Learning Analytics Service:
Data Protection Impact Assessment (DPIA)

Version: 0.04
Date: 7 July 2018

After completing a review of the Learning Analytics Service in July 2018, our conclusion is that it does not present a high risk to the rights and freedoms of individuals.

The following describes how we reached our conclusion.

1. Background
Jisc’s Learning Analytics Service\(^1\) will be launched on 1 August 2018. Rather than wait for UK guidance on DPIAs to be issued, Jisc used guidance currently available from the Article 29 Working Party\(^2\) to develop this DPIA. Jisc identified a DPIA was required for the Learning Analytics Service because it involved:

- Large-scale processing of data
- Matching and combining data sets
- The use of innovative new technologies (which are likely to require new processes and organisational structures to be set up)
- Inclusion of vulnerable data subjects (e.g., students at risk of failing to complete their course of study).

2. Purpose
The purpose of this DPIA is to describe the data protection risks Jisc identified in the Learning Analytics Service and the mitigations in place to ensure they are managed effectively.

3. Learning Analytics
Learning analytics refers to the measurement, collection, analysis and reporting of data about student retention, progression and achievement. Students using digital resources and systems generate data that can be analysed to reveal patterns predicting success, difficulty or failure, which enable teachers - and students - to make timely interventions. These metrics can also support a more accurate, data-informed approach to curriculum design. There may be future interest with analytics based around staff.

Jisc’s Learning Analytics Service consists of a learning data hub, into which institutions and students can load data relevant to their learning activities. Institutions and students can then use a variety of

---

\(^1\) https://www.jisc.ac.uk/learning-analytics

\(^2\) http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
analytics tools, provided by Jisc and third-party commercial suppliers, to identify opportunities to improve the learning process.

4. Description of Processing Operations
Jisc and third parties processes personal data about students and their learning activities. Some information about staff is also processed to help them to support students.

Some tools in the Learning Analytics Service use machine learning and algorithms. The service also involves processing historic and live data.

Some data from the Learning Data Hub will be transferred to the Jisc Learning Analytics Lab Service. This will be subject to its own privacy assessment and notice.

4.1 Legal Basis for Processing
In the Learning Analytics Service each Institution is a Data Controller and Jisc is their Data Processor. Where Institutions grant their students access to learning analytics mobile apps or other applications through which students can upload their own data to the service, Jisc is again a Data Processor for those Institutions.

Each Institution is responsible for determining the appropriate legal basis for its use of the Learning Analytics Service. Jisc suggests that where data is collected and processed by an Institution for its internal purposes, and also uploaded to the Learning Data Hub, the most appropriate basis is likely to be the Institution’s legitimate interest in providing the best educational experience to its students. Where students upload their own data, for example through learning analytics mobile apps, the most likely basis is the student’s free, informed consent.

Each legal basis establishes its own responsibilities and duties on the Data Controller. Jisc provides documents and tools, including this DPIA, that Institutions can use in fulfilling those responsibilities and duties. Jisc will ensure that its systems provide appropriate security for the personal data it processes. For that security to be effective, Data Controllers must also provide appropriate organisational and technical measures, for example by appropriately protecting the credentials that give their staff access to the Learning Analytics Service.

---

3 https://analytics.jiscinvolve.org/wp/2017/02/16/consent-for-learning-analytics-some-practical-guidance-for-institutions/
4 https://www.jisc.ac.uk/gdpr
4.2 Data Processing and Storage

Jisc Learning Analytics open architecture: core

- **Learning Data Hub (LDH):** The central repository for data about students and staff. Based on the open source Learning Locker product from HT2Labs. The LDH stores and passes standardised data between other tools in the service. The LDH is hosted in Amazon Web Services (AWS) in the EEA.

A suite of data extraction, transformation and validation tools are available from Jisc to help institutions to get historic data out of their student records systems and virtual learning environments and into the LDH.

- **Data Explorer:** A data visualisation tool for staff that enables them to view student data held in the LDH. Hosted in AWS in the EEA. Data Explorer provides:
  - Technical tools to view data
  - Overview tools to view visualisations of data across an institution
  - Tools for tutors

- **Traffic Light Calculator:** Provides basic rule-based calculations of student online engagement, attendance and achievement. Hosted in AWS in the EEA.

- **Study Goal:** A mobile app that enables students to see their learning activity, set targets and record their own activity. Students can also share their activity and goals with their peers. Study Goal is available for iOS and Android. Hosted in AWS in the EEA.

- **Predictor:** Offers predictive analytics to support student retention, attainment and success. Predictions are based on data held in the LDH. Hosted in AWS in the EEA.

