Data Protection Policy and Procedures

Author: (Job title)	Director of Governance
Approved by:	Group Senior Management Team
Date of Approval:	21st September 2022
Updated/amended and reason: (Legislative/cosmetic)	Updated / Due for Review
Review Date:	September 2025
EIA Date:	January 2018

Table of Contents

A. Introduction

1. In order to carry out its role as a provider of training and education Capital City College Group ("CCCG") is required to process personal data about its staff, students and other users. This information is used to monitor performance, achievements and ensure the safety of its staff and students. It is also necessary to process information so that staff can be recruited and paid, courses organised and delivered, and legal obligations to funding bodies and the Government complied with. The following definitions are used:
    - "Criminal Records Data" is information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings;
    - "Data Subject" is a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and have legal rights regarding their personal data;
    - "Personal Data" is any information that relates to a living individual who can be identified directly or indirectly from that information.
    - "Processing" is any use that is made of personal data, including collecting, storing, amending, disclosing or destroying it.
    - "Special Category Data" is personal data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record.

2. CCCG will handle personal data with care and in compliance with the applicable law governing data protection including but not limited to the Data Protection Act 2018 ("DPA 2018") and the UK General Data Protection Regulation ("UK GDPR") (collectively "Data Protection Legislation").

3. In line with article 5 of the UK GDPR, CCCG will comply with the following data protection principles and will ensure that personal data is:

    - Processed in a lawful, fair and transparent manner;
    - Collected for a specified and legitimate purpose – and not Processed in a manner which is incompatible with those purposes;
    - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
    - Accurate and, where necessary, kept up to date;
    - Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is Processed; and
    - Processed in a manner that ensures appropriate security of the personal data.

4. CCCG staff and others who process personal data must ensure that they follow these principles at all times. This Data Protection Policy and Procedures document is intended to ensure that this happens.

Status of the Policy

5. This policy does not form part of the formal contract of employment for staff, but it is a condition of employment that all CCCG personnel must comply with this Policy.

6. Any failure to follow this Policy can, therefore, result in disciplinary proceedings. Any member of staff who considers that this Policy has not been followed in respect of their personal data should raise the matter with the designated controller within their area of work within CCCG, in the first instance. If the matter is not resolved, it should be raised as a formal grievance under the Group's Grievance Procedures.

7. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken or access to CCCG facilities being withdrawn and even a criminal prosecution (if there is evidence that personal data has been used for their own purposes without CCCG's consent). Any questions or concerns about the interpretation or operation of this Policy should be taken up with the designated relevant data controller or the Data Protection Officer ("DPO").

B. Designated Data Controllers and the Data Protection Officer

8. As a data controller as defined by Data Protection Legislation CCCG is required to comply with the UK GDPR. Whilst ultimate responsibility for compliance rests with the CCCG Board, the day to day compliance is the responsibility of all members of staff and the management of CCCG.

9. In order to ensure ongoing compliance with Data Protection Legislation CCCG operates a designated controller approach to data protection. For each main operational area there is a senior member of staff who has responsibility for the control and integrity of personal data ("Designated Data Controllers"). The table below gives details of these Designated Data Controllers:

Department / Division within the Group	**Designated Data Controllers**
Management Information Services / Registry / Examinations	Director of MIS
Finance	Director of Finance
Marketing	Director of Marketing
Human Resources	Chief People Officer
CANDI	Head of Quality
CONEL	Head of Quality
WKC	Head of Quality
CCCT	Managing Director

10. Under the UK GDPR it is mandatory to appoint a DPO. This role is performed by the Director of Governance for CCCG whose key responsibilities are to:

- Inform and advise the data controllers and processors with regards to Data Protection Legislation;
- Monitor compliance with Data Protection Legislation;
- Provide advice with respect to data protection issues;
- Co-operate with the Information Commissioner's Office (ICO);

- Act as a point of contact;
- Ensure that CCCG's Data Protection Policy is up to date and in line with current legislation and regulations; and
- Oversee requests and complaints made in relation to data protection using the following email address - dataprotection@capitalccg.ac.uk.

C. Rights of Students and Staff

11. Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under Data Protection Legislation. All Data Subjects are entitled to the following rights:

    - the right to ask whether CCCG processes their personal data and to receive a copy of their personal data;
    - the right to correct any errors in their personal data, and taking into account the purposes, to complete incomplete personal data;
    - the right, in certain circumstances, such as where personal data is no longer needed, to request that CCCG restricts the use that is made of the Personal Data;
    - the right, in certain circumstances, to ask CCCG to review and explain the legitimate interests in processing the personal data;
    - the right, where the legal basis of processing is consent, to withdraw that consent at any time;
    - the right, in certain circumstances, to have personal data erased;
    - the right to have personal data securely transferred to another organisation; and
    - the right to human intervention, to express their opinion and to obtain and challenge explanations where automated decision-making is used and has a significant impact on them.

