Data Management Policy

Signing off requirements:

	Date		Author:
Executive	March 2019		Stuart Barlow
Relevant Union(s)	n/a		Vice-Principal – Curriculum & Quality
Corporation	March 2019		
Equality & Diversity Committee (where relevant)	n/a		

	Date
Date of Policy Writing	March 2019
Date of Policy Adoption	March 2019
Planned Date of Review	June 2019

Kensington & Chelsea College Data Management Policy

Purpose

This guidance note sets out the following procedures under the Kensington and Chelsea College Data Management Policy. Through doing so it explains how the College will discharge its obligations in relation to the General Data Protection Regulations.

The procedures include:

- Individual Rights (Sections A to H)
- Contracts (Section I)
- Documentation – Information Asset Register (Section J)
- Data Sharing Agreement – Local Authorities (Section K)
- Data Protection Impact Assessments (Section L)
- Data Breach Policy (Section M)

Appendices:

- KCC Privacy Notice (students and other stakeholders)
- KCC Privacy Notice (job applicants)
- KCC Privacy Notice (Staff)
- Process for handling Individual Rights requests
- Data Sharing Agreement for Local Authorities
- Data Breach Investigation Form
- Data Retention Policy
- Complaints (and other Feedback) Policy

Queries about the procedures should be forwarded to the Data Protection Officer, or to the Quality & Sub-Contracts Administrator for investigation through the College's Complaints (and other Feedback) Policy.

Section A: Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. The College will meet the right to be informed as follows:

KCC will provide individuals with information including: the purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with. This is called 'privacy information' (see KCC Privacy Notice and information which is set out at Appendix 1)
We will provide privacy information to individuals at the time that we collect an individual's personal data from them. The privacy information will be included in the enrolment form for students.
Where we obtain personal data from other sources, we will provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month. If we

obtain personal data from a source other than the individual it relates to, we provide them with privacy information:

- within a reasonable of period of obtaining the personal data and no later than one month;
- if we plan to communicate with the individual, at the latest, when the first communication takes place; or
- if we plan to disclose the data to someone else, at the latest, when the data is disclosed.

There are a few circumstances when we will not provide privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.

We will provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language. We will ask for feedback on how effective the delivery of our privacy information is.

We will regularly review, and where necessary, update the privacy information on an annual basis in line with the publication of government advice to FE sector. We will bring any new uses of an individual's personal data to their attention before we start the processing.

Section B: Right to access

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. The College will meet the right to access as follows:

- Individuals will have the right to obtain:
- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in the KCC Privacy Notice.

The College will not generally charge for a Subject Access Requests. However, we may charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. We may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that we will charge for all subsequent access requests. The fee will be based on the administrative cost of providing the information.

An individual can make a request verbally or in writing. Staff members receiving a request verbally will log the details of the request and forward the request to the Data Protection Officer

Details of the process for making a request including ID verification, timescales, fees and refusing requests are included at Appendix 2

In line with the Privacy Notice, the College only holds data relating to an individual's enrolment. We may ask the individual to specify the information their request relates to in order provide the information requested.

Section C: Right of rectification

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data. The College will meet the right to rectification as follows:

An individual can make a request verbally or in writing. Staff members receiving a request verbally will log the details of the request and forward the request to the Compliance Manger.

Details of the process for making a request including ID verification, timescales, fees and refusing requests are included at Appendix 2

Where the College receives a request for rectification, it will take reasonable steps to satisfy itself that the data is accurate and to rectify the data if necessary. The College will take into account the arguments and evidence provided by the data subject. The College may wish to check with the requester that it has understood the request, as this can help avoid later disputes about how the College has interpreted the request. The College will keep a log of verbal requests.

What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort you should put into checking its accuracy and, if necessary, taking steps to rectify it. For example, we will make a greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones.

We will also take into account any steps we have already taken to verify the accuracy of the data prior to the challenge by the data subject.

The College may refuse a request and it is aware of the information we need to provide to individuals when we do so.

Determining whether personal data is inaccurate can be more complex if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is, in itself, accurate and should be kept. In such circumstances the fact that a mistake was made and the correct information should also be included in the individual's data. The GDPR does not give a definition of the term accuracy. However, the Data Protection Bill states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

It is also complex if the data in question records an opinion. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified.

An individual has the right to request restriction of the processing of their personal data where they contest its accuracy and the College is checking it. As a matter of good practice, the College will

restrict the processing of the personal data in question whilst it is verifying accuracy, whether or not the individual has exercised their right to restriction.

