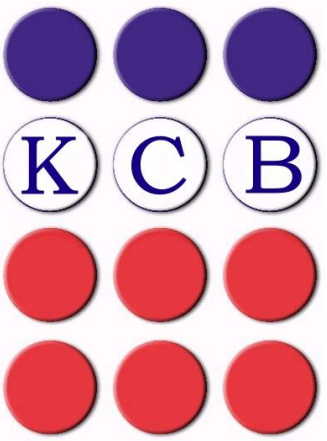

KENSINGTON COLLEGE OF BUSINESS

INFORMATION POLICY

Contents

General Data Protection Regulation 2018

The Data Protection Act (DPA) will be replaced by the General Data Protection Regulation (GDPR) from May 2018. These new EU regulations are intended to strengthen and unify the safety and security of all data held within an organisation, including schools and colleges. The GDPR will fundamentally change the way schools and colleges manage data and information and will bring increased responsibility to ensure all data is managed in the right way.

Information Disclosure

Third Party Disclosure

The College will maintain the rights to confidentiality of our students and will not release information regarding our students even where the third party is a parent or relative, and/or has paid or contributed to fees. The College will not confirm whether individuals are registered students of the College.

Third parties listed as next of kin or emergency contacts have no right to access to information about students. They will be contacted by the College only in cases of emergency or continual non-attendance (as set out in the Attendance Policy).

Where an enquiry is received, it shall be noted by College staff (without giving confirmation that the individual in question is a student of the College). Enquiries from third parties will be taken in writing.

The student shall then be contacted and given details of the enquiry, to include the name of the individual, the means of contact, the information requested and the purpose of the request. They may give written consent to respond to the enquiry, in which case their information disclosure consent will be filed with a record of the enquiry. The College will not record that consent is given to respond to a particular third party in our central records. On the basis that relationships between individuals change, each subsequent request will require new written consent prior to disclosure.

Government / Regulatory Statutory Exemptions

Students must be aware that when information is shared with the College regarding certain matters (with particular reference to immigration) there is a **LIMIT TO THE EXTENT TO WHICH INFORMATION PROVIDED TO THE COLLEGE BY STUDENTS IS CONFIDENTIAL**.

The general policy of the College is not to release information to third parties, unless given specific instruction or permission by the student to do so. This does not include responsibilities as a sponsor and employer, or to otherwise assist the UK Government (in its various departments) and the numerous requests for information bearing reference to specific exemptions from the General Data Protection Regulation which may be sent to the College by the UK Government. These commonly include (but are not limited to) National Security; Crime

and Taxation; Health, Education and Social Work; Regulatory Activity; and Disclosures required by law or made in connection with legal proceedings, etc.

Information collected regarding applicants who are not offered a place or enrolled at Kensington College of Business will be retained and will be subject to the same terms of disclosure.

We will always provide information to the UK Government where requested - this includes (but is not limited to):

Home Office/UK Visa and Immigration (UKVI)

As a sponsor of international students the College is obliged to inform the UKVI of any reasonably suspected or proven breaches of the conditions of the visas of our students. This ranges from illegal working to non-attendance (and standard Reporting duties, as listed in the UK Visa and Immigration Sponsor Guidance).[1]

Please note that the College is required to actively provide the UKVI with information about reasonably suspected breaches of visa conditions by our sponsored students without waiting for a request for information from the UKVI.

We reserve the right to pass information to the UKVI about non-sponsored students (without requiring a request for information from the UKVI) depending on the nature and seriousness of the information we have.

In addition to this, the College will always reply to requests for information from the UKVI where they require further information regarding any persons known to the College (not limited to students) which may help in the prevention or detection of crime and the apprehension of offenders, including matters not directly related to the College. In such cases correspondence from the UKVI will contain reference to the specific provisions / sections of the Data Protection Act by which information is being requested and is exempt from non-disclosure, where required. The individuals concerned will not be informed that information has been given about them.

The Police

The College will always respond to legitimate information disclosure requests by the Police, where specified exemption from non-disclosure under the Data Protection Act is confirmed to us.

The Courts

Where information disclosure is requested by the Courts stating provision / section of the Data Protection act by which the information is required and exempt from non-disclosure, in-line with UK Law, the College will not hesitate to provide it.

