Policy Name	**Data Protection Policy**
Subject	Information Compliance
Approving Authority	IMSSC and UEB
Accountable Person	Data Protection Officer
Responsible Team	Security and Information Compliance Team
First approved	April 2018
Last updated	February 2024
Version Number	Version 2

1. Introductory Purpose and Background

The University of Nottingham ('the University') is committed to protecting the rights, privacy and security of Personal Data relating to employees, students and other third parties in accordance with Data Protection Legislation.

The University is a Controller in respect of Personal Data and will determine how Personal Data is Processed.

This Policy promotes transparency, accountability and the safeguarding of individual's privacy rights and sets out the minimum standards which must be complied with by the University when Processing Personal Data. It outlines the University's responsibilities under Data Protection Legislation and applies to all Personal Data Processed by the University irrespective of the format or media on which that Personal Data is stored or who it relates to.

2. Scope

This Policy applies to all University of Nottingham UK employees (including PhD students who are also employed by the University), students and where appropriate third parties working for or on behalf of the University (such as honorary/associates, hourly paid lecturers). It is important that all employees and students ('you' / 'your') understand the scope of Data Protection Legislation. It is your responsibility to familarise yourself with this Policy which explains how you should carry out your role or research to ensure compliance with Data Protection Legislation.

Compliance with this Policy is mandatory and failure to comply with this Policy or its associated Policies and Procedures may result in disciplinary action. Non-

compliance with this Policy and related Policies/Procedures may also result in damage to the University's reputation, financial loss, and legal and regulatory non-compliance.

3. Definitions

Anonymised	The process of removing or altering certain identifying information from data in such a way that it can no longer be attributed to an individual directly or indirectly and ensures that the individual cannot be re-identified.
Consent	Agreement which must be freely given, specific and informed in terms of an indication of the Data Subject's wishes to Process Personal Data relating to them.
Controller	The organisation who determines when, why and how to Process Personal Data.
Data Protection Legislation	The UK GDPR and DPA 2018 as updated and re-enacted from time to time.
Data Subject	A living individual about whom we hold Personal Data.
DPA 2018	The UK Data Protection Act 2018 which supplements the UK GDPR.
DPIA	Data Protection Impact Assessment, which is an assessment used to identify and reduce risks of Processing and is carried out as part of Privacy by Design.
DPO	The Data Protection Officer appointed by the University and who is the University's main representative on data protection matters.
Lawful Basis	One of the lawful bases set out in UK GDPR Articles 6, 8 and 10, as relevant. This could be contract, legal obligation, protecting vital interests, task carried out in the public interest, a legitimate interest or the data subject has given their Consent. Processing of Personal Data will only be legal if it is necessary and there is a lawful basis for processing.
Personal Data	Information relating to a Data Subject, who can be identified directly or indirectly from that information. Personal Data can be factual (such as name, email address) or an opinion about that person's actions or behaviour.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

Privacy by Design	Implementation of appropriate technical and organisational measures in an effective manner to comply with the UK GDPR and safeguard individual rights.
Privacy Notices	Notices setting out information provided to Data Subjects when Personal Data is collected. These generally take the form of a notice to specific groups (such as employees, students, etc.).
Processing or Process	An activity that involves the use of Personal Data including the obtaining, recording or holding of that data or carrying out any operation or set of operations on that data which can include organising, amending, retrieving, using, disclosing, erasing or destroying it.
Pseudonymisation / Pseudonymised	Replacing information which directly or indirectly identifies an individual with one or more artificial identifiers so that person cannot be identified without additional information which is kept separately and secure.
Special Category Data	Personal Data relating to racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, genetic data, biometric data, physical and mental health data, or data concerning sex life or sexual orientation.
UK GDPR	Has the meaning given to it in Section 3(10) (as supplemented by section 205(4)) of the DPA 2018.
We	The University of Nottingham.

4. Policy

4.1 Key Principles

If you are Processing Personal Data on behalf of the University you must observe and comply with the six principles of the UK GDPR. Personal Data must be:

1. Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
2. Collected only for specified, explicit and legitimate purposes (Purpose Limitation);
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed (Data Minimisation);
4. Accurate and where necessary kept up to date (Accuracy);
5. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation);
6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accident loss, destruction or damage (Security, Integrity and Confidentiality).