Jisc will only retain data for as long as it is relevant and necessary for delivering its Learning Analytics Service.

4.3 Types of Personal Data Used

Personal data is obtained from two main sources:

- The Student Records System

---

5 https://learninglocker.net/
• Other systems as instructed by the Institution, including virtual learning environments, library systems, attendance systems and assessment systems. These systems provide data on student learning activity.

Jisc has defined the data that Institutions may need to supply from their student records systems - the Jisc Learning Analytics Unified Data Definitions (UDD)⁶. The UDD describes data about staff and the courses they teach as well as students, their courses and results. The UDD limits the set of data that an Institution needs to send to the LDH. Some fields in the UDD are mandatory, because they are required in order for products to operate, while others are optional.

The Institution, as Data Controller, may instruct Jisc, on a case-by-case basis, to process other types of student activity data.

The following summarises the main types of personal data about students that an Institution sends to the LDH:

• Demographic information about the data subject including, but not limited to, student id, data of birth, username, first name, last name, institutional email address, address, accommodation type, socio-economic group, parents’ education background, gender;
• Information about the course a data subject is taking including, but not limited to, course/module name, start and end date, course and module marks and outcome of the course;
• Information about the data subject’s achievements including, but not limited to, assignment identifiers, initial and agreed marks; and
• Information about the data subject’s learning activity including, but not limited to, the type of activity, system, time, the module or course it relates to and the result of the activity.

The following summarises the main types of personal data about staff that an Institution sends to the LDH:

• Information about the data subject including, but not limited to, first name, surname and Institution email address

The Institution owns all its data, including personal data, that is used and shared in the Learning Analytics Service.

Institutions may agree to share aggregated or anonymised data sets as part of benchmarking exercises, however these do not involve disclosing personal data.

4.4 Data Sharing
There are three scenarios where personal data is shared in the Jisc Learning Analytics Service:

• Jisc may, from time-to-time, appoint infrastructure contractors (sub-processors), such as AWS, to deliver its Learning Analytics Service.

In the case of AWS, the controls and permissions required to limit data sharing are specified in Jisc’s AWS enterprise level agreement.

⁶ https://github.com/jiscdev/analytics-udd
Jisc may also, from time-to-time, appoint analytics service providers (sub-processors) to deliver its Learning Analytics Service. At the time of publishing (Aug 2018) the following sub-processors were contracted to deliver services to Jisc and Jisc's customers.

HT2 Ltd
Amazon Web Services (AWS)
Kerr Gardiner Consulting Ltd
Sclater Digital Ltd
Blackboard
Cetis LLP

Updates to the list of Jisc sub-processors will be available from the Jisc web site.

Jisc’s contracts with analytics sub-processors require them to implement and maintain appropriate technical and organisational security measures to safeguard any personal data that is shared with them. The contracts also prohibit sub-processors from using an Institution's data for purposes other than delivering their learning analytics services, and from sharing data with other 3rd parties.

- Institutions can integrate add-on analytics services from other providers.

Institutions that use add-on analytics services from other providers are strongly advised to incorporate the wording of the Data Protection Mandatory Terms Jisc has agreed with suppliers under the Learning Analytics Purchasing Service. In this way Institutions can ensure any contracts they place with add-on providers are no less onerous in terms of security requirements than the agreements Jisc has in place with its sub-processors.

- There are no plans for data in the Jisc Learning Analytics Service to be processed, stored or replicated outside the EEA.

- Institutions with add-on services supplied by an analytics provider that is not part of the core Jisc service must ensure that, if international transfers of data are required, use of a compliant transfer mechanism is specified in their contact with that provider.

5. Necessity, Proportionality and Individual Rights

5.1 Necessity
Data in the Learning Analytics Service is processed to generate insights and predictions on student retention, attainment and success. Each tool has its own set of input fields that are necessary for it to function. It is the responsibility of Institutions, as Data Controllers, to upload the appropriate data, including personal data, necessary for the tools they wish to use.

5.2 Proportionality
Proportionality requires that the benefits likely to result from processing justify the risks to individuals that may arise. Jisc will continually test and refine the algorithms it uses to ensure that

---

7 https://www.jisc.ac.uk/learning-analytics
8 https://docs.analytics.alpha.jisc.ac.uk/docs/learning-analytics/Learning-Analytics-Purchasing-Service
they offer a significant benefit to students and staff and represent a low risk of discrimination or other harms. Jisc’s guidance to Institutions purchasing add-on learning analytics services is that contracts with these service providers should assign responsibility for ongoing checks of proportionality.