Council Tax Enquiries

The College will always assist local councils in their enquiries regarding Council Tax. Students who are registered and meeting the Terms and Conditions of the College will be offered

[1] http://www.ukvi.homeoffice.gov.uk/sitecontent/documents/employersandsponsors/pbsguidance/

documentation to confirm that they meet the requirements for Council Tax exemption, where appropriate. In cases where students are not meeting the Terms and Conditions of the College, the management of the College shall reserve the right not to issue documents for Council Tax Exemption to the student and release the same information to the Council should they enquire about the student's eligibility for Council Tax exemption to the College directly.

Terrorism

The College will immediately inform the Police, the UKVI and any other appropriate organisation of the UK Government with any information that reasonably suggests involvement by persons known to the College in terrorist activity.

Verification of Application

The College requires all applicants to accept the condition that all information, registration details, documentation and results provided to the College in the application form can be verified.

False Information / Documentation

The College does not consider that the General Data Protection regulation should protect those who provide false information for their own benefit, and will respond to external requests for verification of students' records (limited to results / overall course outcome) or documentation which is false when sent to the College for verification.

Personal information will not be given out to third parties, but the College will confirm that documents and/or information are false.

(This is **in addition** to instances where information relating to false information / documents may also fall under exemption from non-disclosure to the UK Government, Police, and Regulatory Bodies for the prevention / detection of crime, etc.)

Intellectual Property

Any use of College facilities must abide by the relevant legislation relating to Intellectual Property. The use of facilities (including, but not limited to, library resources, IT facilities, course reference materials) in contravention of Intellectual Property laws

The College is licensed under the terms of the Copyright Licensing Agency. [2]

Students

The College does not make a claim to the Intellectual Property rights of students arising as a result of their work during their course of study, except where they may be considered as an employee.

Employees

Except in reference to inventions made by employees in fields either directly or indirectly unrelated to the activity of Kensington College of Business past or present, any and all

[2] http://www.cla.co.uk/
(03/09/2013)

improvements and inventions made during employment with the KCB shall be the property of Kensington College of Business. As a condition of employment, employees agree to sign all documents required to transfer title of such inventions to the College without receiving compensation or payment.

This condition does not prejudice any rights held under the Patents Act 1977 *(amended 2017).*

The immediate surrender of any intellectual property belonging to the College may be demanded by the College on termination of employment.

Retention of student work

The College will only retain copies of Dissertations for future reference—University of Chester and the University of Wales operate separate rules (which must be acknowledged by each candidate in a Declaration to be submitted with the completed Dissertation). Each University Partner has specific rules regarding the retention and publication of Student Dissertations.

College Documentation

Over their course of study most students will require documentation from the College to confirm their status as students for a range of purposes, including (but not limited to) Visa applications, Council Tax Exemption, National Insurance Number requests, bank registration, etc. Issuance of such letters is at the discretion of College management and will only be offered to students on the condition that they are meeting the Terms and Conditions of the College (with particular reference to attendance, fees, disciplinary matters, etc.)

All letters are issued at the discretion of the College and are issued solely for their stated purpose and for the attention of named addressees, where appropriate.

The College reserves the right to recall documentation issued, where it is subsequently made invalid.

The College reserves the right to take action where we have reasonable suspicions that College documents are being misused, or where information contained on the documents has since become invalid and the student has not returned documentation to the College for amendment. Full details are set out in the Student Welfare and Conduct Policy (under disciplinary matters).

Record Keeping

Documentation and Audit

The College has a policy of record keeping for our students in line with the UK Visa and Immigration requirements for a Tier 4 Sponsor, which can be found on the UK Visa and Immigration website. In particular:

- Passport (including all relevant pages)

- Visa / Biometric Residence Permit
- Regularly updated contact details
- Copies of all any relevant documentation used to assess the student's application prior to receiving an offer from KCB

Once a student has enrolled with the College, every piece of documentation in their file should be a photocopy with a verification stamp and signature to attest that it has been checked against the original by KCB staff.

The College does not keep original documents in student files (except where the documentation has been created specifically for KCB and is addressed to the College).

