KMS 860

Data Protection Policy

(GDPR Privacy Standard)

Appendix A **Personal Data Breach Procedure**

Appendix B **Data Protection Impact Assessment Guidance & Checklist**

Alternative Formats:

If you require this document in an alternative format, please use the following contact information: enquiries@kmc.ac.uk

Created by:	Principal & CEO	Next Review date:	February 2026
Approved by:	The Corporation	Responsibility for Review:	Principal & CEO
Date First approved:	May 2018	Version Control:	V3

TABLE OF CONTENTS

Page

Appendices:

A - Personal Data Breach Procedure
B - Data Protection Impact Assessment

Summary of Changes made between previous issue and current issue	**Page Number**
Full review and revisions to the Policy and Appendix A & B for Open University approval	V3 Full Document

1. INTERPRETATION

1.1. Definitions:

Automated Decision-Making (ADM)	When a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.
Automated Processing	Any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.
College	Kingston Maurward College & Kingston Maurward Enterprises Limited.
College Personnel	All employees, workers [contractors, agency workers, consultants,] directors, members and others.
Consent	Agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller	The person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our College Personnel and Personal Data used in our business for our own purposes.
Data Subject	A living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and have legal rights regarding their Personal Data.
Data Privacy Impact Assessment (DPIA)	Tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.
Data Protection Officer (DPO)	The person required to be appointed in specific circumstances under the GDPR. The College DPO is Mr Jonathan Worth – dpo@kmc.ac.uk
EEA	The 27 countries in the EU, and 30 in the EEA
Explicit Consent	Consent which requires a very clear and specific statement (that is, not just action)
General Data Protection Regulation (GDPR)	The General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

ICO	The Information Commissioner's Office, the UK's data protection regulator.
Personal Data	Any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Category Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
Personal Data Breach	Any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
Privacy by Design	Implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.
Privacy Guidelines	Any College privacy / GDPR related guidelines provided to assist in interpreting and implementing this Privacy Standard and Related Policies.

Privacy Notices or Privacy Policies	Separate notices setting out information that may be provided to Data Subjects when the College collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.
Processing or Process	Any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
Pseudonymisation or Pseudonymised	Replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.
Related Policies	Any College policies, operating procedures or processes related to this Privacy Standard and designed to protect Personal Data.
Special Category Data	Information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation,

biometric or genetic data, and Personal Data relating to criminal offences and convictions.

2. INTRODUCTION

2.1. This Privacy Standard sets out how Kingston Maurward College handle the Personal Data of our students, customers, suppliers, employees, workers and other third parties.

2.2. This Privacy Standard applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

2.3. This Privacy Standard applies to all College Personnel. College Personnel must read, understand and comply with this Privacy Standard when Processing Personal Data on our behalf and attend training on its requirements. This Privacy Standard sets out what we expect from you in order for the College to comply with applicable law. Your compliance with this Privacy Standard is mandatory. Related Policies and Privacy Guidelines may be available to help you interpret and act in accordance with this Privacy Standard. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Privacy Standard may result in disciplinary action.

2.4. This Privacy Standard (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

3. SCOPE

3.1. The College recognises that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The College is exposed to potential fines of up to EUR20 million (approximately £18 million) or

4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

3.2. All Managers are responsible for ensuring all College Personnel comply with this Privacy Standard and need to implement appropriate practices, processes, controls and training to ensure such compliance.

3.3. The DPO is responsible for overseeing this Privacy Standard and, as applicable, developing Related Policies and Privacy Guidelines.

3.4. College Personnel should contact the DPO with any questions about the operation of this Privacy Standard or the GDPR or if they have any concerns that this Privacy Standard is not being or has not been followed. In particular, they must always contact the DPO in the following circumstances:

3.4.1. if they are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the College) (see section 5.1 below);

3.4.2. if they need to rely on Consent and/or need to capture Explicit Consent (see section 5.2 below);

3.4.3. if they need to draft Privacy Notices (see section 5.3 below);

3.4.4. if they are unsure about the retention period for the Personal Data being Processed (see section 9 below);

3.4.5. if they are unsure about what security or other measures you need to implement to protect Personal Data (see section 10.1 below);

3.4.6. if there has been a Personal Data Breach (section 10.2 below);

3.4.7. if they are unsure on what basis to transfer Personal Data outside the EEA (see section 11 below);

3.4.8. if they need any assistance dealing with any rights invoked by a Data Subject (see section 12);

3.4.9. whenever they are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see section 13.4 below) or plan to use Personal Data for purposes others than what it was collected for;

3.4.10. If they plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see section 13.5 below);

3.4.11. If they need help complying with applicable law when carrying out direct marketing activities (see section 13.6 below); or

3.4.12. if they need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see section 13.7 below).