Additionally, the University must ensure that Personal Data are not transferred outside the UK (and EEA) to another country without appropriate safeguards being put in place.

See Appendix I for a detailed description of the UK GDPR principles relating to Personal Data.

4.2 Key Roles and Responsibilities

4.2.1 The **University Executive Board (UEB)** has overall responsibility to ensure the University meets its legal and regulatory responsibilities under Data Protection legislation and to ensure compliance with this Policy. The Information **Management and Security Steering Committee (IMSSC)** is responsible for overseeing the maintenance, implementation, and performance of this Policy.

4.2.2 **Faculty Pro-Vice Chancellors, Directors of Professional Service Departments and Line Managers** are responsible for ensuring employees within their respective areas, including all new employees, are aware of this Policy and for ensuring that their employees undertake data protection training.

4.2.3 **All employees and research students who process Personal Data** are responsible for complying with Data Protection Legislation and attending data protection training as required.

4.2.4 The University has appointed a **Data Protection Officer (DPO)** to assist the University in the monitoring and compliance of its obligations under Data Protection Legislation. The University's DPO is Tracy Landon – Associate Director of Information Compliance and you can contact her directly or through DPO@nottingham.ac.uk.

4.2.5 The University is registered with the Information Commissioner's Office as a Controller – our registration number is: Z5654762.

4.2.6 **Accountability**

The Controller (the University) must demonstrate compliance with the data protection principles which means having adequate resources and controls in place including:

a. Appointing a suitably qualified and experienced DPO, providing them with adequate support and resource;
b. Integrating data protection into internal documentation such as this Policy and Privacy Notices;

c. Providing regular training on data protection and retaining a record of those employees who undertake that training;
d. Ensuring where Processing presents a high risk to the rights and freedom of Data Subjects, the University has carried out an assessment of those risks by undertaking a Data Protection Impact Assessment (DPIA) – *see paragraph 4.5.2 below*; and
e. Regularly testing measures implemented and conducting periodic reviews to assess compliance across the University.

4.3 Key considerations of this Policy

4.3.1 What is Personal Data and what do we mean by Processing Personal Data?

- Personal Data is any information about an individual from which that individual can be identified either directly or indirectly (such as name, identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the Data Subject as well as images, photographs, or films. It does not include Anonymised data.

- There are also Special Categories of Personal Data where additional safeguards apply, these include information revealing, racial or ethnic origin, religious or similar beliefs, physical/mental health conditions, sexual life/sexual orientation, biometric/genetic data, political opinions, trade union membership, and data relating to criminal offences/convictions. See Appendix II for further information.

- Data Protection Legislation applies to Processing Personal Data which is broad in its definition and includes anything that the University might do with the data such as obtaining, organising, structuring, recording, holding/storing, disclosing and destroying Personal Data.

4.3.2 Rights and Requests

The UK GDPR provides Data Subjects with several rights in relation to their Personal Data, these include:

- The right to withdraw their consent where the lawful basis relied upon is that of consent. This can be done at any time.
- The right to be informed – receive certain information about the Controller's processing activities which includes how we collect and Process Personal Data.
- The right of subject access – to request a copy of their Personal Data held by the University.
- The right to rectification of inaccurate Personal Data.

- The right to erasure (right to be forgotten) –deletion of Personal Data where it is no longer necessary for the purpose(s) for which they were collected.
- The right to restrict processing of Personal Data in specific circumstances, such as where the Data Subject believes the Personal Data to be inaccurate or the processing is unlawful.
- The right to data portability (in limited circumstances) by asking the University to transfer Personal Data to a third party.
- The right to object to the Processing of Personal Data where the lawful basis for Processing is the University's legitimate interests.
- The right to object to direct marketing.
- The right to object to decisions which are based solely on automated means.
- The right to be notified of a personal data breach which is likely to result in a high risk to the Data Subject's rights and freedoms.
- The right to make a complaint to the ICO.

Please note that the right to restrict processing and the right to erasure are not absolute rights and the University will consider all requests against valid reasons and will comply with the legislation. This may mean retaining information for archiving purposes or in the public interest.

Should a request be made for a copy of Personal Data (Subject Access Request) to any area of the University, this should be forwarded immediately to the DPO at DPO@nottingham.ac.uk, alternatively direct the Data Subject to our online form.

