

DATA PROTECTION POLICY

2026/27

Contents

1 Policy Statement

2 Application Guidance

2.1 What is “personal data”, who is covered, and what is meant by “processing” personal data?

2.2 Data Subjects – Meaning of “students”, “parents”, and “Staff”

2.3 College Staff nominated to monitor Data Protection

2.4 Processing of personal data by the college (Students and Parents/Guardians data)

2.5 Processing of personal data by the college (Staff data)

2.6 Processing of personal data by the college (General data)

2.7 Special Category Personal Data and Criminal Offence Data

3 Rights of access to personal data (Subject Access Requests and other Data Subject Rights)

3.1 Who can exercise rights?

3.2 Requests from third parties concerning disclosure of personal data

4 Publication of personal data

4.1 Third parties with whom the college may need to share personal data

4.2 Transferring Personal Data Outside the UK

5 Responsibilities and obligations of staff members and governors of the college

5.1 Staff Photographs

5.2 Accuracy of personal data held by the college

5.3 Third Party Data Processors

Appendix 1 – Access Agreement Between Visiting Staff/Contractors and College



1. Policy Statement

This policy applies to Rochester Independent College ("the college").

The college is committed to complying with applicable data protection legislation, including the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 ("DPA 2018"), the Data (Use and Access) Act 2025 ("DUAA") and, where applicable, the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR"), together referred to in this policy as "Data Protection Legislation".

The college is registered with the Information Commissioner's Office ("ICO") where required to do so.

It is the specific policy of the college to:

take all appropriate and reasonable steps to protect the rights and freedoms of college staff, students, parents, governors and other individuals ("Data Subjects") in relation to their personal data;

- process personal data lawfully, fairly and transparently;
- ensure that personal data is collected for specified, explicit and legitimate purposes and is not processed in a manner incompatible with those purposes;
- ensure that personal data is adequate, relevant and limited to what is necessary;
- take reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date;
- retain personal data for no longer than is necessary, subject to applicable legal, regulatory and safeguarding requirements;
- ensure appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- demonstrate accountability for compliance with Data Protection Legislation.

All members of college staff will be made aware of this policy and their responsibilities under Data Protection Legislation. Appropriate data protection training will be provided and refreshed as necessary.

This policy will be made available internally and, where appropriate, externally.

The college will put in place appropriate organisational and technical measures to maintain the security of personal data throughout its lifecycle, from collection to secure deletion or destruction.

The college will maintain appropriate privacy notices explaining how and why personal data is processed, the lawful bases relied upon, applicable retention arrangements, the categories of recipients, relevant international transfers and the rights available to Data Subjects.



2. Application Guidance

The college is required to process relevant personal data regarding staff members, students, prospective students, former students, parents, guardians, governors and other individuals as part of its day-to-day operations.

This policy explains how the college will comply with its obligations when collecting, accessing, using, sharing, storing, retaining and disposing of personal data.

2.1 What is “personal data”, who is covered, and what is meant by “processing” personal data?

“Personal data” means any information relating to an identified or identifiable living individual.

An individual may be identifiable directly or indirectly, including by reference to a name, identification number, location data, online identifier or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

Individuals covered by this policy may include current, past or prospective students, their families or guardians, staff members, job applicants, former staff, governors, contractors, visitors and other relevant Data Subjects.

Personal data includes both facts and opinions about an identifiable individual.

“Processing” is interpreted broadly and includes collecting, recording, organising, structuring, storing, adapting, retrieving, consulting, using, transmitting, disclosing, combining, restricting, erasing and destroying personal data.

Personal data processed by the college may include, amongst other things:

- names, addresses and dates of birth;
- telephone numbers and email addresses;
- National Insurance numbers and other identifiers;
- bank details and other financial information;
- academic, disciplinary, admissions and attendance records;
- references;
- medical and pastoral information;
- examination scripts, results and marks;
- photographs;
- video and CCTV images;
- online identifiers and relevant IT-system records;
- special educational needs and disability information; and
- biometric data where used by the college.

For the purposes of Data Protection Legislation, the college will normally be the “controller” of personal data for which it determines the purposes and means of processing. In some



circumstances the college may act jointly with another controller or process information on behalf of another controller.

