Data Protection Policy and Procedures

Author	Data Protection Officer
Date	January 2022
Person Responsible	Data Protection Officer
Approval/ review bodies	SLT/JNC/Corporate Board
Frequency of Review*	36 months

Policies will be reviewed more frequently if legal changes or good practice require

Review History:		
Date of review	**Reviewed by**	**Reason for review**
January 2011	Compliance & Policy Manager	Title Change of person responsible
March 2011	Vice Principal	New document
September 2011	Vice Principal	Changes in titles Guidance C (contacts)
May 2012	Vice Principal	Good practice
October 2013	Deputy Principal	Good practice and change of Data Protection Officer
October 2014	HR Manager	New document
January 2016	HR Manager	Minor revisions to Archiving
June 2018	DPO and External Consultant	Review in light of GDPR
January 2022	DPO	Organisational changes

Contents

Links to other Policies and procedures:

Freedom of Information Policy

IT Conditions of Use Policy

Mobile Device and Communications Policy

Staff Code of Conduct

Staff Disciplinary policy and procedure (Conduct**)**

1. Introduction

North Kent College ("the College") needs to keep certain information (computer or paper based) about its employees, students and other stakeholders to allow it to monitor such areas as performance, achievements and health and safety. It is also necessary to process the information so that the College meets all legal obligations to its funding bodies and government agencies.

This policy highlights the key issues relating to data protection and the College. It is intended to provide guidance for College employees, all of whom have an important role in ensuring the legislation is adhered to.

All employees and students must comply with the College's policies and procedures relating to data protection. In depth guidance for employees and students can be found in Appendices 3, 4 and 5.

This policy aims to ensure that the College complies with its legal requirement in the handling of personal information. UK Data Privacy legislation* (the Legislation) specifies six principles (see section 2) which must be observed by all employees, students or others dealing with personal data* on behalf of the College. Any digital, computer and manual records, including filing systems, employee files, Human Resource Information System ("HRIS"), Management Information Systems ("MIS") the electronic Document Management System and student trackers are all covered.

The GDPR imposes a 'privacy by design' requirement with the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that privacy and protection of data is not an after-thought.

The College's obligations to meet the legislation will mean ALL employees, students or others dealing with personal data must follow the principles of Data Protection by Design and Default:

1.1. this means everyone should consider data protection in all their dealings and ensure that the data the College takes or holds is kept secure (data by design); and

1.2. that the College only takes and holds data or information it actually needs for the purpose required (data by default).

Terms marked with an asterisk are defined in Appendix 1.

Although this policy concentrates on the UK data privacy legislation (the Legislation) Appendix 2 identifies other associated legislation.

2. Key Principles relating to the use of Data

The College is required to adhere to the six principles of data protection as laid down in the GDPR Article 5(1), which means that information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The six principles are:

a) Personal data shall be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').
b) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes. Further processing for archiving, scientific or historical research or statistical purposes is permissible ('purpose limitation')
c) Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed ('data minimisation').
d) Personal data shall be accurate and where necessary kept up to date ('accuracy').
e) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose ('storage limitation').
f) Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Article 5(2) requires that the College shall be responsible for, and be able to demonstrate compliance with the six principles outlined in Article 5(1) ('accountability').

The College and all staff who process or use any personal information must ensure that they follow these principles at all times.

3. Special Category Data

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details.

The Appropriate Policy Document in Appendix 7 identifies the special categories of data processed, the Schedule 1 conditions from the Data Protection Act 2018 used and the procedures in place to ensure compliance with the GDPR data protection principles.

Special category data is personal data revealing:

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

UK Data Privacy legislations requires additional protection and security measures for special personal data over and above that given to other personal data. Whenever any special category data is to be shared or taken the security of how this is shared or moved needs to be carefully considered to ensure any risks are mitigated. Any doubts about the security measures for sharing special data should be discussed with IT department beforehand.

Additionally, all staff need to be aware that the use (processing) of special category data is prohibited UNLESS at least one of the conditions below is met:

3.1 the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

3.2 processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;

3.3 processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

3.4 processing is carried out in the course of its legitimate activities with appropriate safeguards* by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body;

3.5 processing relates to personal data which are manifestly made public by the data subject;

3.6 processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

3.7 processing is necessary for reasons of substantial public interest;

3.8 processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;

3.9 processing is necessary for reasons of public interest in the area of public health, such as 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; and/or

3.10 processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

The College has identified special data currently used and recognise that in the majority of instances this data will be processed without consent under the permissible exceptions listed above.

For more details of the processing of special category data please refer to the College Data Processing Register.

4. The Data Protection Officer ("DPO")*

The College has appointed a DPO as necessary under UK data privacy legislation.

The role of the DPO is to ensure the College meets its legal obligations for data privacy and provides independent guidance to employees, students or others dealing with personal data.

The role is a protected position to assess the risk to the data subjects in both data privacy and data protection and will be the College focal point for any data subjects and the UK Regulator; the Information Commissioners Office (the "ICO") and the College.

Whilst the DPO assumes the legal responsibility for the College compliance, the College still has the overall responsibility to be compliant with the Legislation. The DPO will deal with day-to-day matters relating to data subjects (with the support of the Senior Leadership Team.

Failure to comply with the legislation renders the College liable for penalties. In the case of an organisation like the College, an employee as well as the organisation may be liable for prosecution.

5. Notification of Data Held and Processed

The College undertakes to maintain an accurate and timely notification of its data processing activities with the ICO and is required to register this annually. Copies of registration are available from the DPO.

Maintenance of the notification is the responsibility of the DPO.

Additionally the College is required to maintain a separate register of all its Processing activities indicating:

5.1 the purpose of the processing;

5.2 the categories of data processed;

5.3 the recipients of the processed data;

5.4 the third parties with whom data is shared;

5.5 the lawful basis for the processing;

5.6 where the data is shared with third countries;

5.7 how long the data is kept; and

5.8 how it is secured.

If you would like to see the College Processing Register please contact the DPO.

6. Legal Basis of Processing

In order for it to be legal and appropriate for the College to process personal data at least one of the following conditions must be met:

a) The data subject has given his or her consent
b) The processing is required due to a contract
c) It is necessary due to a legal obligation
d) It is necessary to protect someone's vital interests (i.e. life or death situation)

e) It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
f) It is necessary for the legitimate interests of the controller or a third party and does not interfere with the rights and freedoms of the data subject (this condition cannot be used by public authorities in performance of their public tasks).

All processing of personal data carried out by the College must meet one or more of the conditions above. In addition, the processing of 'special categories' of personal data requires extra, more stringent, conditions to be met in accordance with Article 9 of the GDPR.

Under the GDPR, colleges are classified as public authorities and therefore the use of the 'legitimate interests' justification is not possible in terms of the College's core activities (public tasks). It is possible to use legitimate interests for processing that is undertaken outside of the College's public task.

The College does not use consent for its core activities due to the imbalance in the relationship between the controller and the data subject, and it is deemed that consent cannot be freely given. As such, the College uses other legal justifications for processing personal data.

7. Subject Consent

There are cases, such as commercial activities, where the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, **express consent** must be obtained. Please view the Appropriate Policy Document in Appendix 7 for further details.

Consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or other clear affirmative action, signifies agreement to the processing of personal data relating to him or her". The GDPR clarifies that silence, pre-ticked boxes or inactivity does not constitute consent and one has to opt in.

Anyone who has provided consent has the right to revoke their consent at any time.

Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions. This is included as part of the recruitment process and is on every student's individual learning agreement.

The College will also ask for information about particular health needs, such as allergies or any conditions such as asthma or diabetes. The College will only use the information for the protection of the health and safety of the individual, but will need consent to process it such as for a college trip, for example.

8. Rights of Data Subjects

Under UK data protection legislation data subjects have clearly defined rights to the data the College holds about them. It is important that you know the College's stance in addressing these rights, as it will not always be possible to fully comply with a request.