4. PERSONAL DATA PROTECTION PRINCIPLES

4.1. The College adheres to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

4.1.1. Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency)

4.1.2. Collected only for specified, explicit and legitimate purposes (Purpose Limitation)

4.1.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation)

4.1.4. Accurate and where necessary kept up to date (Accuracy)

4.1.5. 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)

4.1.6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against

unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality)

4.1.7. Not transferred to another country without appropriate safeguards being in place (Transfer Limitation)

4.1.8. Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests)

The College is responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability)

5. LAWFULNESS, FAIRNESS, TRANSPARENCY

5.1. Lawfulness and Fairness

5.1.1. Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.1.2. College Personnel may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

5.1.3. The GDPR allows Processing for specific purposes, some of which are set out below:

a. the Data Subject has given their Consent;

b. the Processing is necessary for the performance of a contract with the Data Subject;

c. the processing necessary to comply with our legal obligations;

d. to protect the Data Subject's vital interests;

e. to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

5.1.4. The College must identify and document the legal ground being relied on for each Processing activity.

5.2. Consent

5.2.1. A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

5.2.2. A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are not sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

5.2.3. Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

5.2.4. Unless the College can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Category Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, we must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

5.2.5. The College will need to evidence Consent captured and keep records of all Consents so that the College can demonstrate compliance with Consent requirements.

5.3. Transparency (notifying data subjects)

5.3.1. The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

5.3.2. Whenever the College collects Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

5.3.3. When Personal Data is collected indirectly (for example, from a third party or publicly available source), privacy information must be provided within a reasonable period and no later than one month after receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

5.3.4. If the College changes how it uses Personal Data, the College may need to notify Individuals about the change. If College Personnel intend to change how they use Personal Data they must notify the Data Protection Officer who will decide whether the College Personnel'

6. PURPOSE LIMITATION

6.1. Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

6.2. The College cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

7. DATA MINIMISATION

7.1. Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

7.2. College Personnel may only Process Personal Data when performing their job and the duties of their role require it. You cannot Process Personal Data for any reason unrelated to your job duties.

7.3. College Personnel may only collect Personal Data that they require for their job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

7.4. College Personnel must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the College's data retention guidelines.

8. ACCURACY

8.1. Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

8.2. College Personnel will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

9. STORAGE LIMITATION

9.1. Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

9.2. College Personnel must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

9.3. The College will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with any College guidelines on Data Retention.

9.4. College Personnel will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the College's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

9.5. College Personnel will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

10. SECURITY INTEGRITY AND CONFIDENTIALITY

10.1. Protecting Personal Data

10.1.1. Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

10.1.2. The College will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our

Processing of Personal Data. College Personnel are responsible for protecting the Personal Data they hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Category Data from loss and unauthorised access, use or disclosure.

10.1.3. College Personnel must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

10.1.4. College Personnel must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

a. Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

b. Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

c. Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

10.1.5. College Personnel must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

10.2. Reporting a Personal Data Breach

10.2.1. The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

10.2.2. We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

10.2.3. If College Personnel know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches, or the DPO, or the Executive Assistant to the Principal. You should preserve all evidence relating to the potential Personal Data Breach.

Further guidance can be found in **Appendix A** – **Personal Data Breach Procedure**

11. TRANSFER LIMITATION

11.1. The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

11.2. The College may only transfer Personal Data outside the EEA if one of the following conditions applies:

11.2.1. the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

11.2.2. appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European

Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

11.2.3. the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

11.2.4. the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

12. DATA SUBJECT'S RIGHTS AND REQUESTS

12.1. Data Subjects have rights when it comes to how the College handle their Personal Data. These include rights to:

12.1.1. withdraw Consent to Processing at any time;

12.1.2. receive certain information about the Data Controller's Processing activities;

12.1.3. request access to their Personal Data that we hold;

12.1.4. prevent our use of their Personal Data for direct marketing purposes;

12.1.5. ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

12.1.6. restrict Processing in specific circumstances;

12.1.7. challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

12.1.8. request a copy of an agreement under which Personal Data is transferred outside of the EEA;

12.1.9. object to decisions based solely on Automated Processing, including profiling (ADM);

12.1.10. prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

12.1.11. be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

12.1.12. make a complaint to the supervisory authority; and

12.1.13. in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

12.2. The College must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation)

12.3. College Personnel must immediately forward any Data Subject request you receive to the DPO.

13. ACCOUNTABILITY

13.1. The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

13.2. The College must have adequate resources and controls in place to ensure and to document GDPR compliance including:

13.2.1. appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

13.2.2. implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

13.2.3. integrating data protection into internal documents including this Privacy Standard, Related Policies, Privacy Guidelines, Privacy Notices;