4.3.3 Sharing and Transferring Personal Data

Data Sharing

The University may share Personal Data either within the University or with an external third party provided it has identified one or more valid lawful bases for processing.

The University will only share Personal Data we hold with third parties, such as our service providers, where:

a. there is a need to know for the purposes of providing contracted services and a written contract is in place;
b. where the third party complies with required data security standards, policies and procedures and puts adequate security measures in place; and
c. where the transfer complies with applicable data protection legislation.

Sharing of Personal Data must be set out in relevant privacy notices provided to the Data Subject.

Where you are looking to share Personal Data with a third party, please discuss with the Information Compliance Team by contacting DPO@nottingham.ac.uk.

International Data Transfers (transferring data outside the UK)

The UK GDPR restricts data transfers to countries outside the United Kingdom to ensure the level of protection afforded to individuals by the UK GDPR is not undermined. Where data is transferred outside the United Kingdom this is referred to as a 'restricted transfer' and Personal Data may only be transferred where:

a. there are UK adequacy regulations that cover the country or territory where the receiver is located; or
b. appropriate safeguards are in place such as standard contractual clauses issued by the ICO or a certification mechanism applies.

The University must ensure that Data Subjects will continue to have a level of protection that is in essence equivalent to that under Data Protection Legislation. This is achieved by the University undertaking a risk assessment (Transfer Risk Assessment) which considers the protections, safeguards and legal framework of the destination country.

Where a restricted transfer is not covered by UK adequacy regulations or an appropriate safeguard, it can only take place where it is covered by one of the limited exceptions set out in Article 49 of the UK GDPR:

1. The Data Subject has provided consent to the transfer, after they have been informed of potential risks; or
2. The transfer is necessary for one of the reasons set out in the UK GDPR such as performance of a contract (occasional and not regular transfers), public interest, to establish, defend or exercise legal claims or to protect the vital interests of the Data Subject (where they are incapable of giving consent), and, in some cases, our legitimate interests.

If you are looking to transfer Personal Data outside the UK you **must** speak to the Information Compliance Team and/or the DPO at DPO@nottingham.ac.uk.

4.3.4 Direct Marketing

The University is subject to specific rules and privacy laws when it comes to marketing its students, alumni and other Data Subjects. For example,

consent is required for electronic marketing (email, text etc.) other than the limited exception for existing students known as 'soft opt-in' which allows us to send marketing emails/texts where we have obtained the contact details whilst that individual is undertaking a course at the University and we are marketing similar products/services. However, the student must be given the opportunity to opt out of marketing when first collecting details and in each subsequent message – the right to object to marketing must be specifically offered in an intelligible manner.

The University should not undertake direct marketing to any individual who is not an existing student or has an existing relationship (commercial/contractual) without the individual's consent.

4.3.5 Research Exemption

Some data protection rules do not apply where Personal Data is being used for research purposes. This applies where the following conditions are met:

a. Appropriate technical and organisation safeguards exist to protect the data, such as data minimisation, pseudonymisation, or access controls.
b. There is no likelihood of substantial damage/distress to the Data Subject as a result of the Processing.
c. The research will not lead to measures or decisions taking about individuals.
d. Compliance with the requirements that the exemption negates would prevent or seriously impair the research purpose.

Where the above conditions apply, the following applies:

a. Personal Data originally collected for another purpose can be used for research and retained indefinitely.
b. The right of individuals to access their Personal Data does not apply if the research results are made public in a form which does not allow them to be identified (anonymised).
c. The rights of rectification, erasure, restriction and objection do not apply.

4.3.6 Publication of University Information

Members of the University should note that the University publishes information, including Personal Data. It does this using the lawful basis of legitimate interest, engagement in a public task or consent. These Personal Data are:

- Names of members of University Committees (including Council and Senate).

- Names and job titles of staff members. This may include academic and/or professional qualifications.
- Awards and Honours (includes Honorary Graduands and prize winners).
- Graduation programmes and video or other media versions of graduation ceremonies.
- Information within prospectuses (including photographs), annual reports, staff newsletters and campus news etc.
- Staff information on the University website (including photographs).
- Internal telephone directory.