2.2 Data Subjects – Meaning of “students”, “parents”, and “Staff”

For the purposes of this policy, references to “students” include current, past and prospective students.

References to “parents and guardians” include parents and guardians of current, past and prospective students where applicable.

References to “staff” may include employees, visiting music or sports staff, contractors, agency workers, self-employed individuals contracted by the college, governors, relevant Dukes Education personnel, cover teachers and other individuals with a legitimate role-related requirement to access personal data.

Access to personal data will be granted only where there is a legitimate business need and will be restricted to the minimum level of access reasonably required for the individual's role.

Access may be granted on a “read only” or “read and write” basis as appropriate and may be withdrawn when it is no longer required.

2.3 College Staff nominated to monitor Data Protection

The college staff member nominated as Data Champion and to monitor data protection issues is: Peter Holl

The Principal will endeavour to ensure that personal data at the college is processed in accordance with this policy and Data Protection Legislation.

The Data Champion will support the college in relation to data protection matters, including:

- providing advice, education, training and support to staff;
- monitoring compliance with this policy;
- assisting with Data Subject requests;
- supporting the investigation and management of personal data breaches;
- supporting Data Protection Impact Assessments where required;
- overseeing data protection complaints;
- advising on appropriate data sharing and processor arrangements; and
- escalating significant data protection risks to the Principal.

Any individual who believes that a breach of this policy or Data Protection Legislation may have occurred should notify the Data Champion and/or Principal immediately.

Ultimate responsibility for compliance with this policy lies with the Principal, subject to any governance responsibilities applicable to the college.



Where the college is legally required to appoint a Data Protection Officer, or chooses to appoint one voluntarily, the identity and contact details of that person will be communicated separately and the statutory independence of that role will be respected.

2.4 Processing of personal data by the college (Students and Parents/Guardians data)

The college may process a wide range of personal data concerning students and their parents or guardians as part of its operations. This may include, but is not limited to:

- contact details;
- National Curriculum and other assessment results;
- attendance information;
- disciplinary information;
- admissions information;
- references;
- examination scripts, results and marks;
- information relating to special educational needs and disabilities;
- safeguarding and pastoral information;
- images of students participating in college activities; and
- relevant IT, communications and online-system information.

In relation to parents and guardians, personal data may include financial information and information necessary for the administration of the contractual relationship with the college.

The college may also process special category personal data, including information concerning health, racial or ethnic origin, religious or philosophical beliefs and biometric information where applicable.

Personal data will normally be collected directly from students, parents or guardians but may also be obtained lawfully from third parties.

Student and parent/guardian personal data may be processed where necessary to:

- provide education, teaching and learning;
- monitor and report on student progress;
- administer examinations and publish examination results where appropriate;
- provide pastoral, medical and safeguarding support;
- assess and improve the performance and operation of the college;
- administer admissions and the contractual relationship with parents or students;
- fulfil legal, regulatory and safeguarding obligations;
- communicate with students, parents and guardians;
- maintain appropriate contact with former students;



- monitor the use of college IT systems and communications where this is lawful, necessary and proportionate and in accordance with applicable college policies and privacy information;
- promote the college where there is an appropriate lawful basis for doing so; and
- fulfil other legitimate and lawful purposes relating to the operation of the college.

The college will identify an appropriate lawful basis under Data Protection Legislation for each processing activity. Depending on the circumstances, this may include processing necessary for performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task in the public interest where applicable, the legitimate interests of the college or a third party, or consent.

Consent will not be relied upon where another lawful basis is more appropriate.

Marketing communications by electronic mail, including email and SMS, will be sent only in accordance with Data Protection Legislation and PECR. Where consent is required it will be freely given, specific, informed and capable of being withdrawn. Where another lawful marketing exception applies, the college will comply with the conditions of that exception and provide an appropriate means to opt out.

2.5 Processing of personal data by the college (Staff data)

Personal data processed by the college in respect of staff members includes both factual information and, where relevant, opinions or assessments concerning the individual.

It may include information necessary for recruitment and employment, such as a staff member's name, contact details, qualifications, employment history, salary and payment information, performance information, absence records and other information reasonably necessary to manage the employment relationship.

The college will identify an appropriate lawful basis for processing staff personal data.