A data subject has the following rights; this explained in general terms within this section. For the College's actual policy for dealing with each type of request please refer to the relevant subsequent sections:

8.1 Right to Access

8.1.1 This is a request to see what data is held by the College on a data subject. The data subject is entitled to see any hard copy or digital records. To facilitate this need the College will look to simplify storage so that information is, where possible, only held in one place; and

8.1.2 The data subject can only see their own data so should the records make reference or include the personal data of other subjects then this cannot be disclosed. Techniques should be adopted to redact or remove the supplemental information in these cases.

8.2 Right to Rectification

8.2.1 The College makes every reasonable effort to ensure the records it holds on employees, students or others dealing with personal data is fully accurate. Where this is not the case the data subject has the right without undue delay to the rectification of inaccurate personal data concerning him or her.

8.3 Right to Erasure (to be forgotten)

8.3.1 A data subject has the right to the erasure of personal data concerning him or her without undue delay where one of the following grounds applies:

8.3.1.1 the personal data are no longer necessary in relation to the purposes for which they were collected;

8.3.1.2 the data subject withdraws consent on which the processing is based;

8.3.1.3 the data subject objects to the processing and there are no overriding legitimate grounds or reasons for the processing;

8.3.1.4 the personal data have been unlawfully processed;

8.3.1.5 the personal data have to be erased for compliance with a legal obligation in Union or Member State law; and/or

8.3.1.6 the personal data have been collected in relation to the offer of information society services

8.3.2 However, the right to erasure shall not apply

8.3.2.1 where the College has a legal obligation to hold the data;

8.3.2.2 for reasons of public interest in the area of public health;

8.3.2.3 for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; and/or

8.3.2.4 for the establishment, exercise or defence of legal claims.

8.3.3 Where the data has been made personal data public, the data controller (the College) shall take reasonable steps, including technical measures, to inform controllers who are processing the personal data that the data subject has requested the erasure.

8.4 Right to Portability (transfer)

Where a request to transfer data is received the member of staff should refer to the DPO or Human Resources Manager ("HR Manager") for guidance as these are requests that will not be expected by the College. Under the regulation:

8.4.1 A data subject can request to receive any data concerning him or her, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller, where:

8.4.1.1 the data is processed under a consent basis; or

8.4.1.2 where automated means are used (profiling, automated decision-making).

8.4.2 For the processing activities undertaken by the College it does not use profiling techniques; such requests will therefore be unexpected

8.5 Right to Restrict processing

8.5.1 The data subject shall have the right to obtain from the College restriction of processing where one of the following applies:

8.5.1.1 the accuracy of the personal data is contested;

8.5.1.2 the processing is unlawful;

8.5.1.3 the College no longer needs the personal data for the purposes of the processing; and/or

8.5.1.4 the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

8.5.2 Where processing has been restricted, as above, personal data can only, with the exception of storage, be processed with the data subject's consent or for legal purposes.

8.6 Right to Object

8.6.1 the data subject shall have the right to object to any processing by the College under either a "public" or "legitimate interests" basis;

8.6.2 where personal data is processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling; and/or

8.6.3 the data subject may exercise his or her right to object by automated means using technical specifications e.g. profiling or automated decisions.

Any objections to the processing undertaken should be referred to the DPO or HR Manager if the data relates to staff.

9. Dealing with an Access request for Information

The College must respond to an access request promptly, which is taken to mean as quickly as it reasonably can. It must, in any case, respond within 30 calendar days of receipt of the request, or within 30 calendar days of receipt of the information. The College is required to satisfy itself about the identity of the person making the request and the 30 day calendar starts from validation of the ID and the request.

In general, the College works to a service standard of arranging for an employee's or student's request to be satisfied within 20 working days of employees receiving the written request. This standard will only be extended if there is good reason to do so, for example other work pressures within the Department that make it impossible to meet the standard.

An extension by two further months where necessary, taking into account the complexity and number of the requests is permissible but only where the College has informed the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Where the data subject makes the request by electronic means and, unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

The College can only respond to the data subject and will need to satisfy itself about the identity of the subject using appropriate ID techniques. It is not appropriate to seek ID as a means to delay a response or where the requester is known or can be identified by normal means.

Should the request to access come from a third party the College must be certain that the request is properly authorised by the subject. This may require additional checks with the data subject or to only submit the information to the subject for their onward submission.

The provision of data for any access request is free of charge unless the request is considered to be excessive e.g. where a number of requests for similar data have been received or where duplicate records of information already provided are sought.

If a request is considered to be excessive, permission should be sought from the DPO before any charge is applied.

The College reserves the right to refuse requests where they are “manifestly unfounded” or “excessive” or where there is a legal exemption, such as disclosing the information could significantly harm a student.

9.1 Students’ Access to Information

College’s learning agreements and various student publications provide guidance to students regarding information disclosure or requests. See Appendix 3 for student data processing notice.

Students, like any data subjects, are entitled to request access to data about themselves. As personal data includes any expression of opinion about an individual, if the College holds any adverse comments about students in relation to performance, for example, this is included in the right to access. All student requests should ideally be made in writing (letter or email) to the DPO, Oakfield Lane, Dartford. Verbal requests may be made and whilst **not a requirement**, it is recommended that they are followed up in writing to provide a clear trail of correspondence. It will also provide clear evidence of the Data Subjects actions.

When the College makes arrangements for a student to see his/her personal information, the College will provide everything that existed at the date the request was made and will not make any special alterations to data to make it more acceptable. However, sometimes routine data may result in it being amended or even deleted whilst the College is dealing with the request and, in that case, it is reasonable for the College to supply the information available when at the point the response is sent.

The legislation requires the College to provide the information to the student in an “intelligible form”, which the average person is capable of understanding.

9.2 Student documents not allowed to be seen

Information requests regarding student data will not be complied with if to do so would mean disclosing information about another individual who can be identified from the requested information or if they could be put at risk. Exceptions will be made if the other individual has consented to the disclosure or it is reasonable in all the circumstances to comply.

9.3 Employees' Access to Information

The College's StaffNet system provides guidance to employees regarding the processing of their personal data and information about disclosure requests. See Appendix 5.

Employees are entitled to request access to data about themselves, whether it is held in a computer or in paper form. If an employee wants to see what information is held by the Human Resources Department, a written (letter or email) request must be submitted, addressed to the Human Resources Manager.

As personal data includes any expression of opinion about an individual, if the College holds any adverse comments about employees in relation to performance, for example, this is included in the right to access.

When the College makes arrangements for an employee to see his/her personal file, the College will provide everything that existed at the date the request was made and will not make any special alterations to data to make it more acceptable.

There are some exceptions to the information that will be made available defined in the section 7.4 of this policy.

9.4 Employee documents not allowed to be seen

In certain circumstances, access to particular documents may be restricted. The Human Resources Department might restrict access under the following circumstances:

9.4.1 where access to the document would or could cause interference with a current investigation by the College; and/or

9.4.2 where documents contain information dated prior to 1 March 1996 which was provided on the understanding that such information would remain confidential.

Any confidential documents will be sealed by a member of Human Resources staff but a list of these documents will be provided.

10. Dealing with an Erasure request

A data subject can request that the College erases or deletes their data. However, as the majority of the processing the College undertakes is needed for either the education of its students or for the employment of its staff; there will be very limited circumstances, if any, where it can genuinely comply with their request.

The College's policy is that should anyone request that their information be erased that the matter be referred to either the DPO or HR Manager. Under no circumstances, should any records be deleted without prior authorisation.

In the event that an employee may have deleted the records accidentally then please advise the DPO or HR Manager immediately as this is regarded under the legislations as a potential data breach*.

11. Dealing with a Portability or transfer request

Where a request to transfer data is received the member of staff should refer to the DPO or Head of HR for guidance, as these are requests that will not be expected by the College. The majority of data held by the College, is required in order to comply with contractual and legal obligations.

12 Dealing with a request to restrict processing or objecting to profiling

Where a request to restrict processing or an objection is made about the College's data processing, it should refer to the DPO or HR Manager for guidance. The majority of data held by the College, is required in order to comply with contractual and legal obligations.

13 Dealing with a Data request from a Third Party

The College is committed to data security and will make every effort to safeguard against illegitimate disclosure of personal information. Where a request for personal information is received from a third party, the request needs to be promptly forwarded to the DPO who will ensure the request made by the third party meets the requirements of disclosure (see section 18).