Where the College is satisfied that the data is accurate, we will let the individual know that we are satisfied that the personal data is accurate, and tell them that we will not be amending the data. The College will explain the decision, and inform the individual of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy. The circumstances in which the College may extend the time to respond may include further consideration of the accuracy of disputed data - although the College may only do this in complex cases - and the result may be that at the end of the extended time period you inform the individual that you consider the data in question to be accurate.

If the College has disclosed the personal data to other organisations, we will contact each recipient and inform them of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, we will also inform the individual about these recipients.

The GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Section D: Right to erasure

Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances. The College will meet the right to erasure as follows:

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for;
- we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;
- we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- we are processing the personal data for direct marketing purposes and the individual objects to that processing;
- we have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- we have to do it to comply with a legal obligation; or
- we have processed the personal data to offer information society services to a child.

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the GDPR. Therefore, if we process data collected from children, we

should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent.

An individual can make a request verbally or in writing. Staff members receiving a request verbally will log the details of the request and forward the request to the Data Protection Lead. Details of the process for making a request including ID verification, timescales, fees and refusing requests are included at Appendix 2.

The GDPR specifies two circumstances where we should tell other organisations about the erasure of personal data:

- the personal data has been disclosed to others; or
- the personal data has been made public in an online environment (for example on social networks, forums or websites).

If the College has disclosed the personal data to others, we must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, we will also inform the individuals about these recipients.

The GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Where personal data has been made public in an online environment, reasonable steps should be taken to inform other controllers who are processing the personal data to erase links to, copies or replication of that data. When deciding what steps are reasonable you should take into account available technology and the cost of implementation.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or

- if the processing is necessary for the purposes of preventative or occupational medicine (eg where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

We will also provide this information if we request a reasonable fee or need additional information to identify the individual.

Section E: Right to restrict data

Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data. The College will meet the right to restrict data as follows:

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.

Individuals have the right to request you restrict the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their personal data and you are verifying the accuracy of the data;
- the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- you no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data under Article 21(1), and you are considering whether your legitimate grounds override those of the individual.

The right to restrict data is distinct from the right to rectification and the right to object, there are close links between those rights and the right to restrict processing:

- if an individual has challenged the accuracy of their data and asked for you to rectify it (Article 16), they also have a right to request you restrict processing while you consider their rectification request; or

- if an individual exercises their right to object under Article 21(1), they also have a right to request you restrict processing while you consider their objection request.

As a matter of good practice the College will automatically restrict the processing whilst it is considering its accuracy or the legitimate grounds for processing the personal data in question.

An individual can make a request verbally or in writing. Staff members receiving a request verbally will log the details of the request and forward the request to the Data Protection Officer.

Details of the process for making a request including ID verification, timescales, fees and refusing requests are included at Appendix 3.

The College will take action to restrict personal data if required. It is important to note that the definition of processing includes a broad range of operations including collection, structuring, dissemination and erasure of data. Therefore, we will use methods of restriction that are appropriate for the type of processing we are carrying out.

The GDPR suggests a number of different methods that could be used to restrict data, such as:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website.

The College will consider how it stores personal data that is no longer needed to process but the individual has requested is restricted (effectively requesting that the College does not erase the data).

Where we are using an automated filing system, we will use technical measures to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. We will also note on your system that the processing of this data has been restricted.

The College will not process the restricted data in any way except to store it unless:

- we have the individual's consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest.

If the College has disclosed the personal data in question to others, we will contact each recipient and inform them of the restriction of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, the College will also inform the individual about these recipients.

In many cases the restriction of processing is only temporary, specifically when the restriction is on the grounds that:

- the individual has disputed the accuracy of the personal data and you are investigating this; or
- the individual has objected to you processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of your legitimate interests, and you are considering whether your legitimate grounds override those of the individual.

Once the College has made a decision on the accuracy of the data, or whether your legitimate grounds override those of the individual, you may decide to lift the restriction.

If we do this, the College will inform the individual before you lift the restriction. As noted above, these two conditions are linked to the right to rectification (Article 16) and the right to object (Article 21). This means that where the College is informing the individual that you are lifting the restriction (on the grounds that you are satisfied that the data is accurate, or that our legitimate grounds override theirs) we will also inform them of the reasons for our refusal to act upon their rights under Articles 16 or 21. The College will also inform the individual of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek a judicial remedy.

Section F: Right to data portability

The College will meet the right to data portability as follows:

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.

It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- here the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

The College will provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information will be provided free of charge.

