DRAFT Mental Health and Wellbeing Analytics Code of Practice

Draft 0-95 3rd March 2020

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

Summary

Whereas learning analytics uses data to inform decisions – from individual to curriculum level – on how to support students' learning, data may also be used to inform decisions on how to support 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 such uses of data can involve both significant benefits and high risks. This Code of Practice suggests how universities, colleges and other tertiary education providers can ensure that their use of data to support wellbeing does not create risks for students or staff, taking responsibility and demonstrating accountability for their actions in selecting, developing, implementing, operating and reviewing data-informed wellbeing processes. As the headings in the Code indicate, this will involve working with groups and individuals across the institution: Stewardship, Transparency, Responsibility, Validity, Positive Interventions, Privacy, and Access need to be developed with students, staff, data owners, IT services and university governance, as well as student support services and data protection officers. Universities UK refers to this as a **"whole-university approach"**; Student Minds' University Mental Health Charter calls it a **"cohesive ethos"**. To support these discussions, this Code also includes practical tools – for Data Protection Impact Assessments and purpose compatibility assessment for data sources – that should help to ensure the institution's activities are, and can be shown to be, both safe for individuals and compliant with the law.

Introduction

The approach taken by Jisc's **Code of Practice for Learning Analytics** provides a good starting point for mental health and wellbeing applications. This Mental Health and Wellbeing Code provides a detailed discussion of additional issues raised by the use of data for wellbeing purposes. Here we concentrate on the use of data in delivering wellbeing and mental health support: broader issues such as duty of care, healthcare treatment, human rights, equality and discrimination are not covered, though we have referenced relevant guidance on those issues where we are aware of it.

When delivering wellbeing and mental health support, institutions are likely to be processing personal data concerning health; some forms of analytics may aim to infer such data from other, behavioural, indicators, such as the student's engagement with learning systems and processes. Thus, as well as meeting the legal standards that apply to all processing of personal data, wellbeing and mental health applications must satisfy the additional conditions and safeguards that apply to **Special Category Data**. This Code of Practice therefore includes safeguards from several areas of the General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 that may be relevant when addressing mental health and wellbeing. In particular:

- Voluntary wellbeing apps – where each individual makes a positive choice to report or be monitored – could be provided on the basis of "consent", though this requires both clear and detailed information to be given to users and that their consent be freely given, informed, unambiguous, specific, explicit and recorded;

- If, however, an institution wishes to provide support across all students, or all of a group – for example by increasing the information available to appropriately-trained tutors and support staff when they have conversations with students or by flagging students who may need to be contacted proactively – then consent cannot be used as a basis. To help institutions fulfil their responsibilities in these circumstances, this Code includes safeguards applicable to processing in the substantial public interests of preventive medicine and "protecting the physical, mental or emotional well-being" of individuals who are at risk of one or more of those types of harm;
- Where using existing, historic, data to develop and test statistical models, provisions and safeguards on research use of personal data may be most appropriate.

A detailed discussion of these, and other, lawful bases for processing health data can be found in Step 4 of the Annex A: Data Protection Impact Assessment template for Wellbeing/Mental Health Analytics below.

Increased use of data may help to ensure that additional support is offered consistently and effectively, where there is greatest need. However the overall level of such provision – in effect the threshold at which support is offered and the kinds and depth of support that are provided – is likely to remain an institutional choice. AMOSSHE's **discussion of universities' Duty of Care** suggests the level of provision likely to be required by law.

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

- If the organisation decides to collect additional data for the health/wellbeing purpose, this Code, rather than the Learning Analytics one, should apply to the decision to collect that data and thereafter;
- If the organisation decides to use different algorithms for the health/wellbeing purpose, use this Code from the decision to use those algorithms;
- If tutors, or other support staff, are told "this pattern of learning problems may benefit from a wellbeing discussion", use this Code from the decision to create that instruction;
- If, during normal tutorial conversations, an individual tutor suggests to a student that they might seek other kinds of help, that would be covered by normal tutorial processes, not this Code of Practice.

Consideration of Validity and Enabling Positive Interventions/Minimising Adverse Impacts (see below) may indicate that the purposes of learning analytics and health/wellbeing should separate earlier. For example those principles may 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 mental health and 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 mental health and wellbeing analytics may be conducted by appropriately trained and supported tutors and other staff (see under Responsibility below).

A wider range of data sources may be relevant to mental health and wellbeing than for learning analytics: both environmental indicators of when a student may be in a stressful situation (for example a change of course) and behavioural ones that suggest they may not be coping (for example a sudden change in study pattern). Some of these sources may have been collected for very different purposes, and students may not expect them to be re-used in this way. Institutions will therefore need processes to determine whether it is appropriate to include a particular data source and, if so, what additional measures may be needed (see under Transparency and Consent below and Annex B: Purpose and Transparency for Wellbeing/Mental Health Analytics).

Testing and validation of algorithms and processes are even more important for mental health and wellbeing analytics because of the serious consequences if they go wrong. However such testing must be conducted separately, using data pseudonymisation 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 (see under Validity below).

Since the likely legal justification for proactive mental health and wellbeing analytics is to provide support to individuals, institutions must ensure that adequate services to provide such support will actually be available to individuals when data, algorithms or other signals indicate that they may be needed (see under Enabling Positive Interventions/Minimising Adverse Impacts below).

Health and wellbeing applications will require a formal Data Protection Impact Assessment (DPIA), involving stakeholders and the organisation's data protection team (see under Responsibility below and Annex A: Data Protection Impact Assessment template for Wellbeing/Mental Health Analytics).

Mental Health and Wellbeing Analytics CoP

Jisc's **Code of Practice for Learning Analytics** provides a baseline for supplementary uses of student data. This Code uses the same headings: for each it highlights key common areas (for which detail can be found in the Learning Analytics Code) before a detailed discussion of additional issues raised by the use of data for mental health and wellbeing purposes.