The College also completes an annual audit of Passport copies to ensure that documentation provided by students is up to date. Students must be prepared to bring their Passport to KCB at least once per year for a new verified copy to be taken (to ensure that visa documentation has not been curtailed and so that immigration stamps can be copies, for example). Failure to make passport and visa documentation available for auditing purposes and failure to maintain current contact details both put the College in direct breach of our responsibilities as a sponsor and, as such are considered to be disciplinary offences.

Archiving

The College will keep records for the following amount of time:

Rejected / Incomplete Applications:

Documentation:	six years
Summarised Information:	six years

Student Files:

Documentation:	six years after completion of programme
Assessment (hard copies):	six years after completion of programme
Financial Records:	Seven years
Basic Information *:	six years after completion of programme

** includes name, last known address, summary of tuition fees, staff comments*

Web Page Files: Internet Cookies

All workstations: Internet Explorer should be scheduled to delete Internet cookies once per month.

Staff Files

Policy Statement

The College holds personnel records for employees and complies with all requirements of the General Data Protection Regulation. All information in personnel files will be treated in the strictest confidence.

Data Processing

Personal data will be processed fairly and lawfully, and will be obtained and processed solely for the administrative purposes of the College. It will not be passed to other parties unless the employee expressly requests that we do so. The type of personal data collected will be adequate, relevant and limited only to that which is necessary for the College's personnel administration.

Every effort will be made to keep personal data accurate and up to date and it is each employee's responsibility to ensure that they inform the Registrar of any change of address, next of kin or any changes such as bank account in order that the personnel file and pay details may be kept up to date.

Personal data will not be kept longer than is necessary. If at any point during employment the College needs to ask an employee's Doctor/Consultant for a medical report, consent will be obtained under the Access to Medical Reports Act 1988.[3] Personal data will be processed in accordance with rights under the General Data Protection Regulation and will not be transferred to a Country or Territory outside the European Economic Area.

Right of Access to Personnel Files

Each employee has a right to access their personnel file upon reasonable notice to the College. There may be an administration charge for this service or a charge for providing copies.

Company Information

Company information for Kensington College of Business and Kensington Education Foundation is freely available.

Receipt of Correspondence

The College does not encourage students to arrange for correspondence / post to be delivered to the College and does not accept responsibility for loss or failure of delivery.

At the time of writing the UK Visa and Immigration has a policy of sometimes sending documentation to students' care of the College. In our capacity as sponsor of the student, the College reserves the right to open this correspondence for the purposes of identifying the addressee and/or forwarding the letter as a soft copy where the matter may be urgent or the

[3] http://www.legislation.gov.uk/ukpga/1988/28/contents

postal address is not valid. Such cases must be approved by senior management and the confidentiality of student shall be strictly observed.

Section B

Student Data 'Fair Processing' Notice

Kensington College of Business is required to maintain certain information on its employees, students, alumni and other users, so as to allow the College to monitor performance, achievement, and health and safety, just to give a few examples. To comply with legal regulations, information must be collected and used fairly, accurately, stored safely, and not disclose to unauthorized persons unlawfully.
The College therefore complies with principles set out in the *General Data Protection Regulation 2018*.

In accordance with the General Data Protection Regulation, students are obligated to ensure that all personal data provided to the College is accurate, and up to date. They must also ensure that changes to their personal data i.e. addresses, telephone numbers etc., are notified to the College Administrative Team.

During the Admission or Enrolment stage where a student discloses a disability/disabilities that they believe to have, this information may be passed on (unless you have objected explicitly) to other College Departments or Partner Institutions, so appropriate arrangements can be made for assessments or examinations.

The information the College maintains may also be used to provide students with necessary support services, to process fees, bursaries, grants and loan information. We will also use your information to meet obligations to external agencies and organisations. This includes University of Chester, Pearson BTEC (the awarding body for HNC/HND), Local Authorities (Student Financial Support, Council Tax, and Electoral Registration Department), and The Higher Educational Statistics Agency (HESA). If your programme is connected to a Professional Body, then the College may exchange information, in accordance with their requirements.

HESA (Higher Educational Statistics Agency) Student Records

The College will send some of the information that we hold to HESA. Some of this data will be sensitive, such as any disabilities, ethnicity, sexual orientation, gender reassignment, pregnancy/maternity and religion (this list is not exhaustive). This information will be used by HESA in their own right.