If the individual requests it, we may transmit the data directly to another organisation if this is technically feasible. However, the College is not required to adopt or maintain processing systems that are technically compatible with other organisations.

If the personal data concerns more than one individual, the College will consider whether providing the information would prejudice the rights of any other individual.

The College will respond without undue delay, and within one month. This may be extended by two months where the request is complex or the College receives a number of requests. We will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where the College is not taking action in response to a request, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Section G: Right to object

Individuals have the right to object to the manner in which the College fulfils its obligations for data processing. The College will meet the right to object as follows:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Individuals must have an objection on “grounds relating to his or her particular situation”.

The College will stop processing the personal data unless:

- it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

We inform individuals of their right to object “at the point of first communication” which is the College Enrolment Form and in the KCC Privacy Notice.

This right will be “explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information”.

The College will stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.
We will deal with an objection to processing for direct marketing at any time and free of charge.

Individuals must have “grounds relating to his or her particular situation” in order to exercise their right to object to processing for research purposes.

Where the College is conducting research where the processing of personal data is necessary for the performance of a public interest task, we may not comply with an objection to the processing.

The College will provide way for individuals to object online through its website.

Section H: Rights related to automated decision making

The College will meet the rights related to automated decision making as follows:

The GDPR has provisions on automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The GDPR applies to all automated individual decision-making and profiling. Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.

The College will only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent.

The College does not undertake processing that falls under the category of automated decision making.

Section I: Contracts

The College will meet the requirements for contracts as follows:

The GDPR makes written contracts between controllers and processors a general requirement, rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures) under the DPA.

The GDPR allows for standard contractual clauses from the EU Commission or a supervisory authority (such as the ICO) to be used in contracts between controllers and processors. No standard contractual clauses have been issued by the EU or ICO. The College has been provided with its own legal advice on standard clauses.

The GDPR envisages that adherence by a processor to an approved code of conduct or certification scheme may be used to help controllers demonstrate that they have chosen a suitable processor. Standard contractual clauses may form part of such a code or scheme, though again, no schemes are currently available.

The GDPR gives processors responsibilities and liabilities in their own right, and processors as well as controllers may now be liable to pay damages or be subject to fines or other penalties.
Whenever a controller uses a processor (a third party who processes personal data on behalf of the controller) it needs to have a written contract in place. Similarly, if a processor employs another processor it needs to have a written contract in place. Contracts between controllers and processors ensure that they both understand their obligations, responsibilities and liabilities. They help them to comply with the GDPR, and help controllers to demonstrate their compliance with the GDPR. The use of contracts by controllers and processors may also increase data subjects' confidence in the handling of their personal data.

Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller.

The College will identify all contracts where it is either the controller or processor. The Compliance Manager will retain a log of these contracts and their nature. The College will maintain a Contracts Log.

Where the College is the data controller, it will ensure that contracts will include as a minimum the following terms, requiring the processor to:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

A processor must only act on the documented instructions of a controller. If a processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.

Where the College is the data processor, it will ensure that it meets contractual obligations to the controller, under the GDPR a processor also has the following direct responsibilities:

- not to use a sub-processor without the prior written authorisation of the data controller;
- to co-operate with supervisory authorities (such as the ICO);

- to ensure the security of its processing;
- to keep records of processing activities;
- to notify any personal data breaches to the data controller;
- to employ a data protection officer; and
- to appoint (in writing) a representative within the European Union if needed.

If a processor fails to meet any of these obligations, or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.

If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.

Section J: Documentation – Information Asset Register

The documentation of processing activities is a new requirement under the GDPR. We are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention; we call this documentation.

The College will meet the requirements for documentation as follows by documenting our processing activities, we are able to meet a legal requirement, but also support good data governance and demonstrate compliance with other aspects of the GDPR.

Controllers and processors each have their own documentation obligations. As the College has 250 or more employees, it will document all processing activities.

The College will maintain an Information Asset Register which is the documentation log.

Section K: Data Sharing with Local Authorities

Under the Education and Skills Act 2008, Local Authorities have a duty to track participation of all 16 to 17 year olds resident in their area, and to make arrangements for those not in education or training. In some cases, the Local Authority commission a 3rd party to help fulfil their duties on their behalf.

The College is required to share data with each home Local Authority in order for them to fulfil these duties, if an individual falls into one or more of the following categories:

- 16 to 17 years of age
- a vulnerable adult in care of the Local Authority or previously in care of the Local Authority 18-24 years old with an Education Health Care Plan (EHCP).