Responsibility

From the Learning Analytics Code:

"Institutions must decide who has overall responsibility for the legal, ethical and effective use of analytics"

"Student representatives and key staff groups at institutions should be consulted about the objectives, design, development, roll-out and monitoring of analytics"

Confidence and trust among students, staff and wider stakeholders is essential if wellbeing activities are to be beneficial, rather than harmful. To achieve this, institutions will need to show that they are taking responsibility: consulting and planning carefully before implementing any policies, processes, systems or data gathering, and checking to ensure they deliver the expected results. The GDPR's principle of **Accountability** addresses many of these issues: designing processes and systems to ensure they protect personal data and the rights of individuals, monitoring those processes to ensure they are followed, and reviewing them to see where they can be improved. This Code suggests various documents and records – assessments of Data Protection Impact and Purpose Compatibility; Records of Processing Activity, mapping of data flows, and policies on use of Special Category Data – that the institution can use to demonstrate Accountability and reassure students, staff and stakeholders.

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). This includes identifying the relevant legal basis or bases for processing and ensuring that their specific requirements are satisfied. Several organisations have published processes for conducting DPIAs, including **UCISA** and the **Information Commissioner's Office**; Annex A below specific guidance on using these processes to assess proposed wellbeing activities.

Where a high risk cannot be mitigated – though a successful DPIA process should normally do this – the institution should consider whether to continue with the proposal. If it decides to do so, the law requires prior consultation with the national Data Protection Regulator: in the UK, the Information Commissioner's Office.

The law requires that processing for preventive medicine must be done "under the responsibility of a professional subject to the obligation of professional secrecy" (*Data Protection Act 2018* s.11(1)(a)). For mental health and wellbeing applications, UUK suggests that such regulated professionals should be found in Student Support Directorates; both **Jisc** and **UUK** recommend "extensive consultation with mental health and student counselling specialists". 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. Student Minds' **University Mental Health Charter** stresses that "it is vital that staff in these roles are properly equipped, qualified, registered and supervised. This need for quality assurance extends to other interventions, such as the provision of digitally based services".

Transparency and Consent

From the Learning Analytics Code:

"The data sources, the purposes of the analytics, the metrics used, who has access to the analytics, the boundaries around usage and how to interpret the data must be explained clearly to staff and students"

"Collection and use of data for [new purposes] may require further measures, such as data protection impact assessments and obtaining additional consent"

Because health-related applications involve Special Category Data, the legal standards for transparency and consent (if that is the chosen legal basis) are likely to be stronger than for Learning Analytics.

Individuals must be informed which data will be used for mental health and wellbeing purposes. This may be done through a privacy notice at the time of collection and/or through additional communications before data are used; where information is received from third parties individuals must be informed before it is used, and at the latest one month after it is received. Such notices and communications also provide an opportunity to explain that institutions have responsibilities beyond just teaching. The Information Commissioner's Office has guidance on **the content of privacy notices**. All notices and communications must be written so as to enable individuals to make informed choices. Special care is needed to ensure clarity and fairness when **addressing those under 18**: in particular, when providing information about the processing and its consequences, offering choices to individuals, and explaining the rights they have and how to exercise them.

As well as transparency to individuals, institutions can also build trust and confidence more widely by being transparent about how they design and review their processes and systems. Publishing Data Protection Impact Assessments, Purpose Compatibility Assessments and Records of Processing Activity can demonstrate both that the institution is thinking very carefully about what it does, and that it is providing important support services while minimising the risk to individuals.

Purpose Compatibility

Whereas learning analytics will generally be based on data about the learning process, for mental health and wellbeing a wider range of data sources may contain relevant information. This is likely to include both environmental indicators of when a student may be in a stressful situation and behavioural ones that suggest they may not be coping. Particular care must be taken to inform individuals if unexpected data (e.g. finance) are incorporated into wellbeing models or processes, and to enable them to check and correct this information. Such data should always have a plausible, and explained, connection to mental health and wellbeing, not just a statistical correlation (for example financial difficulties might well be a factor in reducing a student's wellbeing). In addition, the original reason for collecting/obtaining the data must be compatible with the new purpose of offering wellbeing/mental health interventions. This requirement is likely to be met where information is already used to provide individual academic or health support, but less so where information was originally collected for statistical, or other, purposes (for example if you already provide additional support to students with no family experience of higher education then wellbeing support is more likely to be a compatible purpose than if you only collect that information for statistical reporting). Where the original purpose is not compatible with wellbeing, the privacy notice must first be changed; only data collected after the notice is changed may then be used for the new purpose. Transparency is likely to be a particular challenge where institutions receive information from third parties since these may offer limited, or no, control over privacy notices. Regular sharing of data with third parties should be covered by a **Data Sharing Agreement**. Annex B below has a more detailed discussion of how to assess purpose compatibility and the need for notification.

Before including a particular data source into a health/wellbeing analytics model, institutions must therefore consider:

- How privacy notices will be provided;
- (For existing data) whether health/wellbeing is compatible with the purpose(s) for which the data are currently collected;
- How they will ensure the data are accurate (see Validity below);
- How students can exercise their legal rights over their data (see Access below).

Where a basis other than consent is used, institutions should have a policy document that sets out the legal basis/bases for the processing and describes how the processing satisfies the **data protection principles**. In particular, this document must state how long health/wellbeing data will be retained for, and how it will 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. The Information Commissioner's **guide to Special Category Data** has more information on when this "appropriate policy document" is required and what it should contain.

Consent

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 **a separate "express statement of consent"** to the use of health data for each purpose. Thus, for example, a student who volunteers health information in requesting special examination or lecture arrangements must have a separate choice whether or not that information is also used in wellbeing assessments.

Step 4 of the Annex A: Data Protection Impact Assessment template for Wellbeing/Mental Health Analytics in Annex A discusses when consent will and will not be an appropriate basis for processing and the alternatives that exist.

Withdrawal/Objection

Where the legal basis for health/wellbeing processing is consent, individuals always have the right to withdraw their consent at any time. Note, however, that so long as a statistical model does not contain personal data, such a withdrawal should not extend to **requiring a model to be recalculated**.

In other cases – except where institutions have a legal obligation to process health information, or when there is a threat to life and the individual is incapable of giving consent – individuals are likely to have a **right to object**. Formally, this only requires the institution to consider whether the individual's personal circumstances mean the processing places them at higher risk. Where the processing is intended to support the individual's wellbeing and mental health, it may be better to treat such objections as a simple opt-out, and record that the individual's data should not be used either for developing systems and processes or for providing personalised treatment. There is unlikely to be any benefit to the institution or to others that justifies continuing to process for wellbeing against an individual's wishes. Since wellbeing support is designed to benefit the individual, institutions may wish to reflect on why such support was refused.