Third party enquiries/requests also include the Police. Police requests should be directed to the DPO, who will advise on what action is to be taken and also inform the Principal's Office and the Safeguarding Officers, where appropriate.

14 Fees for Data Subject Requests

14.1 Under the Legislation, no fees can be passed for data subject access request to their data.

14.2 Only in exceptional circumstances can a fee be passed; a small fee is considered acceptable where:

14.2.1 The request for data has become excessive e.g. where the data subject is continually asking for access or coming back for more and more detail; or

14.2.2 Where duplicates are being requested for information or records already provided.

Staff Responsibilities

15 Human Resources

The College has a duty to ensure that the information held is accurate. In addition, the College can only hold information which is necessary. Members of the HR Department will:

15.1 only request and record information about employees, or prospective employees that is appropriate to the recruitment process and ongoing management of the employment relationship;

15.2 only access and process the information that is necessary to perform the duties of the job or as otherwise consented to by the member of staff;

15.3 ensure information is kept up to date and is accurate; this will be checked through annual appraisals and periodic reminders as considered necessary;

15.4 ensure information is updated at appropriate times e.g. disciplinary details which are considered inactive after a certain period of time;

15.5 maintain the security of information by keeping passwords confidential and locking records away; and

15.6 not access information purely for personal interest.

16 All College Employees

16.1 All employees will need to be aware and ensure that:

16.1.1 the basic concepts as outlined in this policy and follow them where appropriate;

16.1.2 processing of personal data must be for a purpose that is explicit, lawful and covered by the College's notification;

16.1.3 all personal data collected, held, and processed, in hard copy (manual files), on computer and on-line, are subject to the Data Protection Principles (as defined in section 2 above) and should only be collected if really necessary (nothing should be either requested or recorded on the grounds that "it might come in useful", neither should it be used for purposes inconsistent with those specified in the College Data Registration document);

16.1.4 extra care should be taken in the handling and storage of special category personal data;

16.1.5 the circumstances under which they may legitimately access, process or disclose personal data whilst employed at the College;

16.1.6 tany data they hold, that is no longer needed, is securely deleted after they have finished processing the data. This includes the deletion of emails with attachment after the data has been used or saved to the appropriate file; and

16.1.7 All employees should raise any concerns about data, the loss of data or the inappropriate use of data with the DPO or HR Manager immediately.

17 Storage of data

Precautions should be taken to prevent any unauthorised access to personal data. Any information relating to named individuals should be handled and stored securely:

17.1desks or filing cabinets should be locked;

17.2 computers should be password-protected and passwords not disclosed to others;

17.3 data storage devices may only be used in compliance with the College IT Conditions of Use policy;

17.4 papers should not be left out on desks or tables;

17.5 information on computer screens should not be accessible/visible to other than authorised users;

17.6 special category data should be secure and subject to very limited access using, as a minimum, password protection;

17.7 personal data should not be removed from the College or stored elsewhere unless such use is recognised and authorised by the individual's line manager;

17.8 remote access to secure, on-line College information should be used wherever possible as an alternative to taking personal data off-site;

17.9 computers and data storage devices taken off-site should not be left unattended in vehicles;

17.10 laptop computers and data storage devices should be encrypted if they are to be taken off-site holding personal data; and

17.11 off-site security must conform to College standards as outlined above.

To minimise the risk of personal data being mishandled, duplicate records must not be created locally in any format. Only the College-provided systems must be used. If the available systems are not sufficient for your needs, contact the DPO in the first instance.

Data must not be held indefinitely.

18 Disclosure of Information

The requirements as outlined in Section 13 should be observed in all cases where information is requested by a third party. Guidance on disclosure is also included in Appendix 4 for Student records and Appendix 6 for employee records.

Additionally, all staff should be aware that this includes disclosure to parents or other relations (unless the specified next of kin provided at enrolment for learners aged under 18), partners, friends, colleagues, fellow learners.

College procedures may be discussed freely with anyone. Thus it is possible to explain to a parent what, *in principle*, happens when a student must re-take examinations, spend time on work placement, etc. but not to divulge the specific circumstances of an individual's case without the agreement of that student. See section 9.3 of "Working with students" for more in-depth guidance.

You may find yourself being asked by an individual to give them information in accordance with the Legislation. If so, you should not attempt to deal with it yourself, but should refer the enquirer to the DPO.

All requests concerning students, including student references (excluding UCAS), Council Tax requests, Government agency requests (Department for Work and Pensions, Home Office, Immigration Services etc.), Employment Agency Requests, Solicitors Requests and Police Requests, are centrally recorded by the DPO.

All requests concerning employees should be referred to the DPO or HR Manager. These may include requests from government agencies, building societies, solicitors, property landlords and partner organisations.

19 Providing student references

All reference requests need to initially go through Student Support and Inclusion. They will contact the relevant member of the Curriculum team, using a standard pro forma, to collect the information required. When supplying a reference, it should be assumed that the student will have the right to read it. Information should be factual and verifiable with unsubstantiated opinion being avoided.

20 Providing staff references

Requests for staff references must be forwarded to HR for response. Further details concerning staff references is contained with the Staff Employment Policy.

21 Disposal of information

Records must be disposed of securely through shredding or incineration to ensure no accidental disclosure to any third parties.

22 Employee personal data and requirements

Employees must keep their Line Manager and the HR Department advised, without delay, if any of their personal details change. This will enable records to be kept up to date and avoid difficulties later if action is required by the College, for example, sending letters to home addresses.

Students

23 Students

All students are responsible for:

21.1 checking that information they provide to the College in connection with their membership of the College is accurate and up-to-date; and

21.2 advising the College of any amendments to this information, e.g. changes of address. They can update their address by visiting the Student Support.

It is College practice to send all external awarding body certificates to a student's home address or, where appropriate, direct to an external training broker. If a student has not advised a change of address, the College would normally expect the student to pay for their replacement (regardless of age and fund stream). If a

certificate is returned, the College provides the student with the option of re-sending to their revised address or for them to collect in person.

The College cannot be held responsible for any errors, unless the student has provided updated information as here requested. See Appendix 3 for "Data Processing Notice to Students".

24 Children

Under the GDPR the following restrictions apply to the processing of personal information relating to Children (they are deemed to be under the age of 13):

- Online services offered directly to children require parental consent.
- Any information provided to a child in relation to their rights as a data subject has to be concise, transparent, intelligible and easily accessible, using clear and plain language.
- The use of child data for marketing or for profiling requires specific protection.

25 Breaches of the Data Protection Principles and Work Practices

It is imperative that the standards and work practices set out by the College within this Policy in relation to personal data are observed. Failure to do so may result in a breach of the Data Protection Principles and the person in breach would be seen as accessing data that was not for a "specified and lawful" reason.

A data breach is considered as meaning a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

This can arise from many practical scenarios such as:

25.1 lost phone or laptop;

25.2 passwords being shared or compromised;

25.3 sending email containing personal data to the wrong person;

25.4 sending information by group email to recipients not entitled to see the data or the other names on the list; and/or

25.5 accidental deletion or loss of records that should not have been deleted.

In the case of a personal data breach, the College has a mandatory obligation to report, no later than 72 hours after having become aware of the breach, to notify the ICO;

UNLESS the personal data breach is unlikely to result in a risk to the data subject(s).

A record of all breaches that occur across the College will be maintained by the DPO.

For this reason anyone who considers that the practices have not been followed in respect of personal data about themselves or any student or colleague must raise the matter with his/her line manager, or the DPO as soon as they become aware of the incident.

Any alleged breach will be investigated and where appropriate disciplinary action will be taken. Serious cases might result in the person who had accessed data in breach of this policy being dismissed.

26 Using Information for Research

Employees and, where relevant, students engaging in research as part of their studies, will need to ensure the research is undertaken either with the consent of the data subject(s) or using appropriate safeguards.

Research undertaken should not be published in a way that would:

26.1 identify or is targeted towards individuals or cause them damage or distress; and/or

26.2 support measures or decisions with respect to particular individuals.