13.2.4. regularly training College Personnel on the GDPR, this Privacy Standard, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The College must maintain a record of training attendance by College Personnel; and

13.2.5. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

13.3. Record keeping

13.3.1. The GDPR requires the College to keep full and accurate records of all our data Processing activities.

13.3.2. The College must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents

13.3.3. These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

13.4. Training and audit

13.4.1. The College is required to ensure all College Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

13.4.2. College Personnel must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

13.4.3. College Personnel must regularly review all the systems and processes under their control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

13.5. Privacy By Design and Data Protection Impact Assessment (DPIA)

13.5.1. The College is required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

13.5.2. The College must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

a. the state of the art;

b. the cost of implementation;

c. the nature, scope, context and purposes of Processing; and

d. the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

13.5.3. Data controllers must also conduct DPIAs in respect to high risk Processing.

13.5.4. The College should conduct a DPIA when implementing major system or business change programs involving the Processing of Personal Data including:

a. use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

b. Automated Processing including profiling and ADM;

c. large scale Processing of Sensitive Data; and

d. large scale, systematic monitoring of a publicly accessible area.

13.5.5. A DPIA must include:

a. a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

b. an assessment of the necessity and proportionality of the Processing in relation to its purpose;

c. an assessment of the risk to individuals; and

d. the risk mitigation measures in place and demonstration of compliance.

13.6. Automated Processing (including profiling) and Automated Decision-Making

13.6.1. Automated Decision-Making happens where the College makes a decision about an Individual solely by automated means; without any human involvements and the decision has legal or other significant effects.

13.6.2. Profiling happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

13.6.3. Any Automated Decision-Making or Profiling which the College carries out can only be done once the College is confident that it is complying with Data Protection Laws. If College Personnel wish to carry out any Automated Decision-Making or Profiling, College Personnel must inform the Data Protection Officer.

13.6.4. College Personnel must not carry out Automated Decision-Making or Profiling without the approval of the Data Protection Officer.

13.6.5. The College does not carry out Automated Decision-Making or Profiling in relation to its employees.

13.7. Direct marketing

13.7.1. The College are subject to certain rules and privacy laws when marketing to our customers.

13.7.2. A Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

13.7.3. The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

13.7.4. A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

13.8. Sharing Personal Data

Prior to sharing any personal data, or entering into any type of data sharing contract, College staff should seek guidance from the Data Protection Officer who will provide guidance to ensure that the College discharges the responsibility in a lawful manner.

13.8.1. Generally, the College are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

13.8.2. College Personnel may only share the Personal Data we hold with another employee, agent or representative of the College if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

13.8.3. The College may only share the Personal Data we hold with third parties, such as our service providers if:

a. they have a need to know the information for the purposes of providing the contracted services;

b. sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

c. the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

d. the transfer complies with any applicable cross border transfer restrictions; and

e. a fully executed written contract that contains GDPR approved third party clauses has been obtained.

14. RELATED POLICIES

KMS 868 Freedom of Information Policy KMS 900 Complaints

KMS 930 Archiving Procedure

Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

Kingston Maurward College's Data Protection Officer (DPO) is:
Mr Jonathan Worth – dpo@kmc.ac.uk

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.

- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people

- The DPO will alert the Principal and the Chair of Governors.

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether

the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way); in case the ICO, or an individual, challenges it later affected by the breach. Documented decisions are stored in a secure location on the college computer system as well as a hard copy stored in a secure filing cabinet.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours.

As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data
  - breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
  - Records of all breaches will be stored in a secure location on the college computer
  - system as well as a hard copy stored in a secure filing cabinet

- The DPO and Principal will meet to review what happened and how it can be prevented from happening again. This meeting will take place as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach that you might want to consider could include:

- Details of student premium interventions for named children being published on the College website

- Non-anonymised student exam results or staff pay information being shared with governors
- A College laptop containing non-encrypted Special Category data being stolen or hacked
- The College's cashless payment provider being hacked, and parents' financial details stolen

Guide to completing a Data Protection Impact Assessment (DPIA)

A DPIA is a process, which helps an organisation to identify and reduce the privacy risks to individuals whose personal information is used in a project. The General Data Protection Regulation (GDPR) requires a legal requirement to carry out a DPIA where the use of the personal information is likely to result in a **high** risk to the privacy of individuals.

Examples might include use of new technologies, including proposals to use cloud storage facilities for college information, use of software that uses details from the MIS database, use of CCTV and biometrics, such as fingerprint scanning.

A DPIA can be used to help you to design more efficient and effective ways for handling personal data, minimise privacy risks to the individuals affected and financial and reputational impact of a data incident on the College.