Privacy

From the Learning Analytics Code:

"Access to student data and analytics should be restricted to those identified by the institution as having legitimate need to view them"

"Institutions should ensure that student data is protected when third parties are contracted to store or carry out analytics on it"

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 standards for **confidentiality, granting and controlling access** should be the norm. Systems and processes must be designed to use **no more data than is necessary** (see also Validity below); data obtained for one purpose **must not be used for others** without the individual's agreement (see Consent above); data should have a **defined retention period or event**, and be deleted or anonymised once that passes.

Health or wellbeing information can only be shared with third parties if there is an appropriate legal basis for this. For example:

- if processing is based on consent then sharing must be covered by that prior consent;
- if sharing is part of physical, mental or emotional wellbeing services then information may only be shared – under an appropriate data sharing agreement – with those providing those services;

- if there is a legal duty to share, this must be limited to information covered by that duty, and under the safeguards prescribed;
- if none of these applies then information may only be shared in life and death situations where the subject of the information is incapable of giving their consent.

Validity

From the Learning Analytics Code: "It is vital that institutions monitor the quality, robustness and validity of their data and analytics processes in order to develop and maintain confidence in analytics and ensure it is used to the benefit of students"

Given the high risks of adverse consequences (see Enabling Positive Interventions/Minimising Adverse Impacts below) it is essential to ensure that data and predictions derived from them are relevant and accurate.

Systems and processes for wellbeing support may use personal data in three different ways: first when developing models that suggest indicators of need, second ("production") when using the models to identify which individuals may benefit from intervention, and third when reviewing whether the intervention processes were beneficial. At each stage accurate data is essential to reduce the risk of inappropriate interventions. Students and staff should therefore be enabled and encouraged to exercise their **right to correct errors and omissions** in their data, but institutions should not rely on this as the only way to **ensure accuracy**. Processes for obtaining and handling data should also be designed with safeguards to avoid introducing errors, and to detect those that may nonetheless arise.

Processing to develop and review models, systems and processes is vital, but 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.

At each of the three stages, the processing of personal data must be **minimised** (i.e. no more than is necessary to achieve the purpose), while delivering effective results. Development and review are likely to require a wider range of personal data than production systems. To determine effectiveness, they need historic data on the outcome of past (non-)interventions. To identify the most informative data sources, they will consider data sources and fields that are subsequently excluded from production models, for example because tests conclude that they do not make a significant contribution to alerts, or because the risk of including them is not justified by the benefit, or because their accuracy cannot be ensured, or because the required privacy notices and individual rights cannot be supported.

The greater range of data used in development and review requires particular care to be taken to minimise the risk of data processed for these purposes being linked to individuals. Synthetic, anonymous or pseudonymous data should be used wherever possible: the GDPR recognises pseudonymisation as a safeguard, but still classes pseudonyms as personal data; processes for generating anonymous or synthetic data **must be reviewed periodically** to ensure they remain safe. Those developing models should be aware of, and manage, the risks that they may inadvertently reveal personal data: see the Information Commissioner's blog on **Privacy Attacks**.

Development and periodic review must ensure that models are, and remain, proportionate. They should also be checked for signs of bias or discrimination. Models must provide useful information to guide the provision of support while involving the least possible risk to individuals: both those who are identified as needing support and those who are not. Any predictive system or process will make mistakes: organisations should consider, and balance, the risk of alerting someone who did not need support, as well as failing to alert someone who did (see also Enabling Positive Interventions, below). The ICO's AI Framework[1] contains more detail on the use of algorithmic techniques with personal data.

[1] # add hyperlink when available

Access

From the Learning Analytics Code:

"Students should be able to access all analytics performed on their data in meaningful, accessible formats"

"They should normally also be able to view the metrics and labels attached to them"

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 (*Data Protection Act 2018* Schedule 3 Part 2).

Enabling Positive Interventions/Minimising Adverse Impacts

From the Learning Analytics Code:

"Institutions should specify under which circumstances they believe they should intervene"

"The type and nature of interventions, and who is responsible for carrying them out, should be clearly specified"

"The impact of interventions on staff roles, training requirements and workload should be considered"

"Analytics systems and interventions should be carefully designed and regularly reviewed to ensure that: students maintain appropriate levels of autonomy in decision-making; knowledge that their activity is being monitored does not lead to negative impacts; adverse impacts are minimised; staff have a working understanding of legal, ethical and unethical practice"

As with Access, some interventions carry a risk of making a mental health or 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. Note that this may also apply where a concern may has been raised but appears to be a false alarm: as well as reviewing the model and process that led to the concern being raised, institutions should consider whether such individuals now need support to avoid them becoming self-fulfilling prophecies.

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

Stewardship

From the Learning Analytics Code:

"Data for analytics must comply with existing institutional data policies and [relevant legislation]"

The involvement of institutional Data Protection Officers will be essential to maintaining accountability and compliance in this complex and developing area. Regular reviews of the institution's policies, practices and risk assessments should include both DPOs and appropriate health professionals. These reviews should cover, as a minimum, the Data Protection Impact Assessment, Purpose Compatibility Assessment, and the policy document and processes for Special Category Data.

However responsible and respectful use of data is only likely to be ensured by an appropriate cross-institutional culture: in Universities UK's terms a **"whole-university approach"** or Student Minds' **"cohesive ethos"**.

Annex A: Data Protection Impact Assessment template for Wellbeing/Mental Health Analytics

This template is an example of how you can record your DPIA process and outcome. It follows the approach set out in the **Information Commissioner's DPIA guidance**, and should be read alongside that guidance and the **Criteria for an acceptable DPIA** set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
The ICO provides **guidance** on when a DPIA should be completed, including a link to the **European guidelines**. The former includes the ICO requirement that a DPIA is completed in the following (but not limited to) circumstances: ▪ use profiling or special category data to decide on access to services; ▪ profile individuals on a large scale; ▪ match data or combine datasets from different sources; ▪ collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines); ▪ track individuals' location or behaviour (in combination with any of the criteria from the European guidelines); The latter provides examples of the type of processing that is "likely to result in high risks", including: ▪ a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; ▪ processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or ▪ a systematic monitoring of a publicly accessible area on a large scale. Since the "special categories of data referred to in Article 9(1)" include "personal data revealing … data concerning health", these criteria suggest that many health and wellbeing applications will require a formal Data Protection Impact Assessment (DPIA). Even where it is not a legal requirement, a DPIA is likely to reassure students, staff and other stakeholders that the institution is being responsible in its use of personal data.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
The questions in Annex B may help you think about your data sources and the issues that may be involved in using them