Data used or to be considered for research purposes should be referred to the DPO for approval before the research is undertaken.

27 Freedom of Information Requests ("FOIR") and Environmental Information Regulations 2004 ("EIR")

Information that is already in the public domain is exempt from the FOIR and EIR.

All FOIR and EIR requests must be dealt with by the HR Manager. Before any information can be disclosed the following points need to be considered:

24.1 whether the specific data requested, or from the data requested combined with additional information available from other sources, may contain or allow the identification of personal data; (in such cases the College could consider a statistical form to eliminate this risk); and

24.2 whether the cost of providing the data in an appropriate format is reasonable on grounds of cost.

Further information on the Freedom of Information Scheme is located within the Freedom of Information Policy.

28 Retention of Data

Data will be retained by the College in accordance with the North Kent College Data Retention Guide. The guide is available to all College staff on StaffNet. Those who are not members of staff may request a copy from the DPO.

29 CCTV

The College operates a CCTV monitoring system on all sites. The purpose of this system is to:

29.1 assist in the detection and deterrence of crime;

29.2 provide evidence of crime;

29.3 give confidence to students, staff and visitors that they are in a safe environment;

29.4 provide management information with regard to health and safety;

29.5 provide management information to assist in the operation of College policies;

29.6 provide information with regard to traffic management; and

29.7 assist the Police and civil authorities in the event of a major emergency.

The system will be operated in a manner which safeguard individuals' right to privacy.

CCTV Data captured by the College is stored in accordance with the North Kent College Data Retention Guide (See Section 25 above).

The CCTV system only accessible to the College with all data stored on the College network.

The risks associated with CCTV images is taken seriously by the College and utilised in a compliant manner as determined by the ICO.

30 Data Privacy Impact Assessments ("DPIA")

When the College considers adopting or making any changes with regard to how personal data is processed that have a potential risks to the data subjects employees should consult with the DPO.

Where necessary they will be asked to complete a DPIA to consider potential privacy issues and risks and the actions to mitigate these risks.

Further guidance on DPIA can be obtained from the DPO.

Appendix 1:	**Glossary of Data Protection terms**
UK Data Privacy law	UK General Data Protection Regulation (“GDPR”) and UK Data Protection Act 2018.
Personal Data	any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controller:	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data Processor:	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
Data Protection Officer:	a person with expert knowledge of data protection law and practices to assist the data controller or processor to monitor internal compliance with data privacy legislation.
Processing:	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Subject:	an identifiable natural (living) person who can be identified, directly or indirectly, in particular by reference to an identifier such as: • a name; • an identification number; • location data; • an online identifier (e.g. IP address): or • specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Privacy Notice:	is used by North Kent College to provide data subjects with information about the processing of their personal data, usually at the time of its collection. It will describe the purposes for which the College intends to process their personal data and will include details of joint data controllership, as well as third parties to who data may be disclosed or transferred, and the purposes served by those transfers or disclosures. North Kent College makes this information available on the Enrolment/Student Agreement and for prospective and existing staff on Application Forms; and contracts of employment.
Profiling	any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Genetic Data:	personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Biometric Data: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprint data.

Pseudonymisation: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.**Appropriate safeguards/**
to ensure a level of security appropriate to the risk,

Technical and organisational measures such as:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of data security measures.

Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Inaccurate Data: Data which is incorrect or misleading as to a matter of fact.

Notification: entry on the public register maintained by the Information Commissioner's Office showing types and range of information being processed by the College.

Manifestly unfounded subject

access requests:	Where an individual has no clear intention of exercising the right of access.

Appendix 2: UK Legislations and Interaction with other associated legislation

1. The Freedom of Information Act 2000 ("FOIA 2000")

The FOIA give a general right of public access to all types of "recorded" information held by public authorities, sets out exemptions from that general right and places a number of obligations on public authorities. Therefore, this Act applies to schools, colleges and universities. The College has two main responsibilities under the Act:

1.1. the College must produce a publication scheme; and

1.2. the College must deal with individual public requests for information.

There may be circumstances where personal data may be disclosed under the FOIA subject to a public interests test and examination of risks to the individual's rights.

All FOIA requests must be forwarded to the College in accordance with the Freedom of Information Policy. Individual employees must not reply in person.

NB: if a request is made by an individual for information about themselves, it should be handled under UK data protection Legislation.

2. Environmental Information Regulations 2004 ("EIR")

All EIR requests must be forwarded to the College in accordance with the Freedom of Information Policy. Individual employees must not reply in person.

3. Human Rights Act 1998

The main provision of the Human Rights Act 1998 relevant to data protection is Article eight, which states:

3.1. everyone has the right to respect for his private and family life, his home and correspondence; and

3.2. there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others.

Therefore, breaches of UK Legislation could give an indirect cause of action to individuals seeking to claim their Article eight rights were being breached.

4. Regulation of Investigatory Powers Act (RIPA) 2000

This provides, in conjunction with The Investigatory Powers (Interception by Businesses etc for Monitoring and Record-keeping Purposes) Regulations 2018, SI 2018/356, grounds for the lawful interception of communications, including telephone and computer communications. However, personal data collected under these laws must be processed in accordance with the General Data Protection Regulation requirements, unless elements of that processing are derogated to the Data Protection Act 2018, such as for the purposes of law enforcement or national security

5. Privacy and Electronic Communications Regulations 2003 (PECR 2003)

This EC directive regulates direct marketing activities by electronic means (phone, fax, email etc.). They also regulate the security and confidentiality of such communications, with rules governing the use of cookies and spyware. The regulations compliment the UK Legislation in the way that any organisation can use personal data, ensuring appropriate safeguards for individuals' rights and privacy. Where personal data is used UK Legislation always applies

6. Electronic Commerce Regulations 2002

This EC directive aims to ensure that individuals are able to effectively utilise consumer protections and other rights, including those granted under Data Protection Act 2018and the PECR 2003 by providing them with the necessary information about whom to enforce those rights.

7 The Investigatory Powers (Interception by Businesses etc for Monitoring and Record-keeping Purposes) Regulations 2018, SI 2018/356

The College may have to monitor or keep a record of communications for the purposes set out in The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018. These purposes include:

- To ensure compliance with regulatory practices or procedures
- To prevent or detect a crime
- To investigate or detect the unauthorised use of the telecommunication system
- To secure the effective operation of the telecommunication system

The use of monitoring or keeping record of communications would be used in exceptional circumstances for crime detection as agreed by the DPO and Principal.

The College does not need to gain consent before intercepting for the purposes set out in the Regulations. However the College is expected to make reasonable efforts to inform staff, students or any other person who may use the telecommunication system that communications transmitted by means of that system may be intercepted.

Appendix 3: Student Privacy

This section should be read in conjunction with the College Data Privacy Notice which is available by following this LINK or upon request from the College Reception.

North Kent College is notified as a data controller with the ICO and, in compliance with UK data protection regulations, this privacy policy explains what personal information the College collects from you when you visit its website or are a recipient of its services.

The College is committed to processing personal information about its students in ways that comply with its legal and regulatory obligations and to being clear about what it does with their personal information.

What Data does the College collect?

The information the College collects during the enrolment process and when you register with the College is needed for it to fulfil its duties in providing you with higher or further education. The data the College collects includes:

- name, address, email, phone/mobile, date of birth;
- previous school/university, course fees;
- parent(s)/guardian(s) name/email, emergency contact details (name/relationship/email/mobile /landlines);
- car registration;
- nationality;
- qualifications;
- official identification documents;
- referee details (name/address/phone/email);
- household status; and
- employment status/details.

The College also collects special category data necessary for legal requirements and reporting but also to help it provide you with the most effective education and to keep you safe whilst in the College.
The information the College collects may include data revealing or concerning:

- racial or ethnic origin;
- political opinions such as identified through academic study and Student Union involvement
- religious or philosophical beliefs;
- trade union membership;
- health such as to support students with absences and learning difficulties/disabilities, e.g. ECHP);
- a student's sex life and sexual orientation such as to support student well-being.

The College may also collect personal data about criminal allegations, proceedings or convictions to safeguard our College community and as a requirement for students undertaking certain work experience activities where a Disclosure and Barring Service check is required. We may have to share this data for the purposes of law enforcement.