This guide is intended to help you assess whether a DPIA is needed, identify levels of risk of personal data for your project and complete a DPIA report (where applicable), which will need to be agreed and approved by the Data Protection Officer

When to carry out a DPIA

A DPIA must be completed when the project is likely to involve Processing of personal data that may involve a high risk to the privacy of individuals. The DPO must be consulted at the outset of a project / initiative to ensure a DPIA has not been missed.

When to start a DPIA

If you are thinking about starting a project or making changes to existing services/ systems, then you should consider whether a DPIA is necessary from an early stage.

A DPIA must start at the project initiation stage, continued throughout the life of the project and re-visited in each new project phase, for example, when you want to use

the personal data for a new or additional purpose for the use of the data, or if you are collecting new personal data.
This should be proportionate to the level of special category data being collected or processed because of the project.

It is important to start at an early stage of the process to allow time to resolve issues and mitigate for any risks identified, in order to avoid the difficulties of having to address these points late in the project when other decisions have already been made.

How to carry out a DPIA

Use the checklist below to help you decide whether the project involves privacy risks, identify what they are and work out what steps you will need to take to minimise those risks as far as possible.

When you have considered all of the risks, you should conclude about anything you could do to eliminate or minimise the risks you have identified. Some examples might include:

- Minimising the risks of collecting too much personal information on CCTV by siting and angling the cameras so that they are focussed only on perhaps the car park rather than on an area where students congregate, or the entrance door of a building not into an office.
- Checking the questions, you have asked on a form before you send it out and ensuring that you really need all of the personal information you have requested.
- If you need to store personal information on paper records ensuring that you keep them in a secure location, which cannot be readily, accessed by unauthorised individuals.
- Ensuring all staff are instructed to lock their computer screen if they leave it unattended for any length of time.

When you have recorded all of these points and how you will address the risks, you should get it signed off, by the Data Protection Officer.

If the Data Protection Officer is completing the form, the Principal & CEO should sign this off.
A copy will be kept by the Data Protection Officer to refer back to for audit purposes and for updating if, the project is changed or extended in future.

Completing a DPIA

When you have completed the DPIA, considered any risks and mitigated them wherever possible, the college will need to decide whether to accept any remaining risks. It is good practice to document what risks were identified, what steps were taken to minimise them and what risks were accepted.

Checklist

Once the form has been completed, it must be returned to the Data Protection Officer as soon as possible.

The project **will not** start/go ahead until this form has been returned and signed off by the Data Protection Officer.

If the Data Protection Officer is completing this form, the Principal (or appropriate delegate) must sign it off.

Do not hesitate to contact the Data Protection Officer, if you have any queries relating to completing this checklist.

Please note, this form must be completed and returned via dpo@kmc.ac.uk

Paper copies and forms submitted by another means **will not** be accepted.

Project Name:	
Brief description of the project:	
STEP ONE : IDENTIFY THE NEED FOR A DPIA	
Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.	
STEP TWO : DESCRIBE THE PROCESSING	
Describe the nature of the processing: How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?	
Describe the scope of the processing: What is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?	
Describe the context of the processing: What is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws?	

Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?	
Describe the purposes of the processing: What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?	
STEP THREE : CONSULTATION PROCESS	
Consider how to consult with relevant stakeholders: Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?	
STEP 4 : ASSESS NECESSITY AND PROPORTIONALITY	
Describe compliance and proportionality measures, in particular: What is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?	

STEP FIVE : INDENTIFY AND ASSESS RISKS			
Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	**Likelihood of harm**	**Severity of harm**	**Overall Risk**
	Remote, possible or probable	**Minimal, significant or severe**	**Low, medium or high**

STEP SIX : INDENTIFY MEASURES TO REDUCE RISK				
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect of Risk** Eliminated Reduced Accepted	**Residual Risk** Low Medium High	**Measure Approved** Yes No

STEP SEVEN : SIGN OFF AND RECORD OUTCOMES		
Item	**Name / Position / Date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual Risks approved by:		If accepting any residual high risk, consult ICO before going ahead
DPO Advice Provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO Advice Accepted by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individual's views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO will also review ongoing compliance with the DPIA

1	What is the project? What does it seek to achieve?	
2	Will the project collect data about individuals? If YES, whom? If NO, a DPIA will not be required. The form should still be submitted, but the rest of the form can be left blank but signed off.	
3	What type of information will it collect? Will it be special category data?	
4	How will the information be collected? Paper? Electronically?	
5	Who will have access to this information? How will it be kept stored and secured?	
6	How will individuals be made aware of how their personal information is being used?	
7	Do you need consent from the individual to use the information? i.e. if special category data is being collected.	
8	Does the project involve the use of new technology, which could be privacy intrusive? i.e. CCTV, biometrics, GPS and / or Cloud storage.	
9	What risks have been identified? What steps have been taken to minimise them?	
Signature		
Name		
Position		
Date		