Appropriate Policy Document for the processing of special category and criminal offence data

This policy document explains the University's processing of special category data and criminal offence data. It demonstrates that the processing of special category and criminal offence data based on the Schedule 1 conditions in the Data Protection Act 2018 is compliant with the requirements of the United Kingdom General Data Protection Regulation (UK GDPR) Article 5 principles.

This policy satisfies the requirement of the Data Protection Act 2018 (DPA 18), Schedule 1, Part 4 which requires the University as the 'data controller' of the personal data to have an 'Appropriate Policy Document' (APD) in place when processing special category and criminal offence data under certain specified conditions. In addition, it provides some further information about the processing of special category and criminal offence data where an Appropriate Policy Document (APD) isn't a specific requirement. The information supplements the University's privacy notices.

This Appropriate Policy Document includes sufficient information to enable individuals to understand how the University is processing these types of personal data and outline the University's retention policies with respect to special category and criminal offence data.

This Appropriate Policy Document complements the University's general record of processing under Article 30 of the UK GDPR. In accordance with the Data Protection Act 2018, the Appropriate Policy Document will be kept under review and must be retained for six months after the date the relevant processing stops. A copy must be provided to the Information Commissioner free of charge on request.

1. Description of data processed

As part of the University's statutory and educational functions, it processes special category and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation (EU GDPR) and of the United Kingdom General Data Protection Regulation (UK GDPR) and Schedule 1 of the Data Protection Act 2018 (DPA 18).

Special category data is personal data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purposes of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation.

Processing of special category data is strictly prohibited under EU and UK GDPR unless an exemption in Article 9 applies.

Criminal offence data is covered by Article 10 of the EU and UK GDPR. In addition, section 11(2) of the DPA 18 specifically confirms that this includes personal data relating to the alleged commission of

offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

The University relies on various lawful bases under Article 6 including public task for the processing connected with its educational and public interest research activities, legal obligation for processing required by law and as connected with the performance of its contractual obligations to students. Occasionally where it is in the University or a third party (such as the Police or insurer's legitimate interests) which are not outweighed by the fundamental rights and freedoms of individuals.

The University processes special category data under the following EU and UK GDPR Articles:

Article 9(2)(b) - where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the University or the data subject in connection with employment, social security or social protection.
Examples of our processing within this exemption include:

- as an employer managing staff absence records, contractual sick leave entitlement and administering related payments, determining whether any adjustments are necessary to enable staff to carry out their role
- checking applicants' and employees' right to work in the UK
- student and graduate health and disability data relating to physical or mental health or a specific learning disability to offer individuals tailored support when accessing the careers and employability service.

Article 9(2)(f) – for the establishment, exercise or defence of legal claims.
Examples of our processing within this exemption include:

- processing staff information relating to any employment tribunal or other litigation, for example when responding to and investigating engagement and industrial relations matters where permitted by applicable law, including criminal investigations or other associated activities.

Article 9(2)(g) – reasons of substantial public interest
As a higher education institution and public authority, the University is required to process requests made under legislation such as the Equality Act 2010 (statutory requirements, equality monitoring). It also processes personal data for other public interest reasons where necessary, such as for the prevention and detection of crime, for safeguarding reasons or for insurance purposes.
Examples of our processing within this exemption include:

- delivery of student support and wellbeing service (specialist report & support) to provide counselling
- managing and administering our equal opportunities reporting in relation to staff
- complying with our statutory requirements
- processing data (such as CCTV footage) in order to prevent or detect unlawful acts.

Article 9(2)(h) – processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee (when processed by or under the responsibility of a professional subject to the obligation of professional secrecy in law or under rules established by national competent bodies).
Examples of our processing within this exemption include:

- data processing carried out by the Occupational Health team.

Article 9(2)(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) (as supplemented by section 19 of the DPA 18 which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interest of the data subject).

Examples of our processing within this exemption include:

- our HEAT research facilitating service (in collaboration with other organisations) to monitor and evaluate activities delivered by members to examine whether outreach is effective
- health and social care research in the public interest.

Article 9(2)(c) – processing is necessary to protect the vital interests of the data subject

Examples of our processing within this exemption include:

- providing the emergency services with information about a member of staff or student in a medical emergency
- use of CCTV footage (in an emergency where someone's life may be in danger).

Article 9(2)(a) – explicit consent

In circumstances where we seek consent, we make sure it is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

Examples of our processing within this exemption include:

- facilitating administration of any staff subscriptions, initiatives or plans in connection with staff engagement with the University
- processing dietary/health needs for course participation.