The Data Sharing Agreement is set out at Appendix 4.

Section L: Data Protection Impact Assessments

The College will meet the requirements for the Data Protection Impact Assessment (DPIA) requirement as follows:

A DPIA is a process to systematically analyse the College processing and help it identify and minimise data protection risks. We will:

- describe the processing and the purposes;
- assess necessity and proportionality;
- identify and assess risks to individuals; and
- identify any measures to mitigate those risks and protect the data.

The College does not expect to eradicate the risk, but the process should help to minimise risks and consider whether or not they are justified.

The College will complete a DPIA for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability more generally and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

The College will include DPIA as part of its Corporate Risk Management Process. The Risk Register will include any data processing risk that are considered to be 'High Risk'. These risks will be reported through the Risk Management and Board Assurance Process.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – whether physical, material or non-material - to individuals or to society at large.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It should look at risk based on the specific nature, scope, context and purposes of the processing.

We will conduct a DPIA before we begin any type of processing which is "likely to result in a high risk". This means that although the actual level of risk has not been assessed yet, we will screen for factors which point to the potential for a widespread or serious impact on individuals.

In particular, the GDPR indicated that the College will do a DPIA if it plans to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires the College to do a DPIA where we plan to:

- use new technologies;

- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

The College will also consider doing a DPIA for any other processing which is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

Section M: Data Breach Policy

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority, the Information Commissioners Office (ICO), within 72 hours of becoming aware of the breach, where feasible. Recital 87 of the GDPR makes clear that when a security incident takes place, Kensington & Chelsea College (KCC) should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, KCC must also inform those individuals without undue delay.

KCC have a legal duty to keep a record of any personal data breaches, regardless of whether we are required to notify.

<u>Personal data</u>

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data is defined as:

''data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller."

Where a personal data breach has occurred KCC will assess the likelihood and severity of the resulting risk to people's rights and freedoms. This will include consideration of whether this breach will result in result in:

"physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

Reporting a breach

All personal data breaches, whether suspected or confirmed, must be reported by the member of staff to the College Data Protection Officer (DPO) without delay.

Staff must follow the following three steps:

Step one: Report the breach to the DPO - Data breaches should be reported via telephone; to ensure any required action can be taken at the earliest opportunity.

Step Two: Send a breach notification report to the DPO - a summary email must be sent within one hour of the call to dpo@kcc.ac.uk

The email will be referred to as the 'breach notification report'. The breach notification report must include (as a minimum):

- date and time of the breach (if known)
- who reported the breach, if different to the person sending the email
- nature of the breach e.g. theft, loss or damage
- a description of the personal data involved (without identifiers)
- The type and number of persons impacted e.g. 10 students
- Any corrective action(s) taken

Step Three: Take no further action - Once the breach is reported, no further action should be taken by the staff member unless they are requested to do so by the DPO. The DPO will assume responsibility from this point forward.

Data Breach Investigation form (DPO)

The Data Breach Investigation form must be completed by the DPO, or a nominated Data Protection specialist.

The purpose of the Investigation form is to document the circumstances of the breach, what actions have been taken and what recommendations have been made.

The objective of any breach investigation is to identify what actions the organisation needs to take to alleviate any risks to individuals, to prevent a recurrence of the incident and to determine whether the incident needs to be reported to the ICO.

In all cases the DPO will act as the point of contact for the ICO.

Appendix 5 provides a copy of the Data Breach Form.

Appendix 1 – KCC Privacy Notice (students and other stakeholders)

Introduction

Kensington & Chelsea College (the College) is required to collect personal data from its customers whom it defines as "If you contact us for any reason, or you are affected by anything we do, you are one of our customers".

This privacy notice details how we collect your data, what we use it for, what actions you can take if you wish to access your data and how to make changes to the way we are using it.

How we use your data

The data you provide us will only be used by the College for purposes relating to:

- your education and training
- employment
- advice and well-being
- marketing and research

You will be asked to provide personal information about yourself in order to enquire, apply and / or enrol to one of our courses or access our services.

At the point of collecting this data we always aim to clearly explain what it is going to be used for and who we may share it with.

Unless required or permitted by law, we will always ask you before we use it for any other reason. We would only use it for marketing with your prior consent.

Any sensitive personal information will never be supplied to anyone outside the College without first obtaining your consent, unless required or permitted by law.

The basis for collecting data and your rights

Most of the data we collect from you is essential for your enrolment as a student in order to access funding, or is required by law. You must provide the data in order to enrol with us and we will make this clear at time of enrolment.