    Detailed guidance on all of the rights that individuals have with regard to their personal data is available on the ICO website here - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/.

12. CCCG provides all staff and students and other relevant users with privacy notices. The notices inform the individuals of the types of data CCCG holds and processes about them and the reasons for which it is processed. CCCG's student privacy notice is attached as appendix 1 and its staff privacy notice is attached appendix 2.

D. Responsibilities of Staff

13. All staff are responsible for:

    - checking that any personal data that they provide to CCCG in connection with their employment is accurate and up to date;
    - informing CCCG of any changes to personal data which they have provided e.g. change of address;
    - checking the accuracy of information that CCCG will send out from time to time giving details of information kept and processed about staff;
    - informing CCCG of any errors or changes (CCCG cannot be held responsible for any errors unless the staff member has informed CCCG of them)

14. If and when, as part of their responsibilities, staff collect information about other people (i.e. about students' course, work, opinions about ability, references to other academic institutions or details of personal circumstances) they must comply with the guidelines for staff which are included as Appendix 3.

15. Staff should not pass personal data or work contact details of colleagues if a request is made from an external source, unless permission has been received from the staff member in question. In normal circumstances, if a request is made for contact details then the external person should be asked to make a request in writing (usually via email) which provides their contact details and allows the staff member in question to contact them if they deem this to be appropriate.

16. Staff must note that it is a criminal offence to use Personal Data that they have access to as part of their work for their own personal or commercial reasons without the consent of CCCG and doing so can lead to prosecution.

Security of personal data

17. All staff are responsible for ensuring that any personal data which they process is kept securely.

18. Personal data should not be disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party. This includes visual images held as part of CCCG's ID card system and the CCTV security system. Personal data should be:

    - kept in a locked filing cabinet or in a locked drawer or, if it is computerised, be password protected or;
    - kept only on a disk/USB which is itself kept securely or kept in a locked office with restricted access

19. CCTV images must be kept securely and be password protected – the appropriate documentation must be provided by police and other Government Agencies quoting the relevant section of the DPA 2018.

20. Staff should note:

    - that unauthorised disclosure will normally be considered as a disciplinary matter;
    - that this Policy should be read along with the Group's ICT Acceptable Use Policy.
    - that CCCG's data breach policy and procedures are to be followed in the even of a data breach (see appendix 4)

E. Student Obligations

21. Students must ensure that all personal data provided to CCCG is accurate and up to date. They must ensure that all changes of address etc. are notified to their personal tutor, who should notify the registry team. Students who use the CCCG's computer facilities may from time to time have access to personal data about themselves. CCCG can bear no responsibility for the sharing of personal data if this is carried out by the student themselves.

F. Lawful basis for using Personal Data

22. The lawful bases for processing and holding personal data are set out in Article 6 of the UK GDPR. In order to carry its role as an FE institution (i.e. to provide education and training) CCCG is permitted to hold personal data about staff and students, such as their name, contact details and academic achievement to date. We will only process personal data when we have a lawful basis for doing so.

    Most commonly, we will process personal data in the following circumstances:

    - If it is necessary to do so in order to fulfil employment contracts with staff and in fulfilling the student contract with students.
    - Where it is necessary for our legitimate interests (or those of a third party) and the interests and fundamental rights of the individual do not override those interests.
    - Where we need to comply with a legal obligation.
    - Where necessary for the performance of a task carried out in the public interest.
    - We will only rely on vital interests as a lawful basis for processing personal data where it is necessary to protect someone's life.
    - We will use consent as a lawful basis for some Processing. i.e. where there is no other lawful basis. Where we do so we always provide the individual with the choice as to whether or not to opt in to such Processing. Where we rely on consent for Processing, consent may be withdrawn at any time.

G. Processing Special Category Data

23. Special Category Data is subject to additional controls in comparison to ordinary personal data. When processing Special Category Data, in addition to a lawful basis set out in 22 above, CCCG is required under the UK GDPR to have an additional lawful basis for processing, such as:

    - the data subject has given their explicit consent;
    - the processing of special category data is to perform or exercise obligations or rights in relation to employment, social security or social protection law;
    - the Processing is necessary to ensure the vital interest of the data subject or another person, where the individual is physically or legally incapable of giving consent;
    - the special category data has already been made manifestly public by the data subject;
    - the processing is necessary for the reasons of substantial public interest as defined by the DPA 2018, Schedule 1, Part 2 (e.g. safeguarding, preventing/detecting unlawful acts);
    - the processing is required for occupational health, absence management or the provision of health and social care services or treatment; or
    - the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

    In some cases CCCG has a legal obligation to Process Special Category Data; for example the funding agency requires CCCG to pass on data with respect to ethnicity, physical and mental health, and to share this information with them. Where there is not a legal obligation or the processing is not in the substantial public interest as defined by the law Protection and CCCG decides that Special Category Data should be Processed, this will usually be done on the basis of consent and the individual has the choice as to whether or not to opt in to such

Processing. Individuals can withdraw consent at any time. CCCG adheres to the definition of consent as defined within the UK GDPR which is as follows:

Consent is 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

24. In order to ensure a safe work place and that CCCG complies with other areas of the law, such as equal opportunities, there is a requirement to process special category data in relation to gender, race, criminal convictions or health. Also in some instances, the processing of some types of special category personal data is a condition of acceptance of a student onto a course and is a condition of employment for staff.