4.4 The consequences of non-compliance

Breaching Data Protection Legislation can lead to fines and or claims for compensation in addition to the reputational risk of negative publicity for the University and risks to our colleagues and students.

A failure to comply with the principles set out in this policy may amount to a disciplinary offence and may be addressed through the relevant procedures which includes, but is not limited to, the staff Disciplinary Policy and the Code of Discipline for Students.

4.5 How compliance with the Policy will be measured

4.5.1 Reporting personal data breaches

Personal Data Breaches or suspected Personal Data Breaches must be reported through to the Information Compliance Team without delay as soon as they are identified. The University is required to notify the ICO within 72 hours of a breach incident being identified where it poses a high risk to the rights and freedom of individuals. The decision to report to the ICO will be taken by the DPO (or their deputy).

If you are aware or suspect a Personal Data Breach, do not attempt to investigate the matter, immediately report to the DPO and Information Compliance Team through our data incident form or contact DPO@nottingham.ac.uk. You should preserve all evidence relating to the incident. If you fail to report a Personal Data Breach in accordance with this Policy, this could lead to disciplinary action against you. Compliance with this Policy is vital to ensure any Personal Data Breach is dealt with promptly to protect the Personal Data of Data Subjects.

Some common examples of events leading to personal data breaches include (but are not limited to):

- misdirected emails or documents;
- inadequate disposal of information;

- leaving IT equipment unattended when logged-in to a user account without locking the screen to prevent others accessing information;
- loss or theft of laptop, mobile device or USB;
- physical security e.g., forcing of doors or windows into secure area or restricted information left unsecured in accessible area;
- unauthorised use of a University login and password;
- attempts to gain unauthorised access to University systems and information i.e., hacking;
- virus or other malicious (suspected or actual) security attack on IT equipment systems or networks; or
- disruption to, failure or loss of access to information or services due to (non-exclusive list) fire, flood, power outage, cyber-attack, or theft.

The University has in place appropriate procedures to deal with a Personal Data Breach and it will notify the ICO and/or Data Subjects as required. You **must** observe and comply with the University's Data Breach Procedure.

4.5.2 Data Protection Impact Assessments (DPIA)

The University is required to implement *Privacy by Design and Default* measures when Processing Personal Data. This is done by implementing appropriate technical and organisational measures to ensure compliance with the data protection principles. The University will assess:

a. the nature, scope, context and purpose of the processing;
b. necessity, proportionality and compliance measures; and
c. the risks posed in terms of likelihood and severity of risk to individuals, identifying additional measures to mitigate risks.

A DPIA will be conducted when implementing new systems and technology or business change programmes, including:

a. use of new technologies (systems or processes) or changing technologies;
b. large scale processing of sensitive data; and
c. large scale and systematic monitoring of publicly accessible areas.

Where you are responsible for implementing or managing a project that may require a DPIA, you should speak to the Information Compliance Team at DPO@nottingham.ac.uk. Where one is required, a DPIA **must** be completed before commencement of the project or implementation (go live) of the new system.

4.5.3 Annual Training

All staff at the University are expected to undertake statutory annual training on Data Protection, Security and Information Compliance.

4.6 Provisions for monitoring and reporting relating to the Policy

The University shall conduct regular periodic audits/spot checks to assess compliance with this Policy and related Procedures.

4.6.1 Record Keeping

The University must keep full and accurate records of its processing activities in accordance with Data Protection Legislation. This should include a description of the types of Personal Data and Data Subjects, processing activities and purposes, third party recipients, storage locations and retention periods. The University should also keep a record of any Personal Data Breaches.

Personal Data should only be retained for as long as needed for processing for the purposes it was collected. You must observe and comply with the University's Retention Schedule.

You must review systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls are in place to ensure proper use and protection of Personal Data.

4.6.2 Risk and Governance Assurance

This Policy comes within the scope of the University's Governance and Assurance Framework and will be assessed through the annual self-attestation cycle.

4.6.3 Information Management and Security Steering Committee (IMSSC)

Regular updates relating to monitoring statistics relating to this Policy are reported to the IMSSC.

5. Review

This Policy will be reviewed biennially by the DPO, IMSSC and the University Executive Board. It may also be revised as needed to ensure compliance with applicable laws, promote operational efficiencies, advance University strategy, and reduce institutional risks.