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
The questions in Annex B may help you think about the nature and type of data and your **record of processing** could be attached within this section.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, for individuals who may need support, and more broadly? What evidence do you have that this will help to address a current problem?
Depending on the institution's existing student support provision, purposes to improve student wellbeing might include, for example: • Providing wellbeing/mental health support to those who request it. Such requests might take the form of visiting student support services, accepting an offer of assistance, or installing a wellbeing app; • Improving the availability of relevant data to staff who are trained to deal with wellbeing and mental health issues. This might be to enable quicker assessment of need and appropriate intervention (triage, data-informed conversations, etc.) or simply to reduce the amount of stress and potential error involved in re-entering existing data; • Testing and review of the effectiveness of wellbeing services; • Early identification of possible warning signs of a mental health issue within the provision of a universal wellbeing service that is trying to deal with large numbers of students. If you will be including existing data or data sources into your processing, you should consider whether these purpose(s) are compatible with those for which they are currently used: Annex B provides more guidance. Note, in particular, that 1. you are likely to need to add the new purpose to the information (e.g. privacy notice) that is provided to students, and 2. if the new purpose(s) are not compatible then you may only be able to use data that is collected after you make that change, not pre-existing data.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
Prior to the implementation of any Mental Health and Wellbeing Analytics, it is strongly recommended that consultation with relevant groups is conducted, including: ▪ Students or their representative bodies; ▪ Relevant health professionals; ▪ Learning professionals / tutors / others likely to be the first point of contact with the student ▪ Data Protection Officer.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

NB processing for wellbeing is likely to involve Special Category Data and therefore require a lawful basis under both Art.6(1) of the GDPR and Art.9 GDPR/Schedule 1 of the Data Protection Act 2018.

The appropriate basis/bases are likely to vary between institutions, as well as depending on the nature on the proposed activity and, perhaps, the students to be covered. Each institution will therefore need to make its own choice. For a detailed discussion, see Annex 2 of Universities UK's 2015 **"Student mental wellbeing in higher education"** good practice guide and a 2018 article on the **"Duty to Care for Student Mental Health"** by Pinsent Masons.

In terms of GDPR Article 6(1), the likely bases, and the circumstances and conditions under which they may apply, include:

- Art 6(1)(b) "contract", where the institution's contract with students contains provisions relating to the nature, extent and limitations of the wellbeing and mental health support services offered by the institution (see **ICO guidance on this basis**); or
- Art 6(1)(c) "legal duty", where the institution is required to protect the mental health of students and staff, for example under the Health and Safety at Work Act 1974 (see **ICO guidance**); or
- Art 6(1)(e) "public task", where processing is necessary for the institution to perform a task in the public interest of for its official functions, and the task or function has a clear basis in law. This clear basis might be found in a law, statutory code/guidance, charter, statute or ordinance, or **common law duty**, so long as it establishes a clear and foreseeable basis for the institution's actions to support the wellbeing of its students (see **ICO guidance**); or
- Art 6(1)(f) "legitimate interest", where there is no such clear basis in law but, in its own interest and that of students, the institution nonetheless wishes to act to protect their wellbeing. In this case the institution must perform and document a Legitimate Interests Assessment (see **ICO guidance**) to ensure those legitimate interests are not over-ridden by the rights and freedoms of students and staff; and
- Art 6(1)(a) "consent" if the institution wishes to invite students to provide additional information on a voluntary basis, e.g. by reporting study hours through an app or disclosing coursework concerns in a face-to-face meeting. In this case the institution will need to obtain (and record) active, free, informed consent and allow such consent to be withdrawn at any time (see **ICO guidance**). The nature of the institution/student relationship is likely to mean that consent is presumed not to be free unless the institution can demonstrate that there was no direct or indirect pressure on the student to agree.

Likely bases under Article 9(2)/DPA2018 (see also the **ICO guidance**) are

- Art 9(2)(g) "substantial public interest"/Schedule 1 para 18(1)(a)(ii) "protecting the physical, mental or emotional well-being of an individual", where the institution wishes to take proactive measures (e.g. information sharing, linking or analytics) to provide care and support to all, or groups of, its students. Note that sub-paragraphs 18(2)-(4) permit processing the data of groups ("a type of individual") where this is necessary to identify those individuals in the group who are at risk. In this case the institution must

have a policy document setting out how the processing is in accordance with the data protection principles, and how it ensures that data are held in accordance with its retention schedule (see the **ICO guidance on Schedule 1 para 40**); or

- Art 9(2)(j)/Section 19 "scientific research", for the specific purpose of developing or testing statistical models against historic data. This condition cannot be used in a blanket manner: for each development or test the institution must ensure (and document) that the activity is not likely to cause substantial damage or distress to individuals, in particular that models will not retain personal data and that test data are not used for measures or decisions about individual students; and
- Art 9(2)(a) "consent" where the institution wishes to invite students to provide additional information on a voluntary basis, e.g. reporting state of wellbeing through an app or disclosing previous mental health issues in a face-to-face meeting. In this case the institution will additionally need to obtain (and record) active, free, informed and explicit consent. The nature of the institution/student relationship is likely to mean that consent is presumed not to be free unless the institution can demonstrate that there was no direct or indirect pressure on the student to agree.

For any basis other than consent, the institution must also ensure that the processing is "necessary" to achieve the purpose. This does not mean that processing has to be absolutely essential. However, it must be more than just useful, and more than just standard practice. It must be a targeted and proportionate way of achieving a specific purpose. The lawful basis will not apply if the purpose can reasonably be achieved by some other less intrusive means, or by processing less data. It is not enough to argue that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is objectively necessary for the stated purpose, not whether it is a necessary part of your chosen methods. Given the potentially intrusive nature of processing of student data for wellbeing and mental health, the institution must examine the processing closely, and satisfy themselves that the approach to processing is, and continues to be, both necessary and proportionate to the benefits it can provide.