Processing may, for example, be necessary:

- to take steps before entering into or to perform an employment contract;
- to comply with a legal obligation;
- for the legitimate interests of the college or another person, where those interests are not overridden by the rights and freedoms of the individual;
- to protect vital interests; or
- where appropriate, on the basis of valid consent.

Because of the imbalance that may exist in an employment relationship, the college will not rely on staff consent where consent cannot reasonably be regarded as freely given.

Where special category personal data or criminal offence data is processed, an appropriate additional legal condition will also be identified.



Personal data concerning staff will be kept confidential and disclosed only where there is a lawful basis and legitimate need for the disclosure.

2.6 Processing of personal data by the college (General data)

The college will comply with the following data protection principles.

Personal data shall be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- accurate and, where necessary, kept up to date;
- kept in identifiable form for no longer than is necessary, subject to lawful retention requirements;
- processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage; and
- processed in a manner for which the college is able to demonstrate accountability and compliance with the above principles.

The college will determine and document an appropriate lawful basis for processing personal data. This may include:

- consent;
- performance of a contract or steps taken at the request of an individual before entering a contract;
- compliance with a legal obligation;
- protection of vital interests;
- performance of a task carried out in the public interest or exercise of official authority, where applicable; or
- legitimate interests pursued by the college or a third party, provided that those interests are not overridden by the interests, rights or freedoms of the Data Subject.

Where legitimate interests are relied upon, the college will consider and, where appropriate, document the purpose, necessity and balancing of those interests against the rights of affected individuals.

Data protection by design and default

The college will consider data protection requirements when designing, purchasing or materially changing systems, services, projects and processes involving personal data.



Appropriate technical and organisational measures will be implemented so that, by default, only personal data necessary for each specific purpose is processed.

Data Protection Impact Assessments

A Data Protection Impact Assessment ("DPIA") will be completed before commencing processing that is likely to result in a high risk to individuals' rights and freedoms.

A DPIA will be considered in particular where the college proposes significant new processing involving children or vulnerable individuals, systematic monitoring, special category data, biometric technology, innovative technology or other processing presenting an elevated privacy risk.

Where a DPIA identifies a high residual risk that cannot adequately be mitigated, the college will seek appropriate advice and, where legally required, consult the ICO before commencing the processing.

Records and retention

The college will maintain appropriate records of its processing activities and retention arrangements.

Personal data will be retained only for as long as reasonably necessary for the purpose for which it was collected, including applicable legal, safeguarding, contractual, insurance and regulatory requirements, and will then be securely deleted, destroyed or anonymised as appropriate.

2.7 Special Category Personal Data and Criminal Offence Data

"Special category personal data" includes personal data revealing:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data processed for the purpose of uniquely identifying an individual;
- health information; and
- information concerning a person's sex life or sexual orientation.

Criminal offence data is subject to separate legal requirements and is not treated as a category of special category personal data.

The college will process special category personal data only where there is both:

- an appropriate lawful basis for processing personal data generally; and
- an applicable condition permitting the processing of special category data.



Where required under the DPA 2018, the college will also satisfy an applicable Schedule 1 condition and maintain an Appropriate Policy Document.

Criminal offence data will only be processed where permitted by law and where the applicable safeguards and conditions are satisfied.

Depending upon the circumstances, special category data may be processed where necessary for employment or social protection obligations, safeguarding, substantial public interest purposes, provision or management of health care, protection of vital interests, legal claims or where explicit consent has validly been obtained.

Access to special category and criminal offence data will be restricted to individuals who have a legitimate need to access it.

Such information must not be copied, disclosed or otherwise processed outside authorised purposes and procedures.

3. Rights of access to personal data (Subject Access Requests and other Data Subject Rights)

Data Subjects have rights in relation to their personal data under Data Protection Legislation. Depending upon the circumstances, these include:

- the right to be informed about processing;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restriction of processing;
- the right to data portability where applicable;
- the right to object to processing;
- rights relating to certain automated decision-making; and
- the right to withdraw consent at any time where processing is based on consent, without affecting processing lawfully undertaken before withdrawal.

Not all rights apply in every circumstance and statutory exemptions may apply.

Subject Access Requests

A request by an individual for access to their personal data is known as a Subject Access Request ("SAR").

A SAR does not have to use any particular wording and does not have to be submitted on a particular form. It may be made verbally or in writing, including electronically.