25. CCCG may also ask for information about particular health needs such as allergies to particular forms of medication or foods or any conditions such as asthma and diabetes. CCCG will only use the information in the protection of the health and safety of the individual and in the event of a medical emergency and so far as is necessary to comply with disability discrimination law.

26. Some jobs or courses will bring staff, job applicants and students into contact with children including young people between the ages of 16 and 18 years. CCCG's statutory safeguarding duty and other education legislation require it to ensure that they are not barred form working with children or are otherwise suitable for the job or where the course involves Regulated Activities as defined by the Safeguarding Vulnerable Groups Act 2006, the students are suitable for those courses. CCCG also has a duty of care to all staff and students and must therefore ensure that employees and those who use the CCCG's facilities do not pose a threat or danger to other users.

H. Data Sharing

27. CCCG will comply with the relevant legislation with respect to the sharing of personal data. For example, if the Police make a request for personal data associated with carrying a criminal investigation the CCCG will share personal data as long as a legitimate reason is provided and assurance is confirmed that the request is legitimate. Also CCCG is required to supply personal data if requested to the relevant local child protection / safeguarding Board in line with its statutory safeguarding duty in respect of children (learners who are under 18). CCCG may also provide personal data to the Local Adult Safeguarding Board where necessary for safeguarding purposes in respect of learners who are classified as a vulnerable adult. In all cases the Designated Controller for the relevant area of CCCG must agree to the request and authorisation must be sought by the member of staff who is sharing the information.

28. When sharing personal data in line with approved and authorised protocols (for example if a query is being made by or with a funding agency) then personal data must be sent in encrypted format.

I. Subject Access Request

29. Individuals have the right under the UK GDPR to have confirmed whether CCCG processes their personal data and to be provided with a copy of their personal data. Any person who

wishes to exercise this right should complete the Access to Information form and give it to their personal tutor or relevant manager or head of their section, department or service area (see Appendix 6).

30. The CCCG aims to comply with requests for access without undue delay and at the latest within one month of receipt unless there is a good reason for delay. In such cases, the reason for delay (which should be no more than a further two months) should be explained, in writing, to the Data Subject making the request.

J. Examination Marks

31. Students are entitled to information about their examination marks for both course work and examinations. Students are to be made aware that they are not entitled to view this information prior to the official publication date. The publication of examination results at an individual level requires the consent of the individual concerned. Students are not entitled to have access to examination scripts, though they can see any comments on their performance made on those scripts. CCCG however may use data on an anonymous and combined basis to carry out analysis of performance in relation to teaching, learning and assessment

K. Retention of Data

32. CCCG is required to ensure that it only retains personal data for as long as is necessary to fulfil the original Processing purpose for which it was collected. CCCG manages the retention of personal data through setting retention periods after which data will be deleted or archived. Retention periods are set based on legal and regulatory requirements and good practice guidance.

33. CCCG will keep some forms of information for longer periods of time than others. Constraints on storage space determine that information about students cannot be kept indefinitely unless there are specific requests to do so. In general, information about students held in manual files will be kept for a maximum of five years after the student has left college. This will include:

    - name and address;
    - academic achievements including marks for course work; and
    - copies of any references given.

34. Retention periods for different categories of personal data are decided by the respective department that holds the personal data. The following principles will be adhered in ensuring that data is stored, archived and cleared at the end of the retention period:
    - A period will be defined after which the hard copy data will be archived. This will include the method of where and how to store data.
    - A yearly process will be followed by departments to go through all data that is held including, those that are archived, with records deleted that have reached the end of the retention period.
    - Where an archiving company holds the data, retention periods will be informed with check to ensure that data has either been brought back to CCCG to remove/delete the data when retention period is over or is deleted by the company themselves.

35. CCCG's Retention of Records Schedule is attached (Appendix 7)

L. CCTV

36. CCCG utilise Closed Circuit Televisions (CCTV) on an evidentiary basis when incidents of crime or misconduct have been alleged. CCTV data is held securely for thirty days before being permanently erased. The data is sealed, and only authorised individuals may be able to view the data. Permission must be sought and granted from CCCG's Data Protection Officer before any downloads can take place.