Why does the College collect this?

The data the College collects necessary for the education of its students and is shared with teaching, funding and for administrative purposes.

How is the data used or processed

1. disciplinary/grievance procedures;
2. attendance monitoring;
3. correspondence to students relating programme of study;
4. distribution examination/registration documents;
5. storage and usage of student image used to create ID Cards;
6. contact to students via text, email or post using information collected on the enrolment/learning agreement;
7. the provision of advice and support to learners via, amongst others, Student Data Services, Student Support and Inclusion and Additional Support;
8. registration with awarding bodies;
9. Safeguarding;
10. disclosing information to the Local Authority;

11. disclosing information to sponsors/employers (where stated on the Learning Agreement)

12. disclosing information to current external work based training providers;

13. disclosing information to professional and statutory bodies;

14. disclosing information to government agencies including the Police, if deemed necessary and within the confines of legislation. In particular in relation to safeguarding of young people and vulnerable adults and others and in line with the Children's Act and FE Act;

15. Disclosing information to funding agencies;

16. disclosing any outstanding debt to debt collection agencies; and

17. disclosing information on your learning status. This may include information regarding your attendance, performance on course, behaviour, awarding body entry and exam attendance, if you are under 19 years old at the start of your learning programme. This data will only be disclosed to the emergency contact you provided at enrolment. If your emergency contact details change during your time at the College, please contact Student Support & Inclusion to update them.**Who does the College share your data with?**

Access to your personal information is only allowed when required by law or is required as part the College fulfilling its service obligations. The College does not and will never, sell your personal information with other third parties.

The College collects data on behalf of the Education and Skills Funding Agency (ESFA), for the purposes of fulfilling the Secretary of State's statutory functions, as set out in the Apprenticeships, Skills, Children and Learning Act 2009 and for the exercise of functions of the Crown, a Minister of the Crown or that government department. The information you supply is used by the Education and Skills Funding Agency, an executive agency of the Department for Education (DfE), to issue you with a Unique Learner Number (ULN) and to create your Personal Learning Record, as part of the functions of the DfE. For more information about how your information is processed, and to access your Personal Learning Record, please refer to:

https://www.gov.uk/government/publications/lrs-privacy-notices To obtain a list of the third Parties with whom the College shares your data, please contact the College Data Protection Officer.

How is the data kept safe?

The College is committed to keeping students personal information secure to protect it from being inappropriately or accidentally accessed, used, shared or destroyed, and against it being lost.

The College may need to transfer personal information to third parties located outside the UK. If the College does share information, it will ensure that the information is protected to a level which meets the requirements of UK law and only to territories' that are approved or considered to be safe.

How long does the College keep personal information?

The College will only retain student personal information for as long as needed to carry out a particular purpose or to meet a particular obligation (contractual or legislative).

Access to personal information

Under UK data privacy legislation students have clearly defined rights to the data the College holds about them. This information will be provided free of charge, where the requests are not considered excessive and within 30 days.

To make a request to College for any personal information it may hold, or if you are not happy with the way your data is being used please contact the College by writing to the address provided below:

The DPO
North Kent College
Oakfield Lane
Dartford
Kent DA1 2JT

Email: DPO@northkent.ac.uk

Appendix 4: Staff Guidelines for the disclosure of student personal data

1. Introduction

North Kent College receives regular requests for information on students, both past and current. Please do not hesitate to contact Student Support and Inclusion should you need any further information or explanation.

In many cases, UK Data Privacy Legislations ("Legislation") limits disclosure of personal information without the data subject's ("student's") authorisation to third parties

2. Disclosure Overview

Any request should be referred to Student Support and Inclusion and/or the Management Information Systems Manager who will:

2.1 check students have a signed learning agreement;

2.2 deal with requests promptly (as per the legislation) but before responding will ask for information that reasonably would be needed to find the correct data (the 30 day response time does not begin to run until Student Services has received any additional information required);

2.3 ascertain whether the person making the request relates to the information they require;

2.4 verify individual requests received from third party organisations/ bodies listed below; (they must be made in writing on official headed paper and should ideally cite the relevant Legislation exemption or other legislation which authorises the College to release the information, or provide a signed declaration of authority to divulge information.)

2.5 verify individual requests received from third party on behalf of a student by ensuring a signed declaration is provided (if the College feels the student concerned may not understand what information may be disclosed to the third party, it could chose to send the response directly to the student. The student can then choose to share the information after having the chance to read it);

2.6 not comply with a data request if to do so would mean disclosing information about another individual who can be identified from the requested

information (exceptions will be made if the other individual has consented to the disclosure or it is reasonable in all the circumstances to comply); and

2.7 provide information in a permanent form unless it would involve disproportionate effort to do so. (In this case, the College will invite the student to visit to view the original documents and copy any documents they would like to take away. Any visit will be in the presence of Student Support Manager or Management Information Systems Manager).

3. Exceptional circumstances for disclosure

Confidentiality may have to be breached if there is a danger that:

3.1 the student may harm themselves;

3.2 the student may harm other persons; and/or

3.3 the student's life or health or safety may be threatened.

The Legislation makes it permissible to process the data in these circumstances where it is in the vital interests of the student i.e. their life or health depends on it or in the public interest if they are a danger to others.

Should you be unclear then please refer to the Assistant Principal Teaching and Learning; any of the College's designated Safeguarding Officers; or the DPO.

4. Disclosure to Families/Relatives

The College is not under any obligation to provide information to relatives without consent unless the student is under the age of 13 and the relative is either a parent or guardian and/or the relative has Lasting Powers of Attorney. Although employees may come under pressure to discuss learners' cases with parents, it is essential that personal information is not disclosed without the written or verbal consent of the student involved.

Exception:

All students provide "emergency contact" details at point of enrolment. If the student is aged under 19 at start of their Learning Programme, the College will provide information to those persons relating to the student's learning status which may include information regarding attendance, performance on course, behaviour, awarding body entry and exam attendance unless the student has formally requested the College not to. If next of emergency contact details change during the course, learners must contact Student Support and Inclusion. This potential disclosure is made clear on learning agreements and in student publications.

College procedures may be discussed freely with anyone. It is possible to explain to a parent what, in principle, happens when a student must re-take examinations; go on work placement; apply for Additional Support, etc. but not to divulge the specific circumstances of an individual's case without the agreement of that student.

5. Disclosure to third parties or student requests for a student reference

If a student asks any employees to provide them with a reference, the student must be directed to Student Support and Inclusion where a reference request form will be completed.

Student Support and Inclusion will only provide references to individual companies or organisations; the College cannot provide "to whom it may concern" letters. If a reference is being requested by the student they will need to provide the name and address of the company/organisation for which the letter is intended.

When the Student Support and Inclusion team receive a reference in the post that requires a personal opinion by the tutor, they will send a standard email form direct to the tutor concerned. The tutor should complete the reference and send the email response back within five working days.

The Student Support and Inclusion service standard for "full" references is 15 working days.

6. Disclosure to the Police

Disclosures to representatives of the Police are not compulsory except in cases where the institution is served with a Court Order requiring information. However, the Legislation does allow exemption under circumstances of public interest where data is disclosed in relation to "the prevention or detection of crime" and "the apprehension or prosecution of offenders".

The College may choose to release personal information to the Police in limited circumstances. Such disclosures should be made only in cases where the Police confirm that they wish to contact a named individual about a named criminal investigation, regardless of whether that individual is suspect or witness and where the College is reasonably satisfied that failure to release would prejudice the investigation.

Information should be provided only on receipt of written confirmation or College Pro forma with the signature and badge number of the investigating officer.

The request should be explicit as only specific data will be issued. The College Safeguarding Officer must be informed of the information provided.

7. Disclosure to Government agencies

In most cases the College can disclose personal data to Government agencies under Legal obligations as defined within the Legislation. The College's requirement is to ensure the request is legitimate that any data transferred is secure.