By exercising control over what data is uploaded to the Jisc Learning Data Hub, Institutions can ensure that any processing of that data is proportionate.

5.3 Individual Rights
GDPR grants individuals’ rights over the processing of their personal data. In some cases, these rights may vary depending on the legal basis used for the processing.

The rights of adequacy and retention ensure that data is not processed more widely, or for longer, than the purpose of processing requires. The Institution, as Data Controller, is responsible for ensuring that data uploaded to the Learning Data Hub is adequate for the learning analytics tools it wishes to use. It is also the responsibility of the Data Controller to ensure that data is deleted from the Jisc Learning Analytics Service and any add-on analytics services when no longer needed. The institution can delete data from the Learning Data Hub itself, or it can instruct Jisc to do this as laid out in the Learning Analytics Service Agreement it has signed with Jisc. Where the Institution uses an add-on analytics service it should ensure that its contract with the provider covers the deletion of data when it is no longer needed.

The Institution’s ability to download, edit or delete individual records held in the Learning Data Hub enables it to fulfil requests for access, rectification and erasure without further assistance from Jisc. These tools also support the deletion of records following either withdrawal of consent or a successful objection, as required by the legal bases of consent and legitimate interests, respectively.

The Data Controller is responsible for providing information to its students and staff about how their personal data is processed in the Jisc Learning Analytics Service.

Institutions can instruct Jisc to delete or return their data at any time by submitting a service request to help@jisc.ac.uk.

6. Risks to the Rights and Freedoms of Individuals
The following high impact risks were identified:

- Unauthorised access to detailed personal information about a student’s daily activities. For example, unauthorised access to student activity data provided from the institution’s virtual learning environment could enable the elucidation of a student’s location at a given time and so risk their personal safety.
- Unauthorised access to demographic information about students or staff, as this could result in guidance being directed to the wrong student, or a student failing to receive necessary guidance.
- Unauthorised modification of data, as this could result in a student being given inappropriate guidance.

The following medium impact risks were identified:

- Destruction of personal data. Personal data stored in the Learning Data Hub is a copy of data provided from other source systems controlled by the institution. If data is destroyed in the Learning Data Hub it can be re-loaded from these source systems. Students will be affected in this scenario, but the impact on them is lessened because their data can be restored from source systems.
• A lengthy system outage. In the event of a lengthy system outage, staff and students can put in place alternative arrangements outside of the system to ensure contact and engagement are maintained. Students will be affected in this scenario, but the option to use alternative arrangements means the impact on them is lessened.

7. Risk Mitigation
To reduce the likelihood of any event giving rise to the risks identified above, Jisc uses several mitigation measures. These mitigations protect against internal, external or environmental threats. Some mitigations are effective against multiple threats, or against risks that arise out of information sharing.

As Jisc is the Data Processor there is a focus on physical and technical risks and mitigations. As Data Controllers, Institutions will need to look at these areas as well as organisational risks and mitigations in their day-to-day operations.

7.1 Mitigation of Internal Threats
Jisc has controls in place to reduce the risks arising out of internal threats (ie staff acting carelessly or maliciously). All new staff at Jisc, including casual staff, have a confidentiality clause in their contract of employment and are made aware of their responsibilities toward personal data as part of their induction process. All staff at Jisc are required to take an annual online data protection awareness course. All staff at Jisc are subject to a "Secure Working Practices Policy" that defines their responsibilities for information security and personal data handling, as well as providing advice and guidance on common security threats. All Jisc staff involved in the Learning Analytics Service are provided with additional information security training.

Use of activity logs, regular system monitoring and system audits ensure that Jisc can enforce adherence to its information security procedures and corporate policies.

Access control to application servers is in place to limit access to only Jisc staff who require it.

Any Jisc devices that need access to data will be encrypted.

7.2 Mitigation of External Threats
To reduce risks from unauthorised external access a range of preventive, detective and corrective controls are in place.

Any temporary copies of data are encrypted at rest and securely deleted when no longer required.

User logins are via the UK Access Federation and are logged via the Institution's IdP.

User access and activity monitoring controls (both audit trails and logs) are in place:
• Study Goal user access logging is via xAPI to the Learning Data Hub.
• Data Explorer maintains its own user logging service.

Encryption:
• Data at rest in the Learning Data Hub is encrypted at the database level.
• Historic data is encrypted at a field level.
• Data in transit is encrypted using HTTPS or SFTP secure communication protocols.