Staff who receive a request which appears to concern an individual's data protection rights must promptly refer it to the Data Champion or other nominated person.



The college will respond to a valid SAR without undue delay and normally within one month of receipt, subject to the provisions of Data Protection Legislation concerning calculation of time limits.

Where permitted by law, the college may pause the applicable time period while reasonably required clarification is sought from the requester.

Where a request is complex, or where an individual has made a number of requests, the response period may, where permitted by law, be extended by up to a further two months. The individual will be informed within the initial response period where an extension is being applied and of the reasons for it.

Requests will normally be dealt with free of charge. A reasonable fee may be charged, or a request may be refused, only where permitted by Data Protection Legislation, including where a request is manifestly unfounded or excessive.

The college may request reasonable evidence of identity where it has legitimate doubts about the identity of the person making the request. Only information reasonably necessary to establish identity should be requested.

The college will undertake a reasonable and proportionate search for information falling within the scope of a SAR.

Before disclosing information, the college will consider whether it contains personal data relating to another individual and whether disclosure is lawful and appropriate.

Applicable statutory exemptions may result in some information being withheld.

Data protection complaints

Any Data Subject may raise a complaint concerning the college's processing of their personal data.

The college will provide a clear means by which a data protection complaint can be made.

The college will:

- acknowledge receipt of a data protection complaint within 30 days;
- take appropriate steps to investigate the complaint without undue delay;
- keep the complainant appropriately informed about the progress of the complaint; and
- inform the complainant of the outcome without undue delay once the investigation is completed.

The college will maintain appropriate records of data protection complaints.

Individuals will also be informed, where appropriate, of their right to raise a concern with the Information Commissioner.



3.1 Who can exercise rights?

Data protection rights belong to the individual to whom the personal data relates.

A parent, guardian or other person does not automatically exercise a student's data protection rights merely by virtue of that relationship.

In the case of a child or young person, the college will consider whether the student has sufficient maturity and understanding to exercise the relevant right themselves.

Where the student is competent to exercise their own rights, the college will normally respond to the student unless another person has appropriate authority to act on their behalf.

Where the student is not competent to exercise the right themselves, it may be appropriate for a person with parental responsibility to exercise it on their behalf.

In making such decisions, the college will have regard to the student's age, maturity, understanding, best interests, any duty of confidentiality, safeguarding considerations and the particular circumstances of the request.

A third party may exercise a Data Subject's rights on their behalf where the college is reasonably satisfied that the third party has appropriate authority to do so.

3.2 Requests from third parties concerning disclosure of personal data

The college may disclose personal data to third parties where there is an appropriate lawful basis and the disclosure is necessary and proportionate.

Examples may include disclosure:

- to educational institutions or prospective employers for references where appropriate;
- to examining bodies and educational authorities;
- where required for safeguarding or protection of a student's welfare;
- to health professionals where necessary;
- to insurers and professional advisers;
- to organisations involved in college trips, activities or services where necessary;
- to public authorities where required or permitted by law; and
- where the Data Subject has requested or validly consented to the disclosure.

Before disclosing personal data in response to a third-party request, the college will take reasonable steps to establish the identity and authority of the requesting party and determine whether the disclosure has an appropriate lawful basis.

The amount of personal data disclosed will be limited to what is reasonably necessary for the relevant purpose.



4. Publication of personal data

The college may use photographs, videos, names and other personal data in connection with college activities, publications, websites, online portals, social media, promotional materials and communications where there is an appropriate lawful basis.

The college will provide appropriate privacy information concerning such uses.

Where consent is relied upon, it will be obtained in accordance with Data Protection Legislation and may be withdrawn.

Where another lawful basis is relied upon, individuals will be provided with any applicable right to object.

Particular care will be taken when publishing identifiable information about students. The college will consider safeguarding, privacy and the best interests of students when determining whether and how images and other identifying information are published.

The college may:

- use appropriate images of college activities in prospectuses, websites, online portals, social media and other publications;
- compile and maintain registers and lists of students where required for college activities, teams, trips and events;
- communicate information concerning fundraising and initiatives considered beneficial to the college community, subject to applicable marketing requirements; and
- maintain appropriate contact with former students and communicate information concerning alumni events and activities.

Where direct electronic marketing is undertaken, the college will comply with PECR as well as applicable Data Protection Legislation.