Article 10 – criminal offence data

Examples of our processing under Article 10 include:

- pre-employment checks and declarations in line with contractual obligations
- delivering specialist support and ensuring safety and well-being of students and others and/or conducting internal investigation/disciplinary hearings as part of the report & support well-being service to prevent and detect unlawful acts and for equality of opportunity.

Categories of special category and criminal offence data processed:

For **academic appeals**:

- any special category data contained in an Individual Learning Plan (ILP) as may be relevant to any appeal
- any student sponsorship race or ethnicity information shared with the immigration compliance team to ensure compliance with UK immigration law.

For **student administration:**

- ethnic group
- medical information (OH) and special educational needs provision information
- safeguarding data (including criminal offence data).

For **student applications**:

- personal background information collected during the admissions process, such as demographic information
- information collected on admission for compliance monitoring under the Equality Act 2010
- health information for the purposes of implementing reasonable adjustments to support studies, ensure health and safety, organise placements or for extenuating circumstances.

- data relating to DBS/fitness to practice (for relevant degree programmes).

For the **careers and employability service**:

- ethnicity
- health and disability data relating to physical or mental health or a specific learning difficulty is held e.g. for a particular scheme or initiative.

For **student enrolment:**

- special category or criminal offence data as may be necessary for regulatory responses and statutory requirements (for example submission of data to the Higher Education statistics Agency (HESA, part of JISC)).

For the **Gulbenkian Theatre**

- dietary/health requirements for courses.

For the **HEAT service**:

- disability, ethnicity, gender identity, religion, sex (for equalities monitoring).

For **HR** purposes:

- racial or ethnic origin (including nationality and visa information)
- religious and philosophical beliefs
- trade union membership
- data concerning physical and/or mental health (including OH requirements, accident reports, day-to-day health concerns, dietary requirements, allergies and reasons for absence)
- sexual orientation
- health and safety and accident records and reports
- information relating to actual or suspected criminal convictions and offences.

For **immigration**:

- nationality/ethnicity information
- medical information relating to prolonged absence.

For the **Kent and Medway Medical School**

- equal opportunities and health data for monitoring or to provide specific support or reasonable adjustments.

For the **report and support** service:

- sex life, age, disability, race, religion or belief, sexual orientation, health data
- criminal offence data.

For research purposes

- relevant medical information (for research in the public interest) and following the UK policy framework for health and social care research
- protected characteristics (such as ethnic group).

For the **student support and wellbeing** service:

- disability, medical condition, mental health difficulty, specific learning disability to create an Individual Learning Plan (ILP) and to deliver support and wellbeing services.

For the Templeman Library Card:
disability, ethnicity for equality assessments and improvements.

2. Schedule 1 condition for processing

Data Protection Act Schedule 1 Part 1:

Section 1: Employment, social security & social protection - *This condition is met if (a) the processing is necessary for performing or exercising obligations or rights which are imposed or conferred by law in connection with employment, social security or social protection) and (b) when the processing is carried out the data controller has an appropriate policy document (this document) in place.*

- for the purposes of carrying out our obligations as an employer in connection with rights under employment law, social security law or the law relating to social protection (including information about health, wellbeing, ethnicity, photographs and their membership of any trade union). It also includes our health and safety responsibilities as well as other employment rights and obligations
- processing data relating to criminal convictions under Article 10 UK GDPR in connection with our rights under employment law in connection with recruitment, discipline or dismissal
- any processing necessary for tax, revenue and benefits or social protection purposes.

Section 2: Health or social care purposes - *This condition is met if the processing is necessary for health or social care purposes. 'Health or social care purposes' means the purposes of (a) preventative or occupational medicine (b) the assessment of the working capacity of an employee (c) medical diagnosis (d) the provision of health care or treatment (e) the provision of social care, or (f) the management of health care systems or services or social care systems or services.*

- for the purposes of assessing the working capacity of our employees so that we can safeguard their welfare and provide any adjustment necessary for staff and implement any changes advised by our OH provider.

Section 4: Research etc. - *This condition is met if the processing (a) is necessary for archiving purposes, scientific or historical research purposes or statistical purposes, (b) is carried out in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19) and (c) is in the public interest.*

- for research purposes in the public interest (NB for information only as APD not required for this condition).

