DRAFT Wellbeing Analytics Code of Practice

Draft 0-31 26th July 2019

Comments welcome to Andrew.Cormack@jisc.ac.uk

Introduction

Whereas Learning Analytics uses data to inform decisions – from individual to curriculum level – concerning students' learning, data may also be used to inform decisions about their mental health and wellbeing. Possible applications cover a very wide range: from screen-break reminders to alerts when a student appears to be at risk of suicide. Clearly this can involve both significant benefits and high risks.

Voluntary wellbeing apps – where each individual makes a positive choice to be monitored – could be provided on the basis of "consent", though this requires high standards of both the information given to users and the form of consent. If, however, an institution wishes to proactively identify possible mental health and wellbeing problems across all students or staff, rather than waiting for individuals to self-report, Jisc is exploring whether this might be possible under data protection law provisions on "confidential counselling services"[1] or "preventive or occupational medicine".[2]

While proactive use of data may help to ensure that additional support is offered consistently, where there is greatest need, the overall level of such provision – in effect the threshold at which support is offered and the intensity with which it is provided – are likely to remain human and institutional decisions.[3]

The approach taken by Jisc's Code of Practice for Learning Analytics[4] provides a good basis for mental health and wellbeing applications: this Annex indicates – using that Code's headings – where wellbeing practice is likely to differ.

Where wellbeing information is derived from existing learning analytics processes, the stronger controls in this Code should be used from the point where the wellbeing purpose separates from the learning analytics one, in other words where the aim becomes to identify health issues rather than academic ones. For example:

- If additional data are collected for the wellbeing purpose, from the decision to collect that data;
- If different algorithms are used for the wellbeing purpose, from the decision to use those algorithms;
- If tutors are told "this pattern of learning problems may benefit from a wellbeing discussion" then from the decision to create that instruction.

---

[1] *Data Protection Act 2018* Schedule 1 Part 2 section 17

[2] *Data Protection Act 2018* Schedule 1 Part 1 section 2 and *General Data Protection Regulation* Article 9(2)(h)

[3] **https://www.amosshe.org.uk/futures-duty-of-care-2015**

[4] **https://www.jisc.ac.uk/guides/code-of-practice-for-learning-analytics**

Applying the wellbeing standards of validity and minimising adverse impacts may indicate that the two purposes should separate earlier if, for example, they reveal that learning analytics algorithms are not, in fact, the best predictors of wellbeing issues or that some interventions should take place in a health, rather than tutorial, context.

Key Differences from Learning Analytics

Since wellbeing analytics is intended to improve students' health it should be overseen by health professionals, in the same way as analytics to improve students' learning should be overseen by learning professionals. Provided they remain under this authority and are subject to appropriate confidentiality rules, the day-to-day operation of wellbeing analytics may be conducted by appropriately trained and supported tutors and other staff.

Testing and validation of algorithms and processes are even more important for wellbeing analytics, but must be conducted separately, using data minimisation and anonymisation wherever possible, to ensure that information does not leak between the test and production processes. Testers must not see individual identities, counsellors must not be able to see data that was provided only for testing.

Since the likely legal justification for proactive wellbeing analytics is to provide confidential counselling, advice and support, such services must be available to individuals when data, algorithms or other signals indicate that they may be needed.

Wellbeing applications are likely to require a formal Data Protection Impact Assessment (DPIA).

Wellbeing Annex to Learning Analytics CoP

Responsibility

The law requires that processing for preventive medicine must be done "under the responsibility of a professional subject to the obligation of professional secrecy". For wellbeing applications, UUK suggests that such regulated professionals should be found in Student Support Directorates;[5] both Jisc and UUK recommend "extensive consultation with mental health and student counselling specialists".[6] Provided policies and processes remain "under the responsibility" of such professionals, day-to-day operations can be assigned to appropriately trained and resourced tutors and other staff in accordance with appropriate confidentiality rules.

Transparency and Consent

Legal requirements for these are likely to be stronger in health-related applications. If consent is used as a basis for processing (e.g. for installing a wellbeing app, providing additional data, or informing a tutor of contact with a counselling service) there must be "explicit" agreement to the purpose(s) for which the data will be used. In the Information Commissioner's view this requires a separate "express statement of consent" for each purpose.[7] Thus, for example, a student who provides health information for their examination or lecture arrangements should have a separate choice whether or not that information is also used in wellbeing assessments.

Particular care must be taken to inform individuals if unexpected data (e.g. finance) are incorporated into models, and to enable them to check and correct this information. Such data should always have a plausible, and explainable, connection to wellbeing, not just a statistical correlation.

Where a basis other than consent is used, institutions must have a policy document that sets out the legal basis/bases for the processing and describes how the processing satisfies the data protection principles (now in GDPR Article 5). In particular, this document must state how long wellbeing data will be retained for, and how it will

[5] **https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2018/guidance-for-sector-practitioners-on-preventing-student-suicides.PDF**
[6] **http://repository.jisc.ac.uk/6916/1/student-wellbeing-and-mental-health-the-opportunities-in-learning-analytics.pdf**
[7] **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#what5**

be erased. The institution must be able to demonstrate that it is complying with this retention and erasure policy, and that the policy document is being reviewed regularly and updated as necessary.

If, despite these assurances, an individual wishes to opt-out from wellbeing processing, they should be allowed to do so. There is unlikely to be any benefit to the institution or to others that justifies continuing to process for wellbeing against the individual's wishes.

Privacy

As for Learning Analytics, systems must be designed to protect individuals' privacy. Health-related processing and data are likely to require tighter restrictions (both technical and organisational) than that relating to learning. Medical confidentiality standards should be the norm.

Any sharing of information must be in accordance with the legal basis chosen for the wellbeing processing: if processing is based on consent then sharing may only take place where it was covered by that prior consent; if it is part of confidential counselling services then information may only be shared – under an appropriate agreement – with those providing those services. If neither of these apply then information may only be shared in life and death situations where the subject of the information is incapable of giving their consent.[8]

Validity

Given the high risks of adverse consequences (see below) it is essential to ensure that data and predictions derived from them are relevant and accurate. Processing to develop and test algorithms must be kept separate from processing leading to interventions with individuals to ensure that, for example, validation data does not leak into the intervention process and testers are not able to identify individuals.

Particular care is needed to minimise the use of personal data in development and testing: synthetic, anonymous or pseudonymous data should be used wherever possible.

Access

As for learning analytics, individuals have a right of access to their personal data. For data concerning health, however, institutions must first consult with the "relevant health professional" to ensure that disclosing the information is not likely to cause serious harm to the physical or mental health of the data subject or another individual.[9]

Enabling Positive Interventions/Minimising Adverse Impacts

As with Access, some interventions carry a risk of making a wellbeing problem worse, rather than better. Talking to someone about stress, depression or suicide requires both training and readily available support. Data and algorithms will flag individuals with widely differing needs: personalised support is likely to be needed.

Institutions should therefore consider which interventions should be provided in a medical context, in case of a negative reaction, and should ensure that they can provide appropriate support before implementing any wellbeing application.

Stewardship

Wellbeing applications that aim to derive information about an individual's health are likely to represent a high risk to privacy, and thus require a formal Data Protection Impact Assessment (DPIA).[10] Where this risk cannot be

[8] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/

[9] *Data Protection Act 2018* Schedule 3 Part 2

[10] **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/**

mitigated – though referral to a confidential counselling service should usually do this – the law requires prior consultation with the national Data Protection Regulator – in the UK, the Information Commissioner's Office.