M. Training

37. CCCG will provide training to its staff to ensure that they are cognisant of their responsibilities, however as referenced above it is the responsibility of staff to ensure that they conduct themselves in line with this policy. All newly appointed staff will be required to complete a data protection training module as part the onboarding process.

N. Contact us

CCCG (as The WKCIC Group) is registered with the Information Commissioner's Office as a data controller under the reference ZA254956.

Our address is 211 Grays Inn Road, London WC1X 8RA

CCCG's Data Protection Officer can be contacted by email at: dataprotection@capitalccg.ac.uk.

APPENDIX 1

Student privacy notice

Contents

A. Introduction

The purpose of this notice is to inform students about how the college collects, uses and shares their personal data, and their rights in relation to the personal data we hold.

This notice is available on the college website.

Date 01/06/2022

B. Who processes your personal data?

Capital City College Group (CCCG) determines why and how your personal data is used and is considered to be the data controller of the personal data. This places legal obligations on the college group.

CCCG consists of the following colleges and training organisations:

- City and Islington College
- The College of Haringey, Enfield and North East London
- Westminster Kingsway College
- Capital City College Training

CCCG is registered under its licence name of The WKCIC Group with the Information Commissioner's Office as a data controller under the reference A8187792.

Our address is 211 Grays Inn Road, London WC1X 8RA

The college's Data Protection Officer can be contacted by email at: dataprotection@capitalccg.ac.uk

C. What personal data do we process

CCCG processes personal data that is necessary for us to administer and deliver education services to you. This includes:

- information about you and your study and your communications with us including details of your education, qualifications and publications.
- financial information gathered for the purposes of administering fees and charges, loans, grants, bursaries etc.
- copies of passports, visas, and other documents required to ensure compliance with the regulations of our funding organisations.
- photographs and other identification information for student ID cards.
- information about your participation and progression in learning and assessment activities and
- information about your use of learning materials.

Special category data
We may also process “special category data" which includes information about your racial or ethnic origin, religious beliefs or other beliefs, physical and mental health and any disability you may have. We may also process information concerning any criminal offences or criminal proceedings.

D. The legal basis for processing your personal and special category data

(i) Contract

We may process your personal data and special category data because it is necessary for us to do so in order to fulfil the contract you enter into with the college when registering as a student or in order to take steps at your request prior to entering into a contract.

The college collects and processes personal information that is necessary to provide the required services to you for the contract and also to meet its legal and statutory obligations in delivering the contract, including:

- securing grant funding to cover the cost of your education
- the collection of any fee you owe us, or a third party (for example your employer)

(ii) Legitimate interests

We may use and process your personal information where it is necessary for us to pursue our legitimate interests or a third party's legitimate interests. Such legitimate interests can include:

- monitoring your attendance at lectures and other learning activities
- the recording of educational activities including lecture capture
- monitoring and investigating the use of IT services to maintain network and information security
- testing our systems to ensure optimum performance
- verifying the accuracy of data that we hold
- improving our services via staff training
- promoting equality and diversity throughout the college
- tracking your progress into further learning or employment
- staying in touch with you after you graduate including fundraising

(iii) Legal obligation

We may also process your personal data for our compliance with legal obligations. This can include:

- compliance with regulatory obligations such as anti-money laundering laws and safeguarding requirements
- assisting with investigations (including criminal investigations) carried out by the police and other competent authorities
- complying with court or other competent authority orders

(iv) Vital interests

The college will rely on vital interests as a lawful basis for processing your personal data where it is necessary to provide a safe environment for your protection and the protection of others. This includes the investigation and prevention of inappropriate activity

(v) Consent

The college will use consent as a lawful basis for some processing. Where we do so we always provide you with the choice as to whether or not to opt in to such processing.

- We will provide academic references and confirmation of study to prospective employers and to your local authority or council, with your consent.
- We may process personal data provided by you for a specific purpose or purposes (for example, disability, catering preferences or lifestyle status for event management)

E. What we use personal and sensitive data for

CCCG processes your personal and special category data for the following reasons:

- the provision of teaching and associated services (e.g. registration, assessment, graduation and the administration of parents' evenings)
- maintaining student records
- promoting the welfare of students
- to communicate with you for all matters relevant to your study at the college
- providing library, IT and information services
- administering student finances
- managing college accommodation
- managing the use of college services (e.g. student support services, careers service)
- equal opportunities monitoring
- evaluating the performance and effectiveness of the college including research and statistical analysis
- to meet our compliance and regulatory obligations
- the prevention and detection of crime and assisting investigations carried out by relevant authorities
- dealing with disciplinary matters
- dealing with complaints
- If you are aged under 18, or under 24 with an Education and Health Care Plan, a responsible adult you have nominated on