Other data is collected on your consent, and you may withdraw this consent without this affecting your status as a student.

You have a variety of rights about the way we process your data:

- You can request a copy of the data we hold about you
- You may change or stop the way in which we communicate with you
- You may change or stop us processing data about you, if it is not required for the purpose you originally provided it

If you are not satisfied with the way we have processed your data, then you can complain to the Office of the Information Commissioner (ICO)

More information about your rights can be found on the ICO website here https://ico.org.uk/
Government and funding Agencies

We are required to share your data with certain Government and funding agencies in order to meet our contractual and legal obligations, specifically the Education and Skills Funding Agency (ESFA) and the Office for Students (OFS).

The ESFA will share your data with the Department for Education (DfE) and the European Social Fund (ESF) Managing Authority.

Further information can be found here:

ESFA https://www.gov.uk/government/publications/esfa-privacy-notice
OFS https://www.officeforstudents.org.uk/privacy/

Local Authorities

Under the Education and Skills Act 2008, Local Authorities have a duty to track participation of all 16 to 17 year olds resident in their area, and to make arrangements for those not in education or training. In some cases, the Local Authority commission a 3rd party to help fulfil their duties on their behalf.

The College is required to share your data with your Local Authority in order for them to fulfil these duties, if you fall into one or more of the following categories:

- 16 to 17 years of age
- a vulnerable adult in care of the Local Authority or previously in care of the Local Authority
- 18-24 years old with an Education Health Care Plan (EHCP).

How long do we keep your data

We will keep your data for as long as is needed to complete the task for which it was collected. The College Data Retention Policy sets out the specific retention periods for your personal data and this can be found on the College website.

How we keep your data safe

The College takes data security very seriously and has a number of robust systems in place to keep your information secure.

These include a range of physical, technical and organisational security measures, such as access control, an encrypted network and secure storage.

The College has a number of internal policies of which staff and our partners are required to follow, with training and awareness-raising activities undertaken to promote compliance with data protection legislation.

Data protection procedures are regularly reviewed and the College maintains an Information Asset Register of all key personal data; its business purpose, location and how it is secured.

What the Colleges does if you are concerned about its practices

Contact us If you have any questions about this privacy statement or how we communicate with you, please contact:

Data Protection Officer:
Stuart Barlow
Vice-Principal, Curriculum & Quality
Kensington & Chelsea College, Wornington Road, W11 0QQ
dpo@kcc.ac.uk

To implement the College's Complaints (and other Feedback) Policy)

Quality & Sub-Contracting Officer
Shorla Leo
Kensington & Chelsea College, Wornington Road, W11 0QQ
s.leo@kcc.ac.uk

The information in this privacy statement is correct at 30th March 2019 and supersedes all previous versions

Appendix 2 - Privacy Notice for Kensington and Chelsea College Job Applicants

Data controller: Kensington and Chelsea College**, Kensington Centre:** Wornington Road, W10 5QQ**; Chelsea Centre:** Hortensia Road, London, SW10 0QS

Email: DPO@kcc.ac.uk

As part of any recruitment process, Kensington and Chelsea College collects and processes personal data relating to job applicants. Kensington and Chelsea College is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does Kensington and Chelsea College collect?

The organisation collects a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements;
- whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process;
- information about your entitlement to work in the UK;
- identification to be able to complete a DBS application and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health, and religion or belief;
- clarifying whether you are related to an employee or governor to ensure fair recruitment.

Kensington and Chelsea College collects this information in a variety of ways. For example, data might be contained in application forms, CVs, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment, including selection tests.

Kensington and Chelsea College will also collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks. Unless specifically stated, Kensington and Chelsea College will seek information from third parties only once a job offer to you has been made and will inform you that it is doing so.

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

Why does Kensington and Chelsea College process personal data?

Kensington and Chelsea College needs to process data to take steps at your request prior to entering into a contract with you. It also needs to process your data to enter into a contract with you.

In some cases, Kensington and Chelsea College needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

Kensington and Chelsea College has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the organisation to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. Kensington and Chelsea College may also need to process data from job applicants to respond to and defend against legal claims.

Where the Kensington and Chelsea College relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

Kensington and Chelsea College processes health information if it needs to make reasonable adjustments to the recruitment process for candidates who have a disability. This is to carry out its obligations and exercise specific rights in relation to employment.