6. Related policies, procedures, standards, and guidance

Information Security Policy
Data Breach Procedure
Data Subject Rights Procedure
Privacy Notice Procedure
Data Subject Rights Procedure
Data Retention Schedule
CCTV Policy
University Privacy Notices

Appendix I

UK GDPR Data Protection Principles explained.

1. Lawfulness, Fairness and Transparency

The University must have a lawful basis for collecting and processing Personal Data and must do it for a specified purpose. Without a lawful basis the processing will be unlawful and unfair. You will need to consider one of these grounds when processing Personal Data:

a. The Data Subject has given their consent.
b. The Processing is necessary for the performance of a contract with the Data Subject.
c. To comply with the University's legal obligations.
d. To protect the vital interests of the Data Subject or another person.
e. To perform a task carried out in the public interests (this would be teaching and research in the University's case); or
f. To pursue the University's legitimate interests where those interests are not outweighed by the rights of the Data Subject. Legitimate interests is limited.

The University must identify at least one of the above grounds and document why it is relying upon it when Processing Personal Data.

1.2 Consent as a lawful basis

Consent is one of the legal bases which can be relied upon when Processing Personal Data but in order for consent to be valid you must consider the follow:

a. Consent must be 'freely given', specific and informed. Which means there must be a clear indication of agreement (consent). Therefore, pre-ticked boxes or inactivity cannot be taken as consent.
b. Data Subjects must be able to freely withdraw their consent at any time and a wish to withdraw consent must be acted upon promptly.
c. Consent should be refreshed regularly especially if you intend to Process Personal Data for a different or an incompatible purpose for which it was initially disclosed.
d. Consent must be evidenced and documented – this forms part of the accountability principle.

1.3 Transparency

Transparency requires the University to ensure that any information provided to Data Subjects about how their data will be processed is clear, concise, easily accessible and written in plain language. Such information is provided through Privacy Notices. A Privacy Notice will contain information about the Controller (the

University) and the DPO and will set out how the University will use, Process, protect, disclose and retain Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting/receiving the Personal Data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which considers our proposed Processing of that Personal Data, i.e., that the individual knew that their Personal Data was going to be passed to us and for what purpose.

2. Purpose Limitation

The University must only collect and Process Personal Data for a specified, explicit and legitimate purpose and where Data Subjects have been communicated with (Privacy Notice). Personal Data must not be further Processed in a manner which is incompatible for the purpose in which it was first collected. If the University intends to use it for a different purpose the Data Subjects must be informed of the new purposes and the lawful basis relied upon.

3. Data Minimisation

Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purpose for which it is Processed. Therefore, you can only collect Personal Data which is required for that specified purpose and should not seek more Personal Data than is necessary.

As an employee, you must only process Personal Data for the performance of your duties and tasks and not for any other purpose.

When Personal Data is no longer required for that specified purpose it must be deleted or anonymised in accordance with the University's data retention guidelines. The University's Data Retention Schedule provides information about the length of time the University retains records. Personal Data records must be destroyed safely and securely.

4. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. Personal Data must be corrected or deleted without delay where the University is made aware of its inaccuracy. You must ensure that you update all relevant records if you become aware that any Personal Data are inaccurate. Where appropriate, any out-of-date or inaccurate records should be deleted/destroyed.

Employees and students must ensure that they keep the University updated regarding any change of circumstances.

5. Storage Limitation

Personal Data collected and Processed by the University must not be retained in a form where the Data Subject could be identified for longer than is needed for the specified purpose(s) for which it was originally collected (other than where it is retained in order to comply with any legal, accounting or reporting requirements).

Where Personal Data is retained/stored for longer than necessary this may increase the severity of a data breach.

The University's Data Retention Schedule sets out retention periods for records including Personal Data and records should be deleted, destroyed, or anonymised after a reasonable period of time following expiry of the purpose(s) for which they were collected. Employees must comply with the University's Data Retention Schedule and should regularly review any Personal Data Processed in the performance of their duties and tasks to assess whether the purpose(s) for which the data are collected have expired.

All Privacy Notices must inform Data Subjects of the period for which their Personal Data will be stored/retained.

