4. Each Library or its parent institution will appoint and charge a technical security officer with responsibility for the security of information in electronic form within the Library's own organisation.
- 4.5. This undertaking, and each of the Deposit Libraries' performance against the commitments it contains, will be reviewed periodically by a joint committee of senior managers and technical security officers from each Library.

5. Information Security: processing deposited material

- 5.1. The British Library will manage any passwords or access credentials that are supplied by a publisher pursuant to the Regulations in a secure repository, and will ensure that they are only used by authorised personnel for the purposes permitted by the Regulations.
- 5.2. The National Libraries harvesting or taking delivery of deposited material will store it within secure systems, to which only authorised personnel may have access for the purpose of processing it for storage and preservation.

- 5.3. The National Libraries processing deposited material will implement policies and systems to prevent such authorised personnel from making or disseminating unauthorised copies of deposited material.
- 5.4. Any third party employed by a Library to acquire or process deposited material, or to carry out other permitted activities with deposited material, will be required to implement appropriate information security measures and to comply with audits authorised by the Library. Any third party employed by a publisher will not be subject to this undertaking.

6. Information Security: storing deposited material

- 6.1. The Deposit Libraries will store all deposited material, after processing, in the Digital Library System. Any transfer of deposited material between the Libraries, for processing or for ingest into the Digital Library System, will be made by secure network or by secure delivery on physical media.
- 6.2. Once the deposited material has been ingested into the Digital Library System, each relevant Library will delete any copies that remain in processing systems outside of the Digital Library System.
- 6.3. The British Library will maintain the Digital Library System on a Virtual Private Network run over private circuits, protected by firewalls and virus checking systems, with no wider public internet access, and encrypting any communication between the firewalls for transferring data between the nodes in London, Boston Spa, Aberystwyth and Edinburgh.
- 6.4. The British Library will ensure that only authorised personnel with an appropriate business need are granted administrative access rights to the Digital Library System, subject to security checks before being granted such rights.
- 6.5. The National Libraries will employ physical entry controls to ensure that only authorised personnel with an appropriate business need are permitted access to the secure areas hosting the Digital Library System in London, Boston Spa, Aberystwyth and Edinburgh.
- 6.6. The National Libraries will employ additional security controls to prevent unauthorised access to the Virtual Private Network run over private circuits.
- 6.7. The National Libraries will implement policies to prevent such authorised personnel from making or disseminating unauthorised copies of deposited material stored in the Digital Library System.

7. Information Security: using deposited material

- 7.1. The Deposit Libraries will implement systems and procedures to ensure that deposited material may only be used on library premises controlled by a deposit library.
- 7.2. The Deposit Libraries will implement systems and procedures to limit readers' concurrent access for the same relevant piece of deposited material to one device at a time in each Library.
- 7.3. The Deposit Libraries will implement systems and procedures to ensure that deposited material is not made accessible for at least seven days after it has been harvested or delivered, and subject to any embargo (for withholding access) that has been agreed.
- 7.4. The Deposit Libraries will implement systems and procedures to ensure that no digital copies may be made by or for users, unless the copyright holder or database right holder has given permission to do so.
- 7.5. The Deposit Libraries will implement systems and procedures to ensure that fair dealing print copies of deposited material are only supplied to users, or made by users, in accordance with the terms and conditions set out in Regulations.

8. Information Security: incidents and complaints

- 8.1. The Deposit Libraries will publish a point of contact and implement an appropriate escalation process for any queries, complaints or incidents relating to the security of deposited material and this joint undertaking.
- 8.2. The Deposit Libraries will implement a formal process to manage and report any security incidents relating to deposited material and the commitments in this joint undertaking.

9. Audits and Assurance

- 9.1. The British Library will commission independent penetration tests of the Digital Library System on a regular basis.
- 9.2. The National Libraries will implement regular internal and external IT security audits of the shared technical infrastructure, including installations of the Digital Library System, and of processing operations for deposited material.
- 9.3. The Deposit Libraries will commission regular independent audits of their performance against the commitments in this joint undertaking.

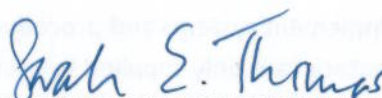
9.4. The Deposit Libraries will also comply with any additional publisher-sponsored audits that may be required by the Joint Committee on Legal Deposit.

9.5. The results of all such internal and independent external audits, together with action plans to remedy any issues of concern that might be identified, will be confidentially reported to all members of the Joint Committee on Legal Deposit.

Signed for and on behalf
of the British Library:



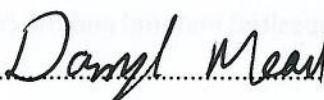
Signed for and on behalf
of the Bodleian Libraries:



Signed for and on behalf
of Cambridge University Library:



Signed for and on behalf
of the National Library of Scotland:



Signed for and on behalf
of the National Library of Wales:



Signed for and on behalf
of the Library of Trinity College Dublin:

