Appropriate policy document for the processing of special categories of personal data and personal data about criminal convictions and offences.
Articles 9 and 10 of the General Data Protection Regulation, Schedule 1 to the Data Protection Act 2018

Introduction

This is the 'appropriate policy document' for University of Nottingham that sets out how the University will protect special category and criminal convictions personal data.

It meets the requirement at paragraph 1 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.

It also meets the requirement at paragraph 5 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018.

This policy supplements the University's Records of Processing Activity (Article 30 GDPR) and outlines occasions where special category personal data or personal data about (alleged or actual) criminal convictions and offences is processed under certain conditions permitted by sections 10-11 of the DPA 2018 and set out in Parts 2-3 of Schedule 1 to the Act, as required under Part 4 of that Schedule.
It outlines the nature of the processing in each case and then summarises why any such processing fulfils the principles in Article 5 of the GDPR as well as explaining relevant retention and erasure policies.

Relevant processing conditions from Schedule 1 of the Data Protection Act 2018 requiring a policy document

Condition 1 – Employment, social security and social protection

This condition applies to special category personal data collected or used for the purposes of complying with employment, social security or social protection laws.
As an employer there are various laws relating to employment and social protection that must be complied with, for instance, laws relating to parental leave, adoption leave, statutory leave, maternity pay, sick pay, unfair dismissal and laws promoting equality and diversity and preventing discrimination and harassment.
Special category personal data under this condition shall only be used for the purposes of complying with legal obligations relating to employment or social protection laws.

Condition 6 – Statutory or government purposes
Special category personal data may be processed where it is in the substantial public interest to do so in order to comply with a legal obligation.
The University is subject to a variety of legal obligations which may require it to process or disclose sensitive personal data to Government or statutory bodies such as the Department for Education, the Charity Commission, Office for Students, the ICO, etc.

Condition 7 – Administration of Justice
Special category personal data or criminal conviction data may be processed for the purposes of the administration of justice.
The use of special category data may be required for the purposes of complying legal proceedings or pursuing remedies.

Condition 8 – Equality of opportunity or treatment.
Most special category personal data used for equal opportunities monitoring purposes is collected under our legal obligation to comply with Equality and Diversity legislation.
Where the provision of special category personal data about racial/ethnic origin, religious beliefs, health (i.e. disability status) or sexual orientation is mandatory and is in the substantial public interest, it is processed under that condition, is kept separate from other personal data, and is solely used for this limited purpose.

Ethnicity data collected under this condition for attendees at outreach and widening participation events/programmes aimed at prospective undergraduate applicants is not kept separate from other personal data so as to enable the long-term tracking and monitoring of the success of those initiatives.

Condition 10 – Preventing or detecting unlawful acts.
This condition applies to personal data about criminal convictions and offences used:

(i) During due diligence screening of prospective major donations, to ensure that the University does not unlawfully collect the proceeds of crime (see also Paragraph 14 – Preventing fraud and Paragraph 15 – Suspicion of terrorist financing or money laundering, either or both of which may on occasion become relevant). Any personal data about criminal convictions and offences used for such purposes is gathered from reputable public sources.

(ii) During the collection of declarations of relevant unspent criminal convictions/criminal records checks by student/job applicants where answers to those questions are mandatory
(see also Paragraph 11 – Protecting the public against dishonesty etc. and Paragraph 12 – Regulatory requirements relating to unlawful acts 2 and dishonesty etc.).

(iii) During the collection of declarations of relevant unspent criminal convictions in the course of recruitment exercises where answers to those questions are mandatory (see also Condition 18 – Safeguarding of children and of individuals at risk which is also relevant). Criminal conviction information is sought by the University on the ground of a reasonable concern that applicants who are as yet

un-rehabilitated may repeat the conduct that gave rise to the unspent conviction. The information is sought to prevent harm occurring to other staff and students.

Any data is used solely for the purposes of safeguarding and protecting the University community, is kept separate from other personal data, and is handled in accordance with strict DBS and security check standards. By virtue of Paragraph 36 of Schedule 1 to the DPA Act 2018, it is not necessary to demonstrate a substantial public interest in the above processing.
This condition also applies to special category personal data (e.g. about religious beliefs or political opinions) and/or personal data about criminal convictions and offences used without explicit consent in connection with the University's obligations under the Prevent duty. Although much data processing surrounding Prevent matters is based on the consent of the individual, on occasion (especially during initial conversations about concerns) there may be a need to process such data in order to meet the substantial public interest in preventing people from being drawn into radicalisation or terrorism.
Any personal data processed under this condition is handled very carefully on a strict need-to-know basis both within and, on occasion, beyond the University (e.g. disclosures to the OfS Prevent Lead or the police) in accordance with Government and OfS guidance.

Condition 11 – Protecting the public against dishonesty etc.
This condition applies to special category personal data or personal data about criminal convictions and offences collected or used under fitness to practice procedures for students on professional courses (e.g. medicine). The processing of such data is in the substantial public interest in ensure the safety of the public with regard to students working towards becoming part of these regulated professions.