4.1 Third parties with whom the college may need to share personal data

From time to time the college may share personal data, including special category personal data where appropriate and lawful, with third parties including:

- local authorities and other public authorities;
- government departments and regulatory bodies;
- the Independent Schools Inspectorate and relevant independent school bodies;
- examination and assessment bodies;
- health and welfare professionals;
- safeguarding organisations;
- professional advisers;
- insurers;
- IT and other service providers;



- educational establishments;
- employers where references have appropriately been requested; and
- other organisations where disclosure is necessary and lawful.

Such information may be shared where necessary:

- to comply with legal or regulatory obligations;
- to safeguard students and provide appropriate pastoral, medical or welfare support;
- to provide education and co-curricular activities;
- to administer assessments and examinations;
- to monitor students' educational progress and needs;
- to obtain professional advice and insurance;
- to fulfil a request made by a student, parent or guardian where appropriate;
- to provide references;
- to operate the college effectively; or
- for another lawful and legitimate purpose.

The college will apply data minimisation and will disclose only information reasonably necessary for the relevant purpose.

Where an external organisation processes personal data on behalf of the college, appropriate contractual and organisational safeguards will be put in place in accordance with Data Protection Legislation.

4.2 Transferring Personal Data Outside the UK

Personal data may be transferred outside the United Kingdom only where the requirements of applicable Data Protection Legislation concerning international transfers have been satisfied.

Before making a restricted transfer, the college will determine whether:

- the destination is covered by applicable UK adequacy regulations;
- an appropriate safeguard recognised under UK Data Protection Legislation can be used; or
- a specific statutory exception applies.

Where appropriate safeguards are required, these may include an approved international data transfer mechanism, such as the UK International Data Transfer Agreement ("IDTA"), the UK Addendum to approved contractual clauses, or another legally recognised safeguard.

Where required, the college will carry out and document an appropriate transfer risk assessment or equivalent assessment before relying on relevant safeguards.

The college will also consider international transfers when appointing suppliers and using cloud or online services, including circumstances where information is stored in the UK but can be remotely accessed from another country.



5. Responsibilities and obligations of staff members and governors of the college

All staff members and governors have a responsibility to process personal data in accordance with this policy, applicable college procedures and Data Protection Legislation.

In particular, staff and governors must:

- access personal data only where necessary for legitimate college purposes;
- ensure that personal data is adequate, relevant and limited to what is necessary;
- take reasonable steps to ensure information is accurate and up to date;
- keep personal data secure while stored, used or transmitted;
- use only college-approved systems, applications and services for processing college personal data unless specific authority has been obtained;
- comply with applicable retention and secure disposal requirements;
- avoid disclosing personal data to unauthorised persons;
- promptly refer Data Subject rights requests to the appropriate person;
- immediately report actual or suspected personal data breaches; and
- complete data protection training as required.

Personal data subject to this policy must not be stored outside approved college IT systems unless express authority has been given by the nominated person and appropriate security arrangements are in place.

Personal data transmitted using approved third-party web or cloud services must be protected using appropriate technical and organisational security measures, including encryption where appropriate.

Staff must not disclose home contact details or other personal data relating to staff, students, parents or other Data Subjects without an appropriate lawful basis and authorisation.

Personal data breaches

All actual or suspected personal data breaches must be reported immediately to the Data Champion, Principal or other nominated person in accordance with the college's breach reporting procedure.

Staff must not delay reporting a suspected breach while attempting to investigate it themselves.

The college will promptly assess and document reported incidents and determine whether they constitute a personal data breach.

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the college will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach.



Where the breach is likely to result in a high risk to the rights and freedoms of affected individuals, the college will also communicate the breach to those individuals without undue delay unless a statutory exception applies.

The college will maintain an appropriate record of personal data breaches, including breaches that do not require notification to the ICO.

5.1 Staff Photographs

Staff photographs may be used for legitimate security, safeguarding, identification and internal operational purposes where there is an appropriate lawful basis.

The use of staff photographs for external promotional purposes will be separately considered and an appropriate lawful basis identified.

Where consent is relied upon for promotional use, staff members may refuse or withdraw consent without detriment.

Staff who wish to object to or discuss the use of their image in college promotional material should notify the Principal or Data Champion.