In particular, if relying on Schedule 1 paragraph 18 to justify processing of a whole group or cohort of students, the processing must be necessary to identify those individuals among the group who need care and support, are at risk of mental or emotional harm, and are unable to protect themselves from that harm. Processing under this basis must be intended, designed and resourced, to support more than just those students who request it (i.e. those who consent).

As well as documenting the legal basis/bases for processing, organisations should assess how the processing will satisfy each of the Data Protection principles (in GDPR Article 5), and how the relevant individual rights (in Articles 13 to 22) will be provided. This information will form part of the Policy Document for Special Category Data that is required for most legal bases.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary, but the focus must be on the impact to individuals. The following table suggests some risks likely to arise when processing data for wellbeing and mental health. Individual organisations may identify others that result from their particular situations. You should assess the likelihood and severity of these inherent risks, and score them as low, medium or high.

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5. The following table suggests some measures that may be used to mitigate risks. Individual organisations may identify others that are appropriate to their particular situations. Assess what the likelihood and severity will be after you apply the mitigations, and score the residual risk as low, medium, or high. Where there is a residual 'high' risk, you should seriously consider whether continuing with the processing is appropriate. If you consider that the processing should continue and there is no way of mitigating or reducing the risk, you must consult with the ICO.

Principle/Right	Example Risk Description / Impact on Individual	Inherent Risk			Example Mitigation	Residual Risk		
		Likelihood	Severity	Risk Score (LxS)		Likelihood	Severity	Risk Score (LxS)
Lawful, Fair, Transparent	Students not provided with privacy notices resulting in confusion, mistrust				▪ *Privacy Notice provided at the point of data collection and/or appropriate points before and during processing.*			
	Privacy notice is unclear / complex and not understood by students				▪ *Privacy Notice is written in plain, intelligible language, with consideration of the audience using a combination of techniques.* ▪ *Feedback from students is solicited when creating Privacy Notices.* ▪ *A governance process exists to review and approve Privacy Notices periodically.*			
	If basis is Public Task, processing not necessary to protecting the physical, mental or emotional well-being of an individual (DPA2018 Sch1 para 18)				▪ *A necessity and proportionality test is carried out and documented.*			
	If basis is Legitimate Interests, balancing test not performed, and the rights and freedoms of the individuals are not properly assessed.				▪ *Legitimate Interests Assessment performed*			

Principle/Right	Example Risk Description / Impact on Individual	Inherent Risk			Example Mitigation	Residual Risk		
		Likelihood	Severity	Risk Score (LxS)		Likelihood	Severity	Risk Score (LxS)
	Except where basis is Consent, the processing is not necessary to achieve the purpose, resulting in unnecessary privacy risks to individuals.				▪ *A necessity and proportionality test is carried out and documented.*			
	If basis is Consent, obtained in invalid ways (e.g. uninformed, not opt-in, or not freely given, not separate to other terms), meaning individuals are not aware of the processing of their personal data.				▪ *Consent, if used, is appropriately informed, granular, fair and explicit* ▪ *Consent is separate to all other terms and conditions.* ▪ *Students who refuse to give consent are not excluded from signposting / services offered.*			
	Unclear or unsafe sharing of data to/from third parties, increasing the risk that personal data could be inappropriately accessed, lost, altered or destroyed. Individuals may be unclear on how / who to submit an individual rights request to, or may be the victim of impersonation fraud etc.				▪ *Privacy notices make clear the identity and relationships of all data controller(s)* ▪ *Privacy notices include third party data sources, any third parties with whom data may be shared, and legal basis* ▪ *Data Controller/Data Processor contracts where appropriate* ▪ *Data Sharing Agreements & Contracts for controller-controller sharing*			
					▪			

Principle/Right	Example Risk Description / Impact on Individual	Inherent Risk			Example Mitigation	Residual Risk		
		Likelihood	Severity	Risk Score (LxS)		Likelihood	Severity	Risk Score (LxS)
Limited to the specified and legitimate purpose	Failure to identify and document the purpose for processing increases the risk that the personal data is inappropriately used or re-purposed.				▪ *Documented legal basis for processing; policies and processes for retention and disposal of personal data.* ▪ *Comprehensive record of the processing activity exists.*			
	Data used for purpose incompatible with original purpose without gaining individual's consent / Data used for undeclared purpose (e.g. special examination circumstances request used for wellbeing alert; third-party data incorporated into models without notice), meaning students are unaware that their personal data is being processed and the purpose is not within their reasonable expectations.				▪ *Record of processing activity defines the personal data being processed and the purpose, any changes must be subject to a defined change management Policy or process.* ▪ *Where research/statistics is used as basis for model building, technical and organisational processes required of that legal basis (see DPA2018 s.19)* ▪ *Data is stored in structured databases with restricted access to prevent further use. Policies, training, access controls & monitored audit logs for staff with authorized access to data and alerts.* ▪ *Students must (re-)consent to incompatible / re-purposing of data and the record of processing is updated to reflect the new purpose.*			

Principle/Right	Example Risk Description / Impact on Individual	Inherent Risk			Example Mitigation	Residual Risk		
		Likelihood	Severity	Risk Score (LxS)		Likelihood	Severity	Risk Score (LxS)
					▪			
Adequate, relevant and limited to what is necessary	Information processed (whether collected or observed) is in excess of what is required for the processing, potentially creating further copies of (unnecessary) personal data and increasing the privacy risks associated with a security breach.				▪ *Consultation with stakeholders (including students and specialists) to identify most appropriate data sources & fields to include in processes* ▪ *Where existing / third party data is used this is limited to what is absolutely necessary. Irrelevant data is deleted.* ▪ *Where forms are used to collect data from students these are subject to specific governance and approval and designed around the specific requirements of wellbeing/mental health processes.*			
	Information processed (whether collected or observed) is not sufficient or relevant to fulfil the purpose, potentially resulting in inaccurate or misleading outputs.							
	Predictive models infer information beyond intended scope, creating unnecessary (potentially special category) data outputs.				▪ *A model governance policy exists to provide a framework for ensuring the integrity of models, including:* ▪ *Designated model owner;* ▪ *Regular performance reviews;* ▪ *Independent validation.*			