Any personal data processed under this condition is kept separate from other personal data, and is solely used for this limited purpose in accordance with strict protocols that are aligned to normal standards and industry-level guidance (e.g. of the General Medical Council) in this professional area.

Condition 17 – Counselling etc.
Most special category personal data or personal data about criminal convictions and offences used during student/staff counselling or other student/staff welfare support services is collected with the explicit consent of the data subject (in some cases through the provision of options such as 'Prefer not to say' on relevant data collection forms).

Where the collection or use of special category personal data in a counselling/welfare context is not carried out with explicit consent, it would only be because a substantial public interest has been identified and is being acted upon (e.g. to prevent harm arising to the data subject or others by a disclosure to another part of the University.)
Where the collection or use of personal data about criminal convictions and offences in a counselling/welfare context is not carried out with explicit consent, it would only be because an urgent need had been identified for the data to be disclosed (e.g. to the police, to prevent or detect crime – see Paragraph 10 above).

Condition 18 – Safeguarding of children and of individuals at risk.
This condition applies to personal data about criminal convictions and offences collected in connection with the delivery of residential events to prospective undergraduate applicants,

some of whom are aged under 18, and solely in relation to a mandatory question on the registration forms for such events asking attendees to declare any relevant unspent criminal convictions. These data are used solely for safeguarding purposes and to ensure that these events can be run in a safe manner for all attendees.

This condition applies to the collection of declarations of relevant unspent criminal convictions in the course of recruitment exercises where answers to those questions are mandatory (see also Condition 10 – Preventing or detecting unlawful acts which is also relevant). This data is used to assess the suitability of candidates for the post; including, assessing the existence and magnitude of any risk of harm that may be posed by the applicant to vulnerable students with whom they will inevitably have close contact.

By virtue of Paragraph 36 of Schedule 1 to the Data Protection Act 2018, it is not necessary to demonstrate a substantial public interest in such processing.
This condition also applies to the processing of special categories of personal data which may relate to individuals that pose a safeguarding risk to the interests of children or other individuals at risk. This personal data may be processed by the University for safeguarding those at risk at the University or, where it is appropriate to do so, passed to third parties for their own safeguarding purposes. Such personal data shall only be processed to the extent that it is necessary for the purpose of the legitimate interests of the University or, if applicable, the third party concerned.

Procedures for securing compliance
Article 5 of the General Data Protection Regulation set out the relevant data protection principles which are summarised below. These are our procedures for ensuring that we comply.

Principle 1
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The University will:

- ensure that personal data is only processed where a lawful basis applies, and where processing is otherwise lawful
- only process personal data fairly, and will ensure that data subjects are not misled about the purposes of any processing
- having regard for the purpose of the processing, ensure that data subjects receive relevant information so that any processing of personal data is transparent

Principle 2
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The University will:

- only collect personal data for specified, explicit and legitimate purposes, and, having regard for the purpose of the processing, we will inform data subjects what those purposes are in a privacy notice

- not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use personal data for a new purpose that is compatible, and having regard for the purpose of the processing, we will inform the data subject first.

Principle 3
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The University will only collect the minimum personal data that we need for the purpose for which it is collected. We will ensure that the data we collect is adequate and relevant.

Principle 4
Personal data shall be accurate and, where necessary, kept up to date.

The University will ensure that personal data is accurate, and kept up to date where necessary. We will take particular care to do this where our use of the personal data has a significant impact on individuals. Having regard for the purpose for which it is being processed, where personal data is found to be inaccurate it will be erased or rectified.

The University will maintain a records management policy.

Principle 5
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

The University will only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer need personal data it shall be deleted or rendered permanently anonymous.

Principle 6
Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The University will ensure that there appropriate organisational and technical measures in place to protect personal data.

The University will maintain an information security policy and data handling policy.

Accountability principle
The University shall be responsible for, and be able to demonstrate compliance with these principles.
The University will:

- ensure that records are kept of all personal data processing activities, and that these are provided to the Information Commissioner on request
- carry out a Data Protection Impact Assessment for any high risk personal data processing, and consult the Information Commissioner if appropriate

- ensure that a Data Protection Officer is appointed to provide independent advice and monitoring of the departments' personal data handling, and that this person has access to report to the highest management level of the department
- have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law.

3. Data controller's policies as regards retention and erasure of personal data

The University will ensure, where special category or criminal convictions personal data is processed or when sensitive processing is to take place, that:

- there is a record of that processing, and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data
- where we no longer require special category or criminal convictions personal data for the purpose for which it was collected, or when sensitive processing is no longer required, we will delete it, render it permanently anonymous or irretrievable
- having regard for the purpose of the processing, data subjects receive information about how their data will be handled, and that this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

The University will maintain a records retention and deletion policy

The University's data retention schedule sets out the retention period for basic types of records:

- https://www.nottingham.ac.uk/governance/records-and-information-management/records-management/retentionschedule.aspx