[1]*"Every year your provider will send some of the information it holds about you to HESA ("your HESA information").*
HESA is the official source of data about UK universities, higher education colleges, alternative HE providers, and recognised higher education courses taught at further education institutions in Wales. HESA is a registered charity and operates on a not-for-profit

basis. Your HESA information is used for a variety of purposes by HESA and by third parties as described below. HESA may charge other organisations to whom it provides services and data. Uses of your HESA information may include linking parts of it to other information, as described below. Information provided to HESA is retained indefinitely for statistical research purposes. Your HESA information will not be used to make automated decisions about you."

Purpose 1 - Named data used for public functions

Your HESA information is used by public authorities for their statutory and/or public functions including funding, regulation and policy-making purposes.
Your information is provided by reference to your name, but your information will not be used to make decisions about you.

Your HESA information is used by some organisations to help carry out public functions connected with education in the UK. These organisations are data controllers in common of your HESA information under the terms of the General Data Protection Regulation. Such organisations may include:

- *Department for Business, Innovation and Skills*
- *Welsh Government*
- *Scottish Government*
- *Department for Employment and Learning, Northern Ireland*
- *Higher Education Funding Council for England*
- *Higher Education Funding Council for Wales*
- *Scottish Further and Higher Education Funding Council*
- *Department for Education*
- *Research Councils*
- *Skills Funding Agency*
- *National College for Teaching and Leadership*
- *National Health Service (including Health Education England)*
- *General Medical Council*
- *Office For Fair Access*
- *The Quality Assurance Agency for Higher Education*

and any successor bodies. These organisations may link your HESA information with other information they or other organisations hold. For example:

- *The Department for Education and the Department for Business Innovation and Skills link your HESA information to the National Pupil Database and the Individual Learner Record.*
- *Your HESA information is linked to information from the Student Loan Company by the HE Funding Councils.*
- *Your HESA information may also be linked to tax information or employment information.*

Linked data is used for research into education and its outcomes.

Other uses

Your HESA information may also be used by some organisations to help carry out public functions that are not connected with education. Such uses may include the following:

- *Measurement of population levels and migration by the Office for National Statistics, National Records of Scotland and the Northern Ireland Statistics and Research Agency*
- *Monitoring of public expenditure by the National Audit Office*

- *Monitoring of the accuracy of electoral registers by Electoral Registration Officials.*

Purpose 2 - Administrative uses
Your named data may be processed by public authorities for the detection or prosecution of fraud. These uses of your HESA information may result in decisions being made about you.

Fraud detection and prevention *–Your HESA information may be used to audit claims to public funding and student finance, and to detect and prevent fraud.*

Your HESA information will not be used to make decisions about you other than for those uses outlined under Purpose 2.

Purpose 3 - HESA publications
HESA uses your HESA information to produce statistical publications. These include some National Statistics publications (http://www.statistics.gov.uk/hub/what-are-national-statistics-) and online management information services. HESA will take precautions to ensure that individuals are not identified from any information which is processed for Purpose 3.

Purpose 4 – Equal opportunity, research, journalism and other processing for statistical and research purposes
HESA information is used for research into higher education and the student population. This research can be academic, commercial, journalistic or for personal reasons. HESA prohibits the identification of individual students by those carrying out this research and information is not shared on a named basis

HESA and the other data controllers listed under Purpose 1 may also supply information to third parties where there is a legitimate interest in doing so. Examples of use for this purpose include:

- *Equal opportunities monitoring*
- *Research - This may be academic research, commercial research or other statistical research where this is in the public interest*
- *Journalism - Where the relevant publication would be in the public interest e.g. league tables*
- *Provision of information to students and prospective students*

Users to whom information may be supplied for Purpose 4 include:

- *Higher education sector bodies*
- *Higher education providers*
- *Academic researchers and students*
- *Commercial organisations (e.g. recruitment firms, housing providers, graduate employers)*
- *Unions*
- *Non-governmental organisations and charities*
- *Local, regional and national government bodies*
- *Journalists*

Information supplied by HESA to third parties is supplied under contracts which require that individuals shall not be identified from the supplied information. A copy of HESA's current agreement for the supply of information is available at http://www.hesa.ac.uk/bds-details#e. HESA student information (linked to the National Pupil Database and/or Individual Learner Record held by DfE) may be supplied by HESA through DfE to researchers. A copy of the