Data Protection Act Schedule 1 Part 2: Substantial public interest conditions.
Section 6: Statutory purposes - *(1) This condition is met if the processing (a) is necessary for a purpose listed in sub-paragraph (2), and (b) is necessary for reasons of substantial public interest.*
(2)Those purposes are (a) the exercise of a function conferred on a person by an enactment or rule of law; (b) the exercise of a function of the Crown, a Minister of the Crown or a government department.

- for the purposes of carrying out our statutory obligations as a Higher Education Institution and public authority
- for the purposes of complying with the Equality Act 2010 where reasonable adjustments are required.

Section 8: Equality of opportunity or treatment - *(1) This condition is met if the processing (a) is of a specified category of personal data, and (b) is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained, subject to the exceptions in sub-paragraphs (3) to (5).*

(2) In sub-paragraph (1), "specified" means specified in the following table

Category of personal data	*Groups of people (in relation to category of personal data)*
Personal data revealing racial or ethnic origin	*People of different racial or ethnic origins*
Personal data revealing religious or philosophical beliefs	*People holding different religious or philosophical beliefs*

Data concerning health	*People with different states of physical or mental health*
Personal data concerning an individual's sexual orientation	*People of different sexual orientation*

(3) Processing does not meet the condition in sub-paragraph (1) if it is carried out for the purposes of measures or decisions with respect to a particular data subject.
(4) Processing does not meet the condition in sub-paragraph (1) if it is likely to cause substantial damage or substantial distress to an individual.
(5) Processing does not meet the condition in sub-paragraph (1) if (a) an individual who is the data subject (or one of the data subjects) has given notice in writing to the controller requiring the controller not to process personal data in respect of which the individual is the data subject (and has not given notice in writing withdrawing that requirement), (b) the notice gave the controller a reasonable period in which to stop processing such data, and (c) that period has ended.

- processing necessary to ensure the University meets its monitoring, maintaining and promoting equality duties under the Equality Act 2010
- ensuring equal access to services.

Section 9: Racial and ethnic diversity at senior levels of organisations - *(1) This condition is met if the processing (a) is of personal data revealing racial or ethnic origin, (b) is carried out as part of a process of identifying suitable individuals to hold senior positions in a particular organisation, a type of organisation or organisations generally, (c) is necessary for the purposes of promoting or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in the organisation or organisations, and (d) can reasonably be carried out without the consent of the data subject, subject to the exception in sub-paragraph (3).*

(2) For the purposes of sub-paragraph (1)(d), processing can reasonably be carried out without the consent of the data subject only where (a) the controller cannot reasonably be expected to obtain the consent of the data subject, and (b) the controller is not aware of the data subject withholding consent.

(3) Processing does not meet the condition in sub-paragraph (1) if it is likely to cause substantial damage or substantial distress to an individual.

(4) For the purposes of this paragraph, an individual holds a senior position in an organisation if the individual (a) holds a position listed in sub-paragraph (5), or (b) does not hold such a position but is a senior manager of the organisation.

(5) Those positions are (a) a director, secretary or other similar officer of a body corporate; (b) a member of a limited liability partnership; (c) a partner in a partnership within the Partnership Act 1890, a limited partnership registered under the Limited Partnerships Act 1907 or an entity of a similar character formed under the law of a country or territory outside the United Kingdom.

(6) In this paragraph, "senior manager", in relation to an organisation, means a person who plays a significant role in (a) the making of decisions about how the whole or a substantial part of the organisation's activities are to be managed or organised, or (b) the actual managing or organising of the whole or a substantial part of those activities.

(7) The reference in sub-paragraph (2)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

- applies only to the processing necessary to identify suitable individuals to hold senior positions within the University for substantial public interest reasons.

Section 10: Preventing or detecting unlawful acts - *(1) This condition is met if the processing (a) is necessary for the purposes of the prevention or detection of an unlawful act, (b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and (c) is necessary for reasons of substantial public interest.*

(2) If the processing consists of the disclosure of personal data to a competent authority, or is carried out in preparation for such disclosure, the condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place.

(3) In this paragraph "act" includes a failure to act; "competent authority" has the same meaning as in Part 3 of this Act.

(NB a 'competent authority' is defined as a person who has a law enforcement function set out in law or as identified in Schedule 7of the DPA 18 such as the Police, Serious Fraud Office, Competitions and Markets Authority etc)

- processing special category or criminal offence data in connection with employment, admissions or complaints processes
- processing CCTV footage.