Vulnerability and patch management is regularly carried out in accordance with our vulnerability management processes. Occasionally, critical security patches may require us to take the Learning Analytics Service offline at short notice. Where possible, we will work with Institutions to minimize any disruption. Our service infrastructure is regularly scanned for vulnerabilities by automated
systems and is subject to periodic penetration testing of the network environment, operating system, and applications. All issues discovered are prioritized and accordingly addressed. Jisc encourages third parties to work with us to resolve any security vulnerabilities discovered.

7.3 Mitigation of Environmental Threats
All data in Jisc's Learning Analytics Service is held in Amazon Web Services (AWS) data centres in the EEA. The ISO 27001 certification of these data centres ensures that physical security and environmental threats are managed effectively.

Full backups of data in the Learning Data Hub are held on a rolling 5-week schedule. Jisc can rollback to any day in the previous 5 weeks. Specific 'Point In Time' restoration is available for any period within the past 48 hours. As each backup overwrites the previous one, data will not be removed from all backups until the 5-week cycle has been completed.

Staff at Jisc are subject to Jisc's "Secure Working Practices Policy" which covers the physical security of information when working remotely at other locations.

7.4 Mitigation of Information Sharing Risks
There are currently no plans to share an Institution's data with any other Institution.

Contracts in place with Jisc sub-processors control how, and under what circumstances, data can be shared with a 3rd party.

Where a benchmarking exercise is agreed, Jisc will ensure that aggregates are always calculated across multiple institutions and use a sufficiently large number of students to avoid the risk of re-identification.

Further detail about all the controls in place to safeguard personal data in the Learning Analytics Service are available.9

9. Information security incidents
Jisc has an established process for handling information security incidents, including data breaches. Should an incident occur, it will be handled according to this process and in line with current data protection legislation. Jisc will inform any affected institutions and sub-processors as soon as possible after becoming aware of an actual or near-miss personal data breach and will assist them to assesses and manage the situation.

10. Conclusions
The table below summarises the full risk assessment for the Jisc Learning Analytics Service:

<table>
<thead>
<tr>
<th>Risk</th>
<th>Source</th>
<th>Principal Mitigations</th>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorised access to student personal data</td>
<td>Internal</td>
<td>Mitigation of Internal Threats</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>External</td>
<td>Mitigation of External Threats</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mitigation of Environmental Threats</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

9 https://docs.analytics.alpha.jisc.ac.uk/docs/learning-analytics/Security-FAQs
<table>
<thead>
<tr>
<th>Risk</th>
<th>Source</th>
<th>Principal Mitigations</th>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access to demographic data</td>
<td>Internal</td>
<td>Mitigation of Information Sharing Risks</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>External</td>
<td>Mitigation of Internal Threats</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mitigation of Environmental Threats</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mitigation of Information Sharing Risks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorized modification of personal data</td>
<td>Internal</td>
<td>Mitigation of Internal Threats</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>External</td>
<td>Mitigation of External Threats</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mitigation of Environmental Threats</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mitigation of Information Sharing Risks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorized destruction of personal data</td>
<td>Internal</td>
<td>Mitigation of Internal Threats</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>External</td>
<td>Mitigation of External Threats</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mitigation of Environmental Threats</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mitigation of Information Sharing Risks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A lengthy system outage.</td>
<td>Internal</td>
<td>Mitigation of Internal Threats</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>External</td>
<td>Mitigation of External Threats</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Risk</td>
<td>Source</td>
<td>Principal Mitigations</td>
<td>Likelihood</td>
<td>Impact</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>-----------------------</td>
<td>------------</td>
<td>--------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mitigation of Environmental Threats</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Given that effective mitigations are in place to manage risk in the Learning Analytics Service, our conclusion is that the service does not present a high risk to the rights and freedoms of individual users.

11. Recommendations
An external audit to assess the readiness of the Jisc Learning Analytics Service for transition to service was undertaken earlier in 2018. It identified a number of recommendations that are currently being implemented. Progress is being monitored via Jisc’s Audit Committee.

12. Next Steps
1. This DPIA will be published on the Jisc website.
2. The scope of Jisc’s ISO 27001 certification will be extended to include the Learning Analytics Service.
3. Jisc will review and adapt this DPIA to meet the requirements of UK guidance when it is available.
4. Jisc will consider developments in the use of special category data for Learning Analytics and how to address them in later versions of this DPIA.
5. Future audits of the Learning Analytics Service will be undertaken and monitored via Jisc’s Audit Committee.

13. DPIA Authorisation Signatures

Approved (Data Protection Officer) __________________________ Date __22/8/18____

Approved (Service Manager) __________________________ Date __22/8/18____

Approved (SIRO) __________________________ Date __3/9/18____