Where Kensington and Chelsea College processes other special categories of data, such as information about key characteristics such as ethnic origin, sexual orientation or religion/ belief, this is for equal opportunities monitoring purposes.

Kensington and Chelsea College is obliged to seek information about criminal convictions and offences. Where Kensington and Chelsea College seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.

Kensington and Chelsea College will not use your data for any purpose other than the recruitment exercise for which you have applied.

Who has access to data?

Your information may be received through a recruitment website for example FE Jobs, your data is protected by their privacy statement.

Your information will be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

Kensington and Chelsea College will not share your data with third parties, unless your application for employment is successful and it makes you an offer of employment. The organisation will then share your data with former employers to obtain references for you, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.

The organisation will not transfer your data outside the European Economic Area.

How does Kensington and Chelsea College protect data?

Kensington and Chelsea College takes the security of your data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties. The recruitment portal is an external portal secure through password controls. Personal details are accessed by HR only, all other data is anonymised. The Recruitment Policy and Recruitment of Ex-Offenders Policy has details of process to follow.

For how long does Kensington and Chelsea College keep data?
If your application for employment is unsuccessful, Kensington and Chelsea College will hold your data on file for 6 months after the end of the relevant recruitment process. At the end of that period, your data is deleted or destroyed.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. The periods for which your data will be held will be provided to you in a new privacy notice.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing; and
- ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact the Data Protection Officer at dpo@kcc.ac.uk or by visiting/calling the College. You can make a subject access request by completing the Kensington and Chelsea College's Subject Access Request Form

If you believe that Kensington and Chelsea College has not complied with your data protection rights, you can complain to us by contacting the Quality & Sub-Contracting Officer, Shorla Leo, who will provide you with the Complaints (and other Feedback) Policy. If you remain unsatisfied by our response you may complain to the Information Commissioner.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to the organisation during the recruitment process. However, if you do not provide the information, Kensington and Chelsea College may not be able to process your application properly or at all.

You are under no obligation to provide information for equal opportunities monitoring purposes and there are no consequences for your application if you choose not to provide such information.

The information in this privacy statement is correct at 30th March 2019 and supersedes all previous versions

Appendix 3 - Individuals' right to have personal data erased.

Introduction

The right to erasure is also known as 'the right to be forgotten' you may tell us verbally or in writing that you wish us to remove your data.

We will respond within one month to confirm

- Which information we have removed
- Which information we are unable to remove (and the reasons why)
- What else we have done (e.g. to communicate with third parties to whom your data has been shared)

Telling Us you wish to exercise your rights under GDPR

1. By telling a member of staff
2. By writing to the Data Protection Officer

When communicating with us you must provide

1. Details of your engagement with the College (e.g. course studied, dates studied)
2. Proof of Identification (e.g. Passport, Driving Licence)

What we will do

1. Respond to your request within ten working days of your request
2. Confirm our actions within one calendar month of your request

When might we not be able to comply with your right to erasure?

The College has identified the following reasons applicable to our work where the right to erasure does not apply (or may not be fully exercised), specifically if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims
- it is manifestly unfounded or excessive (e.g. if we consider the request to be repetitive in nature)

Further details are available on the College website by reference to our

College Privacy Notices
Data Retention Policy
Complaints (and other Feedback) Policy

Appendix 4 – Data Sharing Agreement

Appendix 5

KENSINGTON AND CHELSEA COLLEGE

Data Breach Report Form

Name:
Daytime telephone number:
Email:
Address:
Before completing this form you must: 1. **Report the breach to the DPO** - Data breaches should be reported via telephone (Current number 07921 485233) to ensure any required action can be taken at the earliest opportunity. 2. **Send a breach notification report to the DPO** - a summary email must be sent within one hour of the call to dpo@kcc.ac.uk Please title the 'breach notification report' and attach a copy of this form with Page 2 completed as fully as possible 3. **Take no further action** - Once the breach is reported, no further action should be taken by the staff member unless they are requested to do so by the DPO. The DPO will assume responsibility from this point forward.

Please complete the form overleaf with as much detail as possible

Date and time of the breach (if known)?	
Who reported the breach (if different to the person completing this form)?	
What is the nature of the breach (e.g. theft, loss or damage)?	
What personal data is involved (without identifiers)?	
What type of people are likely to be affected (and how many?)	
What corrective action(s) has already been taken?	
Please return this form to the Data Protection Officer (dpo@kcc.ac.uk). If you do not receive acknowledgement of receipt within two hours please contact the PA to the Executive.	
Reporting Staff signature:	
Date:	