Section 11: Protecting the public against dishonesty - *(1) This condition is met if the processing (a) is necessary for the exercise of a protective function, (b) must be carried out without the consent of the data subject so as not to prejudice the exercise of that function, and (c) is necessary for reasons of substantial public interest.*

(2) In this paragraph, "protective function" means a function which is intended to protect members of the public against (a) dishonesty, malpractice or other seriously improper conduct, (b) unfitness or incompetence, (c) mismanagement in the administration of a body or association, or (d) failures in services provided by a body or association.

Section 12: Regulatory requirements relating to unlawful acts and dishonesty etc - *(1)This condition is met if (a) the processing is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has—(i) committed an unlawful act, or (ii) been involved in dishonesty, malpractice or other seriously improper conduct,(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing, and (c) the processing is necessary for reasons of substantial public interest.*

(2) In this paragraph "act" includes a failure to act; "regulatory requirement" means (a) a requirement imposed by legislation or by a person in exercise of a function conferred by legislation, or (b) a requirement forming part of generally accepted principles of good practice relating to a type of body or an activity.

- carrying out investigations and disciplinary actions relating to employees

- processing data concerning dishonesty, malpractice, unfitness or other improper conduct in order to protect the University community
- processing information in order to comply with legislation including the sanctions regime.

Section 14: Preventing fraud - *(1)This condition is met if the processing (a) is necessary for the purposes of preventing fraud or a particular kind of fraud, and (b) consists of (i) the disclosure of personal data by a person as a member of an anti-fraud organisation, (ii) the disclosure of personal data in accordance with arrangements made by an anti-fraud organisation, or (iii) the processing of personal data disclosed as described in sub-paragraph (i) or (ii).*

(2) In this paragraph, "anti-fraud organisation" has the same meaning as in section 68 of the Serious Crime Act 2007.

(NB an 'anti-fraud organisation' means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has these functions as its purpose or one of its purposes)

- processing necessary for the purposes of preventing fraud.

Section 15: Suspicion of terrorist financing or money laundering - *This condition is met if the processing is necessary for the purposes of making a disclosure in good faith under either of the following (a) section 21CA of the Terrorism Act 2000 (disclosures between certain entities within regulated sector in relation to suspicion of commission of terrorist financing offence or for purposes of identifying terrorist property); (b) section 339ZB of the Proceeds of Crime Act 2002 (disclosures within regulated sector in relation to suspicion of money laundering).*

- processing necessary for the purposes of preventing money laundering or terrorist financing.

Section 17: Counselling - *(1) This condition is met if the processing—(a) is necessary for the provision of confidential counselling, advice or support or of another similar service provided confidentially,(b) is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and (c) is necessary for reasons of substantial public interest.*

(2) The reasons mentioned in sub-paragraph (1)(b) are (a) in the circumstances, consent to the processing cannot be given by the data subject; (b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing; (c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the service mentioned in sub-paragraph (1)(a).

- for the provision of counselling, advice or similar confidential advice service for staff and students.

Section 18: Safeguarding of children and individuals at risk - *(1) This condition is met if (a) the processing is necessary for the purposes of (i) protecting an individual from neglect or physical, mental or emotional harm, or (ii) protecting the physical, mental or emotional well-being of an individual, (b)the individual is (i) aged under 18, or (ii) aged 18 or over and at risk, (c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and (d) the processing is necessary for reasons of substantial public interest.*

(2) The reasons mentioned in sub-paragraph (1)(c) are (a) in the circumstances, consent to the processing cannot be given by the data subject; (b) in the circumstances, the controller cannot reasonably be

expected to obtain the consent of the data subject to the processing; (c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual (a) has needs for care and support, (b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and (c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

- protecting vulnerable children and/or individuals aged over 18 and at risk from neglect, physical, mental or emotional harm (where consent cannot be given by the individual and/or the University cannot reasonably be expected to obtain the consent of the data subject or because obtaining consent would prejudice the provision of the protection).
- meeting our safeguarding responsibilities.

Section 19: Safeguarding of economic well-being of certain individuals - (*1) This condition is met if the processing (a) is necessary for the purposes of protecting the economic well-being of an individual at economic risk who is aged 18 or over, (b) is of data concerning health, (c) is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and (d) is necessary for reasons of substantial public interest.*

(2) The reasons mentioned in sub-paragraph (1)(c) are (a) in the circumstances, consent to the processing cannot be given by the data subject; (b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing; (c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) In this paragraph, "individual at economic risk" means an individual who is less able to protect his or her economic well-being by reason of physical or mental injury, illness or disability.