Principle/Right	Example Risk Description / Impact on Individual	Inherent Risk			Example Mitigation	Residual Risk		
		Likelihood	Severity	Risk Score (LxS)		Likelihood	Severity	Risk Score (LxS)
					▪			
Accurate and up to date	Data collected / used is inaccurate / out of date resulting in counter-productive (non) intervention				▪ *Where data sets are matched, controls exist to ensure accuracy of the matching.* ▪ *Quality assurance checks are performed to ensure the accuracy of manually entered data.* ▪ *Students are required to validate that the information they have provided is accurate.*			
	Lack of context resulting in inappropriate conclusions being drawn (e.g. lack of VLE use due to student preferring books), and inaccurate inferences about individuals.				▪ *Conversations with students are conducted by staff with appropriate training and knowledge of context to identify these problems*			
	Cause/effect impact – predictive model generates a high number of false-positives which affects student behavior/ well-being (e.g. model indicates a mental health problem, student starts to exhibit				▪ *Prior consultation with health professionals to ensure models and processes avoid this risk.* ▪ *Students who are offered interventions based on model output (especially those who appear to be "false positives") are offered on-going support to*			

Principle/Right	Example Risk Description / Impact on Individual	Inherent Risk			Example Mitigation	Residual Risk		
		Likelihood	Severity	Risk Score (LxS)		Likelihood	Severity	Risk Score (LxS)
	signs of deteriorating mental health as a result)				*detect and avoid adverse consequences*			
	Data collected from third parties is inaccurate / out of date, resulting in false positives / false negatives.				▪ *Data is only collected from trusted sources.* ▪ *Due Diligence is completed on all third parties supplying personal data.*			
Storage Limitation – kept for no longer than necessary	Personal data is held for longer than necessary, increasing the privacy risks associated with a security breach				▪ *Where possible, synthetic, anonymized or pseudonymized data is used.* ▪ *Record Retention Policy defines the periods of time for which the personal data can be retained (note that different purposes may require different datasets to be retained for different periods, e.g. model/process review may require pseudonymised historic data).* ▪ *Quality assurance is performed to ensure no records are held outside of the Policy requirements.* ▪ *Processes exist to delete data when students make an individual rights request.*			

Principle/Right	Example Risk Description / Impact on Individual	Inherent Risk			Example Mitigation	Residual Risk		
		Likelihood	Severity	Risk Score (LxS)		Likelihood	Severity	Risk Score (LxS)
Integrity and Confidentiality – Protected against unauthorised or unlawful processing, accidental loss, destruction or damage	Student's personal data, including special categories of personal data is unlawfully accessed, deleted or modified, resulting in the risk of impersonation fraud or other distress caused by sensitive personal data becoming public.				▪ *Where possible, synthetic, anonymized or pseudonymized data is used.* ▪ *Data is encrypted in transit and at rest.* ▪ *Appropriate controls exist to prevent unauthorised access to personal data. Where potential unauthorised access is suspected, this is alerted.* ▪ *Patch & vulnerability management processes are in place including vulnerability scanning and penetration testing.* ▪ *Policies and processes are in place for incident detection, response and notification.* ▪ *Appropriate physical and people security Policy is in place.*			
	Access to necessary personal data is unlawfully / unexpectedly restricted, preventing the identification of a support need or critical intervention				▪ *Patch & vulnerability management processes are in place including vulnerability scanning and penetration testing.* ▪ *Back-up*			
Individual Data Protection Rights	Students cannot exercise their rights in relation to the processing of their personal data (note that subject				▪ *The Privacy Notice clearly explains how requests can be made and where they should be directed*			

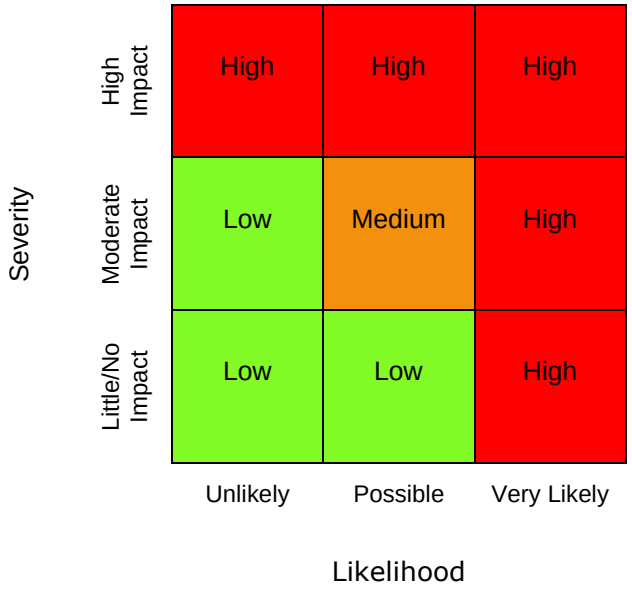
Principle/Right	Example Risk Description / Impact on Individual	Inherent Risk			Example Mitigation	Residual Risk		
		Likelihood	Severity	Risk Score (LxS)		Likelihood	Severity	Risk Score (LxS)
	access right is modified for health data)				▪ *The institution has a clearly defined process for dealing with Individual Rights requests, all relevant colleagues receive training on how to recognise a request* ▪ *[where the basis is Public Task or Legitimate Interests] Students are able to object to their data being processed and a process exists for assessing such objections* ▪ *[where predictive models are used] Students are provided with a means to request manual intervention and the model owner can explain how the model works* ▪ *[if automated decision making is used] Students can object to being subject to individual automated decision making or predictions and a process exists implement these objections.*			
Other Individual Rights and Freedoms	'Surveillance' perception leads to change of behavior (e.g. student avoids using institutional services, or hides true feelings)				▪ *Transparency (e.g. through intranet page and opportunity to ask questions) about data, purpose and interventions.* ▪ *Regular consultation and feedback opportunities with students*			

Principle/Right	Example Risk Description / Impact on Individual	Inherent Risk			Example Mitigation	Residual Risk		
		Likelihood	Severity	Risk Score (LxS)		Likelihood	Severity	Risk Score (LxS)
					▪ *Monitoring of use of services/responses to surveys from which data are gathered*			
	Intervention is perceived as an infringement of privacy (despite the mitigation(s) in place) resulting in students 'dropping out' rather than accepting support				▪ *Prior consultation with student representatives to avoid actions that might trigger these perceptions.* ▪ *Student behaviour (e.g. use of support services) is monitored over time to detect such responses.*			
	Intervention by insufficiently trained/wrong staff, or in wrong setting, causes harm to student and / or staff				▪ *Clear, comprehensive processes and training to ensure signals are acted on promptly by appropriate staff/organisations*			
	Students are refused access to services / subject to discrimination as a result of the model output				▪ *Models and the processes based on them are monitored for signs of discrimination. Process exists for making appropriate interventions and corrections*			
	Critical support need is identified but student refuses assistance				▪ *Alarms at critical level should be handled by health professionals, trained and supported to make decisions on further treatment in these circumstances*			