Specific examples of departments where disclosure may be necessary:

7.1 **Her Majesty's Revenue and Customs ("HMRC")** - Disclosures should be made when an official written application is received from HMRC in relation to the collection of tax or duty;

7.2 **Home Office -** there is a statutory obligation to co-operate when enquiries are received from the Home Office, and its divisions, including Office Security and Counter-Terrorism, Border Force, Immigration Enforcement and UK Visas and Immigration. The request should be made in writing on official paper;

The College must follow the Border Regulations which includes disclosing overseas students' College status and attendance;

7.3 **Child Maintenance Service ("CMD"), Financial Conduct Authority ("FCA")** - there is a statutory obligation to co-operate when enquiries are received from the CMS/FCA. The request should be made in writing on official headed paper;

7.4 **Department for Work and Pensions ("DWP")/Jobcentre plus** - in cases where an officer of the DWP suspects an individual of benefit fraud, statutory powers are available to them to require the College to provide data on one or more named individuals. Written statements should be obtained from the relevant authorised Officer explaining the reason for the request;

7.5 **Health and Safety Executive ("HSE"), Department of Health/ Environmental Health Officers, Environment Agency, College Insurers (relating to student accidents)** - please refer all requests made by the above agencies to the College's Risk Manager;

7.6 **Office for Students ("OfS") and agents such as Higher Education Statistics Agency ("HESA") and OfS auditors** - the College is required by law to disclose information to the Office for Students on request. This includes the incidental disclosure of student data during visits by academic or other auditors appointed by the OfS. Disclosures may also be made to agents of the Funding Council.

7.7 **National Health Service ("NHS") Fraud Investigators** - Official requests received in writing and which cite the relevant DPA exemption to permit disclosure should normally be met.

8. Disclosure to College Related agencies

Similar to Government agencies, the College will have legal requirements to share personal data with:

8.1 **Internal and External Auditors/OFSTED/Quality Assurance Agency for Higher Education** - the College is required by its own statutes (and funding bodies) to appoint external auditors. It is acceptable that such auditors will inevitably see student data (via controlled access) during the course of their investigations;

8.2 **Student Loans Company ("SLC")** - The SLC provides loans and, in some cases, fee payments for eligible students. Students who are in receipt of such funding sign a formal agreement with the SLC regarding the financing of their studies, a contract which permits disclosure of personal information by the College as necessary.

8.3 **Sponsors including Training Providers** - the College is under no obligation to provide information to sponsors/ employers without consent. Consent is gained via the College Learning Agreements. If consent has been gained the following information will be divulged:

8.3.1 progress/achievement; and/or

8.3.2 attendance reports.

8.4 **UCAS** - as applicants are made aware by UCAS when they first submit their details that information will be passed between them and the College, relevant data may be shared freely with UCAS as the need arises. For further information please refer to Student Support.

9. Disclosure to Local Authorities

9.1 **Census**

Census officers have no statutory right to ask the College to provide student data. The College should co-operate with the distribution of Census forms as far as is possible but personal information should not be released directly to Census officers without prior permission from the student(s) involved.

9.2 Council Tax Registration Officers

Student data may be disclosed to Council Tax Registration Officers as necessary, even without consent. The request must be made in writing and specify the exact provisions under which the request is made.

There must be reasonable grounds for believing that failure to disclose to these officers would adversely affect the collection of or assessment of any tax.

9.3 Electoral Registration Officers

Electoral Registration Officers have certain powers to require the provision of student information for the purposes of maintaining registers of parliamentary and local government electors.

If approached by an Electoral Registration Officer for information about learners, the College should check the reason for the request and under what legislative act. If satisfied with this, the disclosures can be made but learners should be informed of the disclosure.

9.4 Social Services (Children and Vulnerable Adults) – including looked after children

All requests to go via the College's designated Safeguarding Officers.

10. Disclosure to other organisations

10.1 Survey/research organisations

The College may be approached, from time to time, by survey and research organisations, or others conducting research, who wish to be provided with student information or contact details for a sample of the student body.

The College must seek informed consent from any student whose details might be disclosed in this context unless there are appropriate guarantees about the anonymity or similar techniques are used in providing the data i.e. the data is unidentifiable

10.2 Other Educational establishments

The College may be asked for information about current or former students by other educational establishments. Requests for information from institutions formerly attended by the student should not normally be met, unless either the student has authorised the disclosure or the other institution can provide verifiable justification under the Legislation.

10.3 Employers and Recruitment Agencies

The College may be asked for information about existing or former students by current or potential employers and recruitment agencies. Evidence of authority to divulge is required before disclosure.

10.4 Solicitors acting on behalf of other persons/bodies

The legislation's non-disclosure provisions are waived for the purpose of "or in connection with legal proceedings or is otherwise necessary for establishing, exercising or defending legal rights".

In cases where the College is approached by solicitors or others engaged in a Court case (not directly involving the College); it is College policy that any such requests should be directed to Student Support and Inclusion. Information will not be disclosed without the consent of the student concerned.

Appendix 5: Staff Privacy Notice

North Kent College is notified as a data controller with the ICO and, in compliance with UK data protection regulations, this privacy policy explains what personal information the College collects from you when you are employed by the College, visit the College's website, or are a recipient of its services.

The College is committed to processing personal information about its staff in ways that comply with its legal and regulatory obligations and to being clear about what it does with their personal information.

What does the College collect?

The information the College collects during the recruitment process and when you sign the contractual agreements to become a member of staff are needed by the College to fulfil its duties as an employer. The data collected includes:

- name, address, date of birth, gender, email address, telephone numbers;
- referees' details;
- family/emergency contacts;
- proof of identification;
- proof of qualifications;
- National Insurance Number; and
- Bank details.

The College also collects special category data necessary for legal requirements and reporting but also to help keep you safe whilst in the College, The information the College collects includes:

- Medical details / questionnaire;
- Ethnicity
- Criminal convictions, including driving convictions where relevant to the job role; and
- Sickness / absence monitoring (The Bradford Factor)

Additional information about how the College collects special category data and criminal conviction data can be found in the Appropriate Policy Document in Appendix 7.

Why does the College collect this?

The data the College collects necessary to meet legal requirements as an employer and to provide you with a salary and the other benefits it provides.

How is the data used or processed?

1. the purpose of the recruitment and selection process;
2. to support the administration processes underpinning the employment of staff;
3. to support the College in the operation of its policies;
4. to enable the College to monitor the effectiveness of its policies;
5. to assist with statistical returns to funding bodies and government agencies;
6. to assist with College internal and external audit requirements;
7. to ensure compliance with employment law; and
8. disclosing information to government agencies including the Police, if deemed necessary and within the confines of legislation, in particular in relation to safeguarding of young people and vulnerable adults and others and in line with the Children's Act and FE Act.

Who does the College) share your data with?

Access to your personal information is only allowed when required by law or is required as part of the College fulfilling its service obligations. The College does not, and will never, sell your personal information with other third parties.

How is the data kept safe?

The College is committed to keeping staff personal information secure to protect it from being inappropriately or accidentally accessed, used, shared or destroyed, and against it being lost.

The College may need to transfer personal information to third parties located outside the UK. In this case, the College will ensure that information is protected to a level which meets the requirements of UK law and only to territories that are approved or considered to be safe.

How long does the College keep personal information?

The College will only retain staff personal information for as long as it needs it to carry out a particular purpose or obligation. Specific information on data retention periods may be obtained from the DPO.

Access to personal information

Under UK data privacy legislation staff have clearly defined rights to the data the College holds about them. This information will be provided free of charge, where the requests are not considered excessive and within 30 days.

To make a request to the College for any personal information it may hold, or if you are not happy with the way your data is being used please contact the College by writing to the address provided below:

The DPO
North Kent College
Oakfield Lane
Dartford
Kent DA1 2JT

Email: DPO@northkent.ac.uk

Appendix 6: Staff Guidelines for the Disclosure of Staff Personal Data

1. Introduction

North Kent College receives requests for information on employees, both past and current. Please do not hesitate to contact the HR team ("HR") should you need any further information guidance.

The main thing to remember is that, according to UK Data Privacy Legislations ("Legislation"), there is limited disclosure of personal information without the data subject's (staff's) authorisation to third parties whether personally related or from Legal bodies.