- protecting the economic wellbeing of an individual at economic risk who is aged 18 or over.

Section 20: Insurance - *(1) This condition is met if the processing (a) is necessary for an insurance purpose, (b) is of personal data revealing racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health, and (c) is necessary for reasons of substantial public interest, subject to sub-paragraphs (2) and (3).*

(2) Sub-paragraph (3) applies where (a) the processing is not carried out for the purposes of measures or decisions with respect to the data subject, and (b) the data subject does not have and is not expected to acquire (i) rights against, or obligations in relation to, a person who is an insured person under an insurance contract to which the insurance purpose mentioned in sub-paragraph (1)(a) relates, or (ii) other rights or obligations in connection with such a contract.

(3) Where this sub-paragraph applies, the processing does not meet the condition in sub-paragraph (1) unless, in addition to meeting the requirements in that sub-paragraph, it can reasonably be carried out without the consent of the data subject.

(4) For the purposes of sub-paragraph (3), processing can reasonably be carried out without the consent of the data subject only where (a) the controller cannot reasonably be expected to obtain the consent of the data subject, and (b) the controller is not aware of the data subject withholding consent.

(5) In this paragraph "insurance contract" means a contract of general insurance or long-term insurance; "insurance purpose" means (a) advising on, arranging, underwriting or administering an insurance contract, (b) administering a claim under an insurance contract, or (c) exercising a right, or complying with an obligation, arising in connection with an insurance contract, including a right or obligation arising under an enactment or rule of law.

(6) The reference in sub-paragraph (4)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

(7) Terms used in the definition of "insurance contract" in sub-paragraph (5) and also in an order made under section 22 of the Financial Services and Markets Act 2000 (regulated activities) have the same meaning in that definition as they have in that order.

- claims for loss or damage to university property
- claims for compensation made against the University by third parties.

Data Protection Act Schedule 1 Part 3 Additional conditions relating to criminal convictions etc.

Section 29: Consent - *This condition is met if the data subject has given consent to the processing.*

Section 30: Vital interests - *This condition is met if (a) the processing is necessary to protect the vital interests of an individual, and (b) the data subject is physically or legally incapable of giving consent.*

Section 33: Legal claims - *This condition is met if the processing (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), (b) is necessary for the purpose of obtaining legal advice, or (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.*

- if it is necessary for the purposes of or in connection with legal proceedings, to obtain legal advice or otherwise necessary to establish, exercise or defend legal rights.

Section 36: Extension of conditions in Part 2 referring to substantial public interest - *This condition is met if the processing would meet a condition in Part 2 of this Schedule but for an express requirement for the processing to be necessary for reasons of substantial public interest.*

- see above under Schedule 1 Part 2, for example: Section 1 – employment social security & social protection, Section 6 – statutory etc purposes, Section 10 - preventing or detecting unlawful acts.

Section 37: Extension of insurance conditions - *This condition is met if the processing (a) would meet the condition in paragraph 20 in Part 2 of this Schedule (the "insurance condition"), or (b) would meet the condition in paragraph 36 by virtue of the insurance condition, but for the requirement for the processing to be processing of a category of personal data specified in paragraph 20(1)(b).*

- see above under section 20 insurance.

3. Procedures for ensuring compliance with the principles

Accountability principle
We maintain appropriate documentation of our processing activities and have data protection, data subject rights and data breach policies in place. We regularly review our compliance using the ICO's Accountability Tracker and regularly undertake data protection audits.

We take a data protection by design and default approach to our activities. We carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests. This requirement is included in the Data Protection Policy.

We maintain logs of information security incidents, requests from students, staff and other individuals exercising their data protection rights.

We keep records of the mandatory data protection and information security training for all staff.
We maintain a Record of our Processing activities (ROPA) in the form of our Information Asset Registers (IARs).

We ensure that the University has written contract terms in place with data processors.

We employ a designated Data Protection Officer with expert knowledge of data protection law and practices. We review the ICO's general checklist for accountability and governance.

Principle (a): lawfulness, fairness and transparency

As a public authority we are bound by numerous statutes. Our functions are set out in Education Acts. We process special category/criminal offence data to comply with our obligations imposed by statute.

We ensure that:

- personal data is only processed where a lawful basis applies - this is stated in our data protection policy

- data subjects are provided with clear and transparent information about why we process their personal data in our privacy notices and this policy document. Our data protection policy requires that privacy notices are provided to data subjects on collecting the information and also made available on our webpages and on our intranet (for staff). We provide supporting guidance to assist staff with the mandatory elements of a privacy notice.