Principle/Right	Example Risk Description / Impact on Individual	Inherent Risk			Example Mitigation	Residual Risk		
		Likelihood	Severity	Risk Score (LxS)		Likelihood	Severity	Risk Score (LxS)
					▪ *Review of processes/procedures following any such event*			
	Support need is identified but the university don't have the resources to deal with it				▪ *Prior consultation with relevant parties (e.g. health professionals supporting the universities) to assess likely level and nature of support needs* ▪ *Clear signposting of other support provision, where appropriate* ▪ *Review group established to identify trends and recommend priorities*			

Assessing the risk

In considering the risk score it may be useful to use the matrix below as a guide.



Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Annex B: Purpose and Transparency for Wellbeing/Mental Health Analytics

Many of the data sources likely to be used for wellbeing and mental health analytics will have been collected for other purposes. Some may have been collected by other organisations acting as data controllers. This raises various issues under data protection law, including:

- Whether the wellbeing and mental health analytics purpose is compatible with that original purpose; and, deriving from that
- What processes and privacy notices may be needed to inform students of the new purpose, to ensure that the new purpose is fair and transparent and, in some cases, to get individual's consent to it.

Article 6(4) of the General Data Protection Regulation covers compatible and incompatible purposes, Articles 13 and 14 cover privacy notices respectively where the information is obtained direct from the individual data subject or from a third party (for example through a data sharing agreement). The following questions aim to help institutions to gather and record the information they will need to assess purpose compatibility and transparency requirements. Two examples show how this can be used to update the organisation's Record of Processing Activities, and how to identify which data sources are likely to be more or less challenging to reuse for the purpose of wellbeing and mental health analytics.

Purpose/Transparency questions

For each data source being considered the institution should answer the following questions. Much of this information should already be available in the institution's **Record of Processing Activities**.

- What was the original source of the data? (e.g. collected by the institution itself, or provided by a third party. If the latter, which third party?)
- How was the data originally obtained? (e.g. from the student directly; from the student by observation, for example VLE or swipe card activity)
- For what purpose was the data originally collected? (e.g. to provide individual healthcare support, to provide individual tutorial support, to provide other individual support, for operational purposes, statistical purposes, or something else)
- Under what lawful basis was the data originally provided? (under Article 6 GDPR: necessary for performance of a contract with the individual, necessary to comply with a legal obligation, necessary to protect the vital interests of the individual, necessary for a public interest task (if so, what task), necessary for a legitimate interest of the institution or a third party (if so, what interest), consent; for Special Category Data an Article 9 condition will also be required)
- What was the individual told about how their data would be used?
- Is the new use for wellbeing and mental health compatible with the original purpose (see below)?

The institution should then document the following conclusions:

- Is a new privacy notice needed? If so, how will it be provided to individuals?
- Is new consent needed from individuals because of purpose incompatibility?
- Is new consent needed from individuals because the original legal basis was consent and the new purpose is not covered by that consent?

Purpose Compatibility/Fairness Considerations

According to Article 6(4) of the GDPR, the following considerations should be taken into account when assessing whether a new purpose is, or is not, **compatible with an existing one**:

- Any link between the purposes;
- The context of collection, in particular the relationship between the individual and the institution, and what the individual was told at the time of collection;
- The nature of the personal data, in particular whether it includes Special Category Data (covered additionally by Article 9), or criminal records data (covered by Article 10): any institution considering holding or processing these should take additional legal advice;
- The possible consequences (risks and benefits) of the new processing for individuals;
- The existence of appropriate safeguards (to protect the data, processing, and individuals).

A helpful rule-of-thumb, frequently cited by regulators, is that if individuals would be surprised by your new processing, then it is unlikely to be compatible. Purposes may also be incompatible if they are entirely unrelated, or the new purpose introduces an unjustified impact.

Considering the legal bases for the new and existing purposes may also be relevant: if those are different then the purposes are likely to be incompatible. Note, however, that if the new purpose is required to comply with a clear legal obligation, then purpose compatibility is unlikely to be an issue: conversely if the existing purpose was a legal obligation and it is now proposed to use the data for some other purpose then compatibility issues are very likely to arise.

The key significance of purpose (in)compatibility is the effect on existing assessments and data that have already been collected or observed. The starting point is that using existing data for a compatible purpose is permitted: re-using it for an incompatible purpose is not.

If a new purpose is determined to be incompatible, you must first ensure that it satisfies all the Data Protection principles (see GDPR Article 5), in particular that it is fair and lawful; if so, you may then add the new purpose to the relevant privacy notice. If you want to use existing data for the new, incompatible, purpose, you must then obtain each individual's specific consent to the new purpose. Without such consent you can only apply the new purpose to new data, collected after the purpose was assessed against the principles and added to the relevant privacy notice.

Transparency Considerations

All new uses of personal data – even if they are compatible with the original purpose – must be transparent. This means that they should, as a minimum, be clearly described in a privacy notice. Where the institution collects data directly from the student this should be relatively straightforward: the existing privacy notice at point of collection can be updated and, if appropriate, this change highlighted to students. Where information is collected by a third party, the institution may be able to agree with that third party to update its privacy notice to cover the new processing, in accordance with Article 13. If this is not possible then Article 14 requires the institution to provide its own, additional, privacy notice; this must be done at the latest within one month of receiving the personal data, but earlier if the information is being used to communicate with the individual or is being disclosed to another recipient.

Where information is collected by observation (for example records of use of swipe cards or virtual learning environments) the same transparency information must be communicated to students, but this may be more challenging as there may be no obvious transaction (for example typing the information into a form) during which a privacy notice can be displayed.

Note the ICO's comment that a privacy notice – no matter how well communicated – "cannot make fundamentally unfair processing fair and lawful".