2. Disclosure overview

Please note that any request should be referred to the Human Resources team and/or the HR Manager.

The Human Resources team will:

2.1. deal with requests promptly (as per the legislation and the College's service level) but before responding will ask for information that reasonably would be needed to find the correct data (the 30 day response time does not begin until to run until Human Resources has received the any additional information required);

2.2. ascertain whether the person making the request is a valid recipient of the information they require;

2.3. verify individual requests received from third party organisations/bodies listed below; (they must be made in writing on official headed paper and should ideally cite the relevant Legislation exemption or other legislation which authorises the College to release the information, or provide a signed declaration of authority to divulge information);

2.4. verify individual requests received from third party on behalf of an individual (employee) by ensuring a signed declaration is provided (if the College feels the employee concerned may not understand what information may be disclosed to the third party, it could chose to send the response directly to the employee. The employee can then choose to share the information after having the chance to read it);

2.5. not comply with a data request if to do so would mean disclosing information about another individual who can be identified from the requested information (exceptions will be made if the other individual has

consented to the disclosure or it is reasonable in all the circumstances to comply); and

2.6. provide information in a permanent form unless it would involve disproportionate effort to do so (in this case, the College would invite the employee to visit to view the original documents and copy any documents they would like to take away. Any visit will be in the presence of a member of the HR team).

3. Exceptional circumstances for disclosure

Confidentiality may have to be breached if there is a danger that:

3.1. the employee may harm themselves;

3.2. the employee may harm other persons; and/or

3.3. the employee's life or health or safety may be threatened.

The Legislation makes it permissible to process the data in these circumstances where it is in the vital interests of the member of staff i.e. their life or health depends on it or in the public interest if they are a danger to others

Should you be unclear then please refer to the HR Manager or the DPO.

Sections 4 - 10 below show who might request employee information from the College either as a regular or ad hoc occurrence.

4. Disclosure to Families/Relatives or other third parties

The College is not under any obligation to provide information to relatives or other third parties, such as landlords, building societies and casual enquirers, without consent. It is essential that personal information is not disclosed without the written or verbal consent of the employee involved. Such enquiries should be directed to the HR team who will contact the employee to pass on any enquiries.

5. Disclosure to potential employers: requests for an employee reference

College policy is to respond only to written requests for a reference and to reply in written form only. The Legislation has an impact on the type of information which may be given and also on an individual's right to view data written about them. Requests for staff references should be prepared in line with the College Staff Employment Policy (available on StaffNet) then sent to HR for final preparation and issue. It should be assumed that the employee will have the right to read it. Information should be factual and verifiable with unsubstantiated opinion being avoided.

Human Resources will normally only provide references to individual companies or organisations.

6. Disclosure to the Police

Disclosures to representatives of the Police are not compulsory except in cases where the institution is served with a Court Order requiring information. However, the Legislation does allow exemption in cases where data is disclosed in relation to "the prevention or detection of crime" and "the apprehension or prosecution of offenders".

The College may choose to release personal information to the Police in limited circumstances. Such disclosures should be made only in cases where the Police confirm that they wish to contact a named individual about a named criminal investigation, regardless of whether that individual is suspect or witness and where the College is reasonably satisfied that failure to release would prejudice the investigation. Information should be provided only on receipt of written confirmation or College Pro forma with the signature and badge number of the investigating officer. This should always include a statement confirming that the information requested:

6.1. the request should be explicit as only specific data will be issued;

6.2. all requests for information regarding a member of staff should be directed to the Human Resources Manager; and

7. Disclosure to Government agencies

In most cases the College can disclose personal data to Government agencies under Legal obligation as defined within the Legislation. The College's requirement is to ensure the request is legitimate that any data transferred is secure.

Specific examples of departments where disclosure may be necessary

7.1. Her Majesty's Revenue and Customs ("HMRC")

Disclosures should be made when an official written application is received from HMRC in relation to the collection of tax or duty.

7.2. Home Office

There is a statutory obligation to co-operate when enquiries are received from the Home Office. The request should be made in writing on official paper.

There is a statutory obligation to co-operate when enquiries are received from the Home Office, and its divisions, including Office Security and Counter-Terrorism, Border Force, Immigration Enforcement and UK Visas and Immigration. The request should be made in writing on official paper;

7.3 **Child Maintenance Service ("CMD"), Financial Conduct Authority ("FCA")** - there is a statutory obligation to co-operate when enquiries are received from the CMS/FCA. The request should be made in writing on official;

7.4. Department for Work and Pensions ("DWP")/Jobcentre Plus

In cases where an officer of the DWP suspects an individual of benefit fraud, statutory powers are available to them to require the College to provide data on one or more named individuals. Written statements should be obtained from the relevant authorised Officer explaining the reason for the request.

7.5. Health and Safety Executive ("HSE"), Department of Health/ Environmental Health Officers, Environment Agency, College Insurers (relating to staff accidents)

Please refer all requests made by the above agencies to the Risk Manager.

7.6. National Health Service ("NHS") Fraud Investigators

Official requests received in writing and which cite the relevant Legislation exemption to permit disclosure should normally be met. They should be directed in the first instance to the HR Manager.

8. Disclosure to College Related agencies

8.1. Internal and External Auditors/OFSTED/Quality Assurance Agency for Higher Education

The College is required by its own statutes (and funding bodies) to appoint external auditors. It is acceptable that such auditors will inevitably see staff data (via controlled access) during the course of their investigations.

9. Disclosure to Local Authorities

9.1. Census

Census officers have no statutory right to ask the College to provide employee data. The College should co-operate with the distribution of Census forms as far as is possible but personal information should not be released directly to Census officers without prior permission from the employee(s) involved.

9.2. Council Tax Registration Officers

Employee data may be disclosed to Council Tax Registration Officers as necessary, even without consent. The request must be made in writing and specify the exact provisions under which the request is made.

There must be reasonable grounds for believing that failure to disclose to these officers would adversely affect the collection of or assessment of any tax.

10. Disclosure to other organisations

10.1. Solicitors acting on behalf of other persons/bodies

The Legislation's non-disclosure provisions are waived for the purpose of "or in connection with legal proceedings or is otherwise necessary for establishing, exercising or defending legal rights".

In cases where the College is approached by solicitors or others engaged in a Court case (not directly involving the College) any such requests should be directed to the Human Resources Manager in the first instance. Information will not be disclosed without the consent of the employee concerned.

10.2. Partnership organisations

Requests for information, such as Curriculum Vitae, should be submitted in writing and the purposes for which the information is required should be stated, along with the organisation representative responsible for the secure storage and legitimate use of the information in accordance with the Legislation. Requests should be submitted to the Data Protection Officer in the first instance for authorisation.

The HR team will prepare the data, ensuring that no unnecessary personal information is included, notify the employee(s) of the disclosure and obtain their explicit permission to disclose it. The information will normally be encrypted to ensure its security when transferred electronically.

Academic staff who teach on Higher Education courses through our partner universities will be required to provide a summary of their academic and industry experience for quality assurance, shared with the partner university.

Appendix 7: Appropriate Policy Document

1. Introduction

As part of North Kent College's ("the College") public function as a further and higher education provider, we process Special Category and Criminal Offence data in accordance with Article 9 of the General Data Protection Regulation ("GDPR") and Schedule 1 of the Data Protection Act 2018 ("DPA").

Schedule 1 Part 4 of the DPA requires us to have in place this document, called an 'Appropriate Policy Document', when we rely on certain conditions for processing Special Category and Criminal Offence data. This policy will tell you what Special Category ("SC") and Criminal Offence ("CO") data we process, our lawful basis (schedule 1 condition in the DPA) for processing it, the purposes for which we process it, and how we ensure compliance with the principles of data protection law provided in Article 5 of the GDPR.

We will also tell you how long we will hold the Special Category and Criminal Offence data. Some of the information is already held in other documents on the NKC website or is available from the Data Protection Officer.

2. Description of the data processed

We process the following types of Special Category and Criminal Offence data:

a) Health and disability
b) Religious/philosophical belief
c) Ethnic/racial background
d) Sexual life/sexual orientation
e) Political views
f) Trade Union membership
g) Criminal Offence data

We do not process biometric or genetic data.