Agreement for the supply of linked data is available at https://www.gov.uk/government/collections/national-pupil-database

Students and Alumni Survey
Your contact details may be passed on to survey contractors to carry out the National Student Survey, and surveys of student finances. This will be done on behalf of organisations listed under *'HESA's Purpose 1'*. Read more

Your Rights
Under the General Data Protection Regulation May 2018, students have a right to access personal data that Kensington College of Business and HESA holds on them. For access to data that Kensington College of Business holds on you, please make a request to the College Registry Office (Room G2). Access to data that HESA hold on students are subject to payment of a fee. For further information please see HESA Student Records www.hesa.ac.uk.
If you need more information or clarification please contact the College Registry or compliance Office.

Useful links:

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

https://www.hesa.ac.uk/files/HESA_Student_Collection_Notice_2017-18_updated_20180417.pdf

SECTION C

DATA PROTECTION POLICY

Introduction

Kensington College of Business (KCB) processes the personal data of living individuals such as its staff, students, contractors, research subjects and customers. This processing is regulated by the Data Protection Act 1998 (DPA) and from May 2018 the General Data Protection Regulation (GDPR). The UK's regulator for the DPA and GDPR is the Information Commissioner's Office (ICO). KCB is registered as a Data Controller with the ICO and is responsible for compliance with the GDPR and DPA.

Key Definitions

This DPA and GDPR contain a number of key definitions which are referenced in this policy such as 'personal data', 'processing' and 'Data Controller'. Those definitions are set out in **Annex A**.

Purpose and Objectives of Policy

This policy sets out the KCB's commitment to comply with the Data Protection Act 1998 ('DPA'), and from May 2018, the *General Data Protection Regulation* ('the GDPR').

Scope and Status of the Policy

This policy applies to all KCB staff, students and others who use or process any personal data. This policy applies regardless of where personal data is held and or the equipment used if the processing is for KCB's purposes. Further, the policy applies to all personal data, sensitive personal data or special category data held in any form whether manual paper records or electronic records.

Roles and Responsibilities

The Academic Board is responsible for approval of the Policy.

Information Asset Owners

KCB will appoint an Information Asset Owner (IAO) with local responsibility for data protection compliance for personal data processed in their area.

Information Asset Managers

KCB will appoint an Information Asset Manager who will hold local responsibility for data protection compliance processed within their faculties.

Data Protection Officer

KCB's Data Protection Officer (DPO) is primarily responsible for advising on and assessing the KCB compliance with the DPA and GDPR and making recommendations to improve practice in this area. Further, the DPO acts as KCB's primary point of contact for DPA and GDPR matters.

Legal Services

Legal Services are responsible for providing advice, support and guidance in relation to day-to-day data protection matters.

All staff

All staff, including permanent staff, fixed term contractors and temporary workers must comply with this Policy, the DPA and from May 2018 the GDPR whenever processing personal data held by KCB or on behalf of KCB.

All Students

All students are responsible for compliance with the rules and policies made by KCB. Students must comply with this policy where collecting and processing personal data as part

of their course, studies or research.

Contractors and Consultants

Third parties such as consultants, contractors or agents, undertaking work on behalf of KCB involving personal data, must adhere to KCB's Data Protection Policy and comply with the DPA and from May 2018, the GDPR. Provision will be made in contracts with external providers to ensure compliance with this Policy, the DPA and GDPR.

Compliance with the DPA and GDPR

Awareness & Capability

KCB will implement, and monitor annual completion of, mandatory Data Protection training for all staff. The content of that training will be reviewed annually.

Privacy by Design

KCB will implement a Privacy by Design Approach to processing personal data through integrating Privacy Impact Assessments into business processes and projects.

Security

KCB will protect the security of personal data by maintaining, and monitoring compliance.

Record Keeping & Retention

KCB will maintain a Records Retention and Disposal Schedule setting the periods for which records containing personal data are to be retained.

External Contractors and International Transfers

KCB will enter into legally binding contracts with external bodies where those bodies are engaged to process personal data on our behalf. KCB will implement adequacy arrangements where transferring any personal data outside of the European Union.