5.2 Accuracy of personal data held by the college

The college will take reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date.

Staff, students, parents, guardians and other Data Subjects should notify the college of relevant changes to their information.

A Data Subject has the right to request correction of inaccurate personal data and completion of incomplete personal data.

In appropriate circumstances a Data Subject may also have the right to request erasure or restriction of processing.

Requests relating to these rights should be referred promptly to the Data Champion or nominated person and will be handled in accordance with Data Protection Legislation.

5.3 Third Party Data Processors

Access to personal data may be granted to visiting teachers, contractors, agencies, self-employed individuals, cover teachers and other persons contracted by the college where they have a specific and legitimate role-related requirement to access that information.

Access will be limited to the minimum personal data necessary for the relevant purpose.

Where appropriate, such individuals will be required to read this policy and sign and return the agreement at Appendix 1.



Where the college appoints another organisation to process personal data on its behalf, the college will undertake appropriate due diligence and use only processors providing sufficient guarantees that appropriate technical and organisational measures will be implemented.

A legally compliant written contract or other binding arrangement will be put in place with processors as required by Data Protection Legislation. This will address, as appropriate:

- the subject matter and duration of processing;
- the nature and purpose of processing;
- the types of personal data and categories of Data Subjects;
- processing only on documented instructions from the college;
- confidentiality;
- information security;
- use of sub-processors;
- assistance with Data Subject rights;
- assistance with security incidents, personal data breaches and DPIAs;
- deletion or return of personal data at the end of the service;
- provision of information necessary to demonstrate compliance; and
- audit and inspection rights where appropriate.

The college will maintain appropriate oversight of processors throughout the contractual relationship.

Any person who believes that the college, a member of staff or a processor has failed to comply with this policy or Data Protection Legislation should notify the Data Champion or Principal.

Created/Reviewed/ Updated	Author/Reviewer	Approved by	Date
September 2017	PL	AB	September 2017
August 2018	AD	AB	August 2018
August 2019	AD	AB	August 2019
August 2020	AD	AB	August 2020
August 2021	AD	AB	August 2021
August 2022	AD	AB	August 2022
August 2023	AD	AB	August 2023
August 2024	AD	AB	August 2024
July 2025	AD	AB	July 2025
August 2026	KS/PH	KF	August 2026



Appendix 1

ACCESS AGREEMENT BETWEEN VISITING STAFF/CONTRACTORS AND COLLEGE

(To be kept on staff/contractor files)

Access to personal data may be granted to visiting teachers, contractors, agencies, self-employed individuals or other persons providing services to the college where they have a specific, legitimate and role-related requirement to access personal data, including special category personal data where appropriate.

I, the undersigned, confirm that I have a legitimate reason to be granted the level of access authorised by the college to personal data held or controlled by the college.

I confirm that I have read and understood the college's Data Protection Policy and undertake to comply with its requirements and with all instructions given to me by the college concerning personal data.

In particular, I undertake that:

- I will access personal data only where necessary to perform my authorised duties;
- I will not use personal data for any purpose other than the authorised purpose;
- I will not copy, download, retain or share personal data except where this is authorised and necessary for my role;
- I will not disclose personal data to any unauthorised third party;
- I will use only systems, devices and methods authorised by the college when accessing or processing personal data;
- I will take appropriate measures to keep account credentials, devices and personal data secure;
- I will comply with any confidentiality, retention and secure-deletion requirements notified to me by the college; and
- I will comply with the college's instructions when my access is changed or withdrawn.

I undertake to notify the nominated person immediately:

- when I no longer have a legitimate need to access any or all of the personal data for which access has been granted;
- if I believe my account, device, IT security or credentials have been or may have been compromised;
- if personal data has been lost, disclosed to an unauthorised person, sent to an incorrect recipient, altered without authority or otherwise compromised;
- if I become aware of any other actual or suspected personal data breach; or
- if I receive a request from an individual concerning their personal data or data protection rights.



I understand that I must not investigate a suspected personal data breach myself before reporting it and that my access rights may be suspended or withdrawn at any time by an authorised member of college staff.

I understand that failure to comply with these requirements may result in withdrawal of access and may constitute a breach of my contractual or other obligations to the college.

Name: _____

Organisation/Role: _____

Signed: _____

Dated: _____