3. Schedule 1 condition for processing

Below are the Schedule 1 conditions on which we rely, covered by this document. Special Category Data is abbreviated as SC; Criminal Offence Data is abbreviated as CO.

3.1. **Schedule 1 Part 1 para 1 (employment and social protection)** where the College needs to process SC/CO data for the purposes of performing its obligations or rights as an employer including providing human resources and

occupational health facilities for employees, or for guaranteeing the social protection of individuals

3.2. **Schedule 1 Part 2 para 8 (equality of opportunity)** where the College needs to process SC/CO data for the purposes of monitoring equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained

3.3. **Schedule 1 Part 2 para 10 (prevention of crime)** where the College needs to process CO data for the purpose of preventing or detecting unlawful acts, such as to safeguard and protect College students, by virtue of Schedule 1 para 36 of the DPA it is not necessary to demonstrate a substantial public interest in the above processing

3.4. **Schedule 1 Part 2 para 11 (protecting the public from dishonesty)** where the College needs to process CO data to protect members of the public from malpractice, unfitness, incompetence or mismanagement in the administration of a body or organisation, and obtaining consent would prejudice the exercise of the protective function

3.5. **Schedule 1 Part 2 para 12 (Regulatory requirements relating to unlawful acts and dishonesty)** where the College needs to process CO data to comply with a requirement which involves taking steps to establish whether an individual has committed an unlawful act, or been involved in dishonesty, malpractice or other seriously improper conduct.

3.6. **Schedule 1 Part 2 para 17 (counselling)** where the College needs to process SC/CO data in order to provide confidential counselling, advice or support or of another similar service provided confidentially, only where, in the circumstances, consent cannot be given by the data subject, cannot be reasonably obtained from the data subject, or where the processing must be carried out without the consent of the data subject because obtaining consent would prejudice the provision of the service, and is necessary for reasons of substantial public interest

3.7. **Schedule 1 Part 2 para 18 (safeguarding)** where the College needs to process SC/CO data in order to protect the physical, mental or emotional well-being of an individual under the age of 18, or over the age of 18 and at risk, only where, in the circumstances, consent cannot be given by the data subject, cannot be reasonably obtained from the data subject, or where the processing must be carried out without the consent of the data subject because obtaining the data subject's consent would prejudice the provision of the protection, and is necessary for reasons of substantial public interest

4. How we comply with the data protection principles in the GDPR Article 5

Article 5(2) of the GDPR requires Data Controllers to demonstrate how they comply with the data protection principles provided in Article 5(1). This section explains the measures we have taken to demonstrate accountability for the personal data we process and contains details about how we ensure compliance with the principles of the GDPR.

The GDPR sets out seven key principles:

a) Lawfulness, fairness and transparency
b) Purpose limitation
c) Data minimisation
d) Accuracy
e) Storage limitation
f) Integrity and confidentiality (security)
g) Accountability

4.1. Accountability

We demonstrate our compliance with the data protection principles provided in Article 5 of the GDPR through the following measures and documents:

We have appointed a Data Protection Officer whose role and responsibilities align with the provisions of Articles 37-39 of the GDPR.

Our Record of Processing Activities sets out the personal data categories we process, the purposes, the lawful basis, our retention periods for the data, our legitimate interests, Schedule 1 conditions for processing, recipients of personal data, any international transfers of data and our means of keeping data secure.

Our Privacy Notices in our Data Protection Policy explain to individuals how and why their data is processed by the College, what their rights are, and how they can get in touch with our DPO and the regulatory authority.

When we routinely and/or regularly share data with third parties, we enter into written agreements with Data Controllers and Data Processors which meet the provisions of Articles 26 and 28 of the General Data Protection Regulation respectively.

When we make decisions on whether to share data with third parties on an occasional or one-off basis, we do so in accordance with the Kent and Medway Information Sharing agreement overseen by the Kent and Medway Information Partnership (K-MIP).

We carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in a risk to individuals' data protection rights and freedoms.

We implement appropriate security measures which are proportionate to the risk associated with the processing.

4.2. Lawful, fair and transparent processing

We provide clear and transparent information to individuals about why we process their personal data, including our lawful basis in our Privacy Notices. This includes information about why we process Special Category and Criminal Offence data.

As a public authority we need to process Special Category Data for the substantial public interest conditions outlined in section 3 of this policy to meet the requirements of legislation such as the Equality Act 2010, the Health and Safety at Work etc Act 1974, the Counter-Terrorism and Security Act 2015 and legislation relating to safeguarding and education.

We process employment data to meet our legal obligations as an employer.

4.3. Purpose limitation

We process Special Category and Criminal Offence data where it is necessary to meet the following purposes.

- Equal opportunities monitoring, including statutory returns to the Education and Skills Funding Agency and Higher Education Statistics Agency
- Certain work placements or casual work opportunities where a DBS check is required
- Supporting special arrangements, such as building access plans, study inclusion plans, and mitigating circumstances applications
- Providing individuals with appropriate support in a counselling session
- To allow us to fully investigate a complaint or grievance
- To understand dietary requirements based on health or belief
- Recording sickness absence
- Complying with health and safety obligations
- Report actual or suspected cases of reportable diseases to the relevant governmental authorities/bodies

- Where processing is necessary to respond to an emergency situation
- Responding to binding requests or search warrants from courts, the government, regulatory or enforcement bodies
- To fully process job applications
- For the prevention and detection of unlawful acts (e.g. incidents captured on CCTV)
- To verify the good character, competence and integrity of senior managers and governors
- To take necessary steps to ensure that a natural or legal person offering philanthropic support or other support to the College has not committed an unlawful act, or been involved in dishonesty, malpractice or other seriously improper conduct.

We will only process Special Category and Criminal Offence data for the listed purposes, and in accordance with a condition in Articles 9-10 of the GDPR and Schedule 1 Parts 1-3 of the DPA. We process some Special Category and Criminal Convictions data for purposes not covered in this policy document. These conditions are:

- where we ask for your explicit consent to process Special Category and Criminal Offence data
- for the purposes of preventative or occupational medicine,
- where processing is necessary to protect your vital interests, and
- for research, statistics and archival purposes.

We may process data collected for any one of these purposes (whether by us or another Data Controller), for any of the other listed purposes, so long as the processing is necessary and proportionate to that purpose.

We will not process any personal data for purposes which would be incompatible with the purpose for which the data was originally collected.

4.4. Data minimisation

We design our data collection forms and other data collection tools to ensure we only collect the Special Category or Criminal Offence data necessary to achieve the purpose. Our purposes are set out in our Privacy Notices in the Data Protection Policy. Layered privacy statements are also included in data collection tools.

Where we operate systems which cannot control the volume of special category data collected (i.e. CCTV) we take measures to minimise the volume of data processed. We only monitor public spaces with the minimum number of cameras needed to cover the area, and we operate a retention period of 30 days from the date the footage is recorded.

We are satisfied that we collect and retain Special Category and Criminal Offence data for long enough to fulfil our purposes. We collect enough but no more than we need in accordance with the data minimisation principle, and we only hold Special Category and Criminal Offence data for the period set out in our retention policies.

Our retention schedule sets out the correct disposal action once records containing special category data are no longer required.

4.5. Accuracy

When we identify data that is inaccurate or out of date, having due regard for the purpose for which the data was processed, we will take necessary steps to rectify, replace or erase it as soon as possible and within one month. If there is a specific reason we cannot rectify or erase the data, such as the lawful basis does not permit it, we will record the decision.

We provide tools for staff and students to keep their personal data up to date, as well as issuing regular reminders to update or provide equalities monitoring data.

4.6. Storage limitation

Special Category and Criminal Offence data processed for the purpose of employment or substantial public interest, will be retained for the periods set out in our retention schedule. The retention policy for record categories is determined by our legal and regulatory obligations, and our business requirements. The retention schedule is available on request from the Data Protection Officer.

4.7. Security

Electronic data is hosted on a secure network, and on the secure servers of third party cloud storage providers with whom we have contractual agreements. Electronic and hard copy data is managed according to our internal IT policies.