Other Third Party Access

KCB will only disclose personal data to third parties such as the police, central government and other education institutions where there is a lawful basis for doing so and appropriate arrangements are in place with those parties.

Internal Sharing

KCB will seek to ensure that personal data is only shared across different teams, divisions or faculties where those areas have a business need for accessing that data**.**

Data Subjects Rights

KCB will comply with requests from an individual to exercise their rights under the DPA, and from 25 May 2018, the GDPR. All individuals have the right to be informed what information KCB holds about them and to request copies of that information. This is known as a Subject Access Request. Any individual wishing to submit a Subject Access Request should follow the instructions on the student portal.

Under the DPA and GDPR, individuals also have the following rights in relation to their personal data:

- The right to request their personal data is rectified if inaccurate
- The right to request erasure of their personal data
- The right to request that the processing of their personal data is restricted
- The right of portability in relation to their personal data
- The right to object to the processing of their personal data
- The right to object to processing which involves automated decision making or profiling.

Individuals who wish to exercise the above rights should contact the KCB's Data Protection Officer. Individuals should submit their request in writing and specify exactly what personal data and/or processing they are referring to and which right they wish to exercise. If you are seeking access to your personal data (i.e. making a 'Subject Access Request') then you may find it helpful to complete a form.

Any staff member who receives a Subject Access Request or a request from an individual to exercise the above rights under the DPA and GDPR must be forwarded to the Date Protection Officer.

Own Personal Data

All staff and students are responsible for checking that information they provide to KCB in connection with their employment or studies is accurate and up to date. Any changes to personal data provided (e.g. change of address) must be promptly notified, in writing to KCB .KCB cannot be held responsible for errors unless the member of staff or students has properly informed KCB about them.

Personal Data Breaches

KCB will respond promptly to any identified personal data breaches and thoroughly investigate those incidents to ascertain whether;

- The breach should or must be reported to the ICO
- Data subjects should or must be made aware of the breach; and
- It is necessary to amend processes or introduce new measures to mitigate against any further breaches.

Any staff member who knows or suspect an actual or potential personal data breach has occurred must immediately notify the Data Protection Officer. All staff are responsible for fully engaging and cooperating with the Officer in relation to their investigation of a personal data breach.

Compliance

Compliance with this Policy, the DPA and from May 2018, the GDPR is the responsibility of all members of staff and students. Employees must comply with the rules and procedures made by KCB. It is a condition of being a student that all KCB rules and policies are fully complied with.

Any breach of the policy by a member of staff may result in disciplinary action or access to KCB'S facilities being withdrawn. Serious or deliberate breaches of the DPA can result in a criminal prosecution.

Any breach of the GDPR by the KCB may result in a substantial fine or actions imposed upon KCB by the ICO.

Further Information

Questions about the interpretation or operation of this policy should be taken up in the first instance with the Data Protection Officer. Any individual who considers that the Policy has not been followed in respect of personal data about themselves should also raise the matter with KCB'S Data Protection Officer.

Further information about the Data Protection Act 1998 and the GDPR can be found on the Information Commissioner's Office (ICO website).

Annex A Key Definitions:

1. Personal Data: data which relate to a living individual who can be identified from those data or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual. Under the GDPR, the definition of personal data will explicitly extend to IP addresses.

2. Sensitive Personal Data: information about an individual's ethnicity, political opinions, their religious beliefs or other beliefs of a similar nature, membership of a trade union, disability, sexual orientation, the commission or alleged commission by them of any criminal offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal

of such proceedings of the sentence of any court in such proceedings.

3. Under the GDPR, the term 'sensitive personal data' will be replaced by the definition special category data which means any personal data information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and their genetic or biometric data.

4. Processing: any operations or set of operations which is performed on personal data whether or not by automated means such as collection, use, disclosure or storage of personal data etc.

5. Data Controller: the organisation which either alone or jointly with another organisation, determines the manner and purpose of the processing of personal data. The Data Controller is responsible for compliance with the DPA and GDPR.

6. Data Processor: an organisation (such as a contractor) which processes personal data on behalf of a Data Controller.

7. 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.

Next Review Date: **July 2019**
Reviewed By: **Academic Board**