To help gather this information, and document the conclusions on compatibility and transparency, a worksheet such as the following may be useful. Once this has been done, the new processing should

be added to the organisation's overall Record of Processing Activities, which will include most of this information. Note that although this example worksheet mentions a large number of particular data sources these, and the respective answers to the questions, are purely for illustrative purposes. Individual universities and colleges may be considering fewer, different, data sources and the answers they find, even if they do choose some of the same sources, may be different.

Data Description				Record of Compatibility Assessment							
Ref.	Data Source	Data attributes/ categories	Collection method	Original purpose	Lawful basis	Privacy notice?	New purpose	New lawful basis	New Privacy Notice?	Notice Provider	Re-consent needed?
1	Health questionnaire	Existing conditions	Direct	Health/ wellbeing support	Public task (duty of care)	<link>	Health/ wellbeing support	Public task (protecting mental health)	Yes	Institution	No
2	Use of NHS services	Clinic etc attendance	From NHS/GP through ISA	Health/ wellbeing support	Public task (statutory duty)	<link>	Health/ wellbeing support	Public task (protecting mental health)	Yes	??	??
3	Engagement	VLE use	Observed from institution systems	Individual tutorial support	Necessary for contract	<link>	Health/ wellbeing support	Public task (protecting mental health)	Yes	Institution	??
4	Student loan service	Payment problems	From Student Loan Company	Financial support	SLC-student contract	<link>	Health/ wellbeing support	Public task (protecting mental health)	Yes	??	??
5	Residences/ campus activity	Access card use	Either internal or 3rd party provider	Security/ safety	Legitimate interest or Contract	<link>	Health/ wellbeing support	Public task (protecting mental health)	Yes	??	??
6	Student background	E.g. family educational experience	Direct via UCAS	Statistical reporting	Consent/ legal obligation	<link>	Health/ wellbeing support	Public task (protecting mental health)	Yes	??	Yes

Purpose/Transparency Heatmap

To give a visual indication of how challenging it is likely to be to incorporate particular data sources into a wellbeing/mental health analytics programme, presenting key data from the preceding worksheet in the form of a heatmap may be helpful. Again, note that although data sources are mentioned in this table they, and the respective answers to the questions, are purely for illustrative purposes. Individual universities and colleges may be considering different data sources and the answers they find, even if they do choose some of the same sources, may be different.

Rows in the table indicate the current purpose for which the university or college (or the third-party organisation that collects the data) holds the data that the institution wishes to reuse for a wellbeing/mental health purpose. Sources nearer the top of the table are more likely to satisfy the Data Protection requirement of Purpose Compatibility:

- **Individual health/wellbeing support** covers data already used for providing health/wellbeing support to the individual (e.g. health centre records);
- **Individual tutorial support** covers data already used for providing tutorial support to the individual (e.g. VLE use);
- **Other individual support** covers data already used for providing support of other kinds to individuals (e.g. finance);
- **Operational purposes** covers data used for purposes other than student support (e.g. access card logs for building security);
- **Statistical purposes** covers data collected for statistical and reporting purposes (e.g. HESA).

Columns in the table indicate how data are collected and by which organisation. This is relevant to the difficulty of providing the notice and/or consent processes that will be required for both compatible and incompatible processing. Their sequence from left to right reflects the most common situation where data collected directly from the individual will normally involve transactions where an amended privacy notice can be displayed; information observed by the institution will be harder to clearly link to a privacy notice, but the institution is still in full control of that process; information obtained from a third party may be most challenging as it is likely to involve working with, and relying on, that third party. The ordering of the second and third columns, in particular, is not a hard and fast rule: some partner organisations may have sufficiently close links that updating their privacy notices is straightforward; in other cases the institution may find it no harder to provide an Article 14 (“information received from third party”) privacy notice than one relating to information it observes itself.

- **Institution (direct)** covers data that are collected direct from the student by the university/college, which controls (and can presumably update) the privacy information provided;
- **Institution (indirect)** covers data that are observed about the student by the university/college, so it may be harder to provide an adequate link between this collection and the privacy information;
- **Third Party** covers data that are collected by another organisation, where the university/college may find it difficult to update or guarantee the privacy information provided.

As the shading indicates, sources nearer the top left of the matrix are likely to be legally simpler to re-use for wellbeing or mental purposes as the institution should be able to communicate this new use to students, and the increased likelihood of compatibility between existing and new purposes is likely to place a lower burden on the content and form of that communication. Conversely, sources towards the bottom right are likely to involve much higher requirements: potentially including re-assessing their compliance with the Data Protection Principles, obtaining individuals’ consent to the reuse of data, and updating communications, which may need a new agreement with the third party to achieve.

Note that in this heatmap, font has been used to record two additional features of each data source:

1. Sources in normal/roman font may contain factors affecting the likelihood of wellbeing issues arising (“environmental stresses”);
2. Sources in *italic* font are observations that may indicate that wellbeing issues are occurring (“behavioural indicators”);
3. Sources in **bold** font are those likely to contain Special Category Data as defined in the GDPR;

		Notifiability: Who controls the data collection and privacy notice?		
		Institution (direct collection)	**Institution (indirect collection)**	**Third party/none**
Purpose Compatibility: Why do we currently have the data?	**Individual health/wellbeing support**	**Pre-enrolment health questionnaire** • Obtained from: student, before arrival • How obtained: direct • Purpose declared: health/wellbeing support		***Use of NHS services*** • Obtained from: NHS, GP • How obtained: ?? • Purpose declared: health/wellbeing support
	Individual tutorial support		*VLE engagement* • Obtained from: institution systems • How obtained: observed • Purpose declared: tutorial support	
	Other individual support			Student loan (non-)payment notification • Obtained from: Student Loan Company • How obtained: ?? • Purpose declared: validation of loan payment
	Operational purposes		*Residences/campus activity data (e.g. access card use)* • Obtained from: institution systems • How obtained: observed • Purpose declared: security/safety	*Residences (private) activity data (e.g. access card use)* • Obtained from: residence systems • How obtained: observed • Purpose declared: security/safety
	Statistical purposes	**Student record (religion, race, sexuality)** • Obtained from: student • How obtained: direct • Purpose declared: statistical reporting (e.g. equality)		Relevant background (family occupation, experience of tertiary education, etc.) • Obtained from: UCAS • How obtained: direct • Purpose declared: statistical reporting (e.g. widening access)