6. Security, Integrity and Confidentiality

6.1 Security of Personal Data

Personal Data must be secured by appropriate technical and organisational measures to protect it against accidental loss, destruction or damage and against unauthorised or unlawful processing.

The University will develop, implement, and maintain safeguards appropriate to the scope and size of our business, available resources, the amount of Personal Data that we control/maintain and identified risks (this will include the use of encryption and pseudonymisation where applicable).

The University will regularly test and evaluate the effectiveness of such measures to ensure they are adequate and effective.

You are responsible for ensuring the security of Personal Data processed by you in the performance of your duties and tasks and must follow all relevant procedures the University has in place to maintain the security of Personal Data; and you must observe and comply with our Information Security Policy. You must exercise particular care in protecting Special Category Data from loss and unauthorised access, use or disclosure.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use Personal Data can access it. This means if you have access to Personal Data but it is not required for you to perform your duties and tasks, you should not access this data.
- Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users can access Personal Data when they need it for authorised purposes. This means that you should not access or use any Personal Data if you are not permitted to.

You must not attempt to circumvent any administrative, physical or technical safeguards that have been implemented by the University as doing so may result in disciplinary action.

Appendix II

Policy on Processing Special Categories of Personal Data and Criminal Offence Data

As part of its statutory functions and obligations as both a higher education provider and employer the University processes Special Category Data and Criminal Offence Data in accordance with Articles 9 and 10 of the UK GDPR and Schedule 1 of the DPA 2018. This includes (but is not limited to) Personal Data relating to health, wellbeing, race, ethnicity and trade union membership. Further information can be found in our staff and student privacy notices.

Schedule 1 of the DPA 2018 requires the University to put in place an appropriate policy document in relation to the Processing of Special Category Data in accordance with Article 5 of the UK GDPR. This Appendix explains our processing and thus satisfied the requirements of Schedule 1 of the DPA 2018 and supplements the University's staff and student privacy notices. It satisfies the substantial public interest condition and the condition for processing employment, social security and social protection data.

Article 9 of the UK GDPR defines Special Category Data as racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, genetic data, biometric data, physical and mental health data; or data concerning sex life or sexual orientation.

Article 10 and of the UK GDPR and Section 11(2) of the DPA 2018 covers processing in relation Criminal Offence Data. This includes the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing.

The University processes Special Categories of Personal Data under the following UK GDPR Articles (these are not in order of requirement):

Article 9(2)(a) – Explicit Consent.

Article 9(2)(b) – where processing is necessary for the purposes of carrying out the obligations and exercising the University's rights as a Controller or in connection with employment, social security or social protection – for example staff sickness absence.

Article 9(2)(c) – where processing is necessary to protect the vital interests of a Data Subject or another natural person. For example, processing health information in the event of a medical or other emergency.

Article 9(2)(f) – where it is necessary for the establishment, exercise or defence of legal claims. For example, employment tribunal or other litigation.

Article 9(2)(g) – where processing is necessary for reasons of substantial public interest and is necessary for the University to carry out its role. For example, equality of opportunity.

Criminal Offence Data is processed under Article 10 of the UK GDPR – for pre-employment or pre-admission checks and declarations (for employees and students) in accordance with contractual obligations.

The University processes Special Categories of Personal Data under Part 1 of Schedule 1 of the DPA 2018:

Paragraph 1(1) – for employment, social security and social protection purposes.

The University processes Special Categories of Personal Data under Part 2 of Schedule 1 of the DPA 2018:

Paragraph 6(1) and 2(a) – for statutory purposes.

Paragraph 8(1) – to review absence of equality of opportunity or treatment between specific groups.

Paragraph 9(1) – where processing is carried out as part of a process of identifying suitable individuals to hold senior positions.

Paragraph 10(1) – preventing and detecting unlawful acts.

Paragraph 11(1) and 11(2) – where protecting the public against dishonesty.

Paragraph 12(1) and 12(2) – regulatory requirements relating to unlawful acts and dishonesty.

Paragraph 24(1) and 24(2) – disclosure of elected representatives.

The University processes Criminal Offence Data for the following purposes under Part 1 and Part 2 of Schedule 1 of the DPA 2018:

Paragraph 1 – for employment, social security and social protection purposes.

Paragraph 6(2)(a) – statutory purposes.