We are open and honest when we collect the special category or criminal offence data and ensure we do not deceive or mislead people about its use. Our privacy notices can be found on our website. We review the ICO's checklist for lawfulness, fairness and transparency.

Principle (b): purpose limitation
We process special category and criminal offence data to fulfil our statutory obligations in accordance with relevant legislation.

We ensure that we have:

- clearly identified our defined purpose(s) for using and processing the special category and criminal offence data as required by our data protection policy
- included appropriate details of these purposes in our privacy information for individuals
- where we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), we check that this is compatible with our original purpose or get specific consent for the new purpose. These principles are enshrined in our data protection policy
- if we are sharing data with another controller, we document their lawful basis for their purpose
- we do not process personal data for purposes incompatible with the original purpose it was collected for.

We review the ICO's checklist for purpose limitation.

Principle (c): data minimisation

We ensure that:

- we only collect special category and criminal offence personal data we actually need for our specified purposes as is sufficient to properly fulfil those purposes
- we do not collect excessive amounts of personal data; it is necessary and proportionate to the purpose stated in our privacy notice
- we periodically review this particular special category and criminal offence data and delete anything we don't need
- where information is provided to us but not relevant to our stated purposes, we erase it.

We refer to the ICO's general checklist for data minimisation.

Principle (d): accuracy

We ensure that:

- special category and criminal offence data we collect is accurate and kept up to date
- any data which is out of date is erased or updated without delay
- requests from individuals challenging accuracy are processed within the statutory timeframes
- we follow our Data Subjects' Rights policy and ensure that individuals' right to rectification is complied with
- we ensure lessons are learned when challenges to the accuracy of data are upheld.

We refer to the ICO's general checklist for accuracy.

Principle (e): storage limitation

The University ensures that:

- University special category and criminal offence data is retained in accordance with privacy notices and retention schedules unless we have identified the need to keep it for public interest archiving, scientific or historical research or statistical purposes
- retention periods are based on recommended retention periods for the sector, and/or in line with statutory requirements or business purposes.
- data is not kept for longer than necessary for the purposes for which it was collected and we regularly review our information and erase or anonymise this special category and criminal offence data when we no longer need it
- staff undertake mandatory data protection training which includes a section on records management including the disposal of records.

We refer to the ICO's general checklist for storage limitation.

Principle (f): integrity and confidentiality (security)

The University ensures that:

- all special category and criminal offence data is processed in a manner which ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- appropriate organisational (policies and standards) and technical (IS measures) are in place.
- data protection training is completed by all staff and refreshed every 2 years. This includes an Information Security section
- data protection and data breach policies are in place
- an information security policy and information technology management policy is in place
- all users abide by the IT regulations
- role-based access controls are in place
- laptops are encrypted.

We refer to the ICO's general checklist for security.

4. Retention and erasure policies

Special category and criminal offence data is held and destroyed in line with the University's retention schedules referenced in its records management policy.

We ensure that:

- Information Asset Registers are kept up to date and set out the ownership, governance and maintenance of the University's assets
- disposal of records is carried out securely
- retention periods are considered carefully and aligned with recommended sector standards provided by JISC or in line with legal or regulatory requirements
- where we no longer require special category and criminal offence data for the purpose for which it was collected, we delete it or make it permanently anonymous.

5. Appropriate Policy Document review date

This statutory Appropriate Policy Document (APD) has been based on the ICO Appropriate Policy Document and template and will be reviewed at least biennially by the Assurance and Data Protection team or more frequently if deemed necessary by the Data Protection Officer. It will be made available to the Information Commissioner free of charge in line with legal requirements in Schedule 1, Part 4 of the Data Protection Act 2018 and retained for at least 6 months after any relevant processing has ceased.

This policy will be reviewed at least biennially by the Data Protection Officer or an appropriately qualified member of the Assurance and Data Protection team.

Version	Author	Description of Change	Date
0.1	Assistant Director (Assurance)	Policy created	October 2022

0.2	Data Protection Officer	Amendments suggested for clarity including further definitions	October 2022
0.3	AD (Assurance)	Further additions following privacy notice reviews	April 2023

Version	Governing or Reviewing Body	Recommendations	Review/ Approval Date
1	EG		5 June 2023
1	Audit Committee		13 June 2023