

## Data Protection Checklist for Learning Analytics

### 1. Introduction

The Data Protection Commissioner's Office has posted eight rules which highlight the responsibilities of data controllers with regard to data management (<https://www.dataprotection.ie/docs/Data-Protection-Rules/y/21.htm>). These rules are listed below along with a checklist derived from the Data Protection Checklist at <https://www.dataprotection.ie/docs/Self-Assessment-Data-Protection-Checklist/y/22.htm>. The purpose of this guide is to enable institutions and individuals to design Learning Analytics systems, policies and practices which are compliant with the Data Protection Acts 1988 & 2003. Institutions should be able to answer 'Yes' to all of the questions below to be compliant.

Please note that the EU's General Data Protection Regulation (GDPR) will come into application from 25 May 2018. The full and precise implications of this act are, at the time of writing, under exploration. Please see the relevant section below which outlines the implications of this regulation as they are currently known.

Please note that this document is for guidance purposes only. Undertaking these checks is not a legal substitute for a full diligence exercise.

### 2. Responsibilities of Data Controllers (eg Institutions)

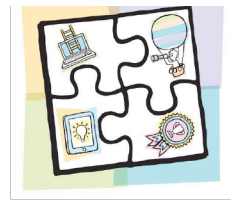
Data Controllers must:

- Obtain and process student data fairly
- Keep it only for one or more specified and lawful purposes
- Process it only in ways compatible with the purposes for which it was initially given
- Keep it safe and secure
- Keep it accurate and up-to-date
- Ensure that it is adequate, relevant and not excessive
- Retain it no longer than is necessary for the specified purpose or purposes
- Give a copy of his/her personal data to any student or graduate, on request.

### 3. Data Protection Checklist

#### Rule 1 – Obtain and process data fairly:

- At the time when information is collected about students, are they made aware of the uses for that information?
- Are students made aware of any disclosures of their data to third parties?
- Learning Analytics involves the use of personal data in a way which may not be obvious to students. Have students been asked for their consent to use it in this



**ORLA: Online Resource for Learning Analytics** | <http://tinyurl.com/NFORLA>

way? (Please see the ORLA discussion document on informed consent for further information)

- Are the institution's data-collection practices open, transparent and up-front?

### **Rule 2 – Keep only for specified purpose**

- Has the institution explicitly defined for what purposes Learning Analytics will be used?
- Have students been informed of these purposes?
- Has the institution assigned responsibility for maintaining a list of all data sets and the purpose associated with each?

### **Rule 3 – Data use and disclosure**

- Are there defined rules about the use and disclosure of student information in relation to Learning Analytics?
- Are all staff aware of these rules?
- Are students aware of the uses and disclosures of their personal data? Would they be surprised if they learned about them?

### **Rule 4 – Security**

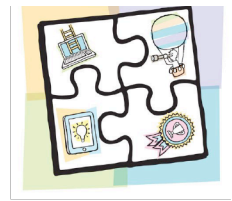
- Is there a list of security provisions in place for each data set?
- Is someone responsible for the development and review of these provisions?
- Are these provisions appropriate to the sensitivity of the personal data?
- Are computers and databases password-protected, and encrypted if appropriate?
- Are computers, servers, and files securely locked away from unauthorised people?

### **Rule 5 – Data is adequate, relevant and not excessive**

- Does this institution collect all the information needed to serve this purpose effectively, and to deal with students in a fair and comprehensive manner?
- Has the institution checked to make sure that all the information collected is relevant, and not excessive, for the specified purpose(s)?
- If a student asked the institution to justify every piece of information held about him or her, could the institution do so?
- Does a policy exist in this regard?

### **Rule 6 – Data is accurate and up-to-date**

- Does the institution check data for accuracy? (See ORLA document on data



**ORLA: Online Resource for Learning Analytics** | <http://tinyurl.com/NFORLA>

validation for further information)

- Is the institution informed of how much of the personal data held is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?
- Does the institution take steps to ensure its databases are kept up-to-date?

#### **Rule 7 – Data retention**

- Is there a clear statement on how long data are to be retained?
- Are there any legal requirements to retain data for a certain period?
- Does the institution have a plan for regularly purging databases of data which is longer needed?
- Is there a policy on deleting personal data as soon as the purpose for which it was obtained has been completed?

#### **Rule 8 – Right of access to personal data**

- Is a named individual responsible for handling access requests?
  - Are there clear procedures in place for dealing with such requests?
  - Do these procedures guarantee compliance with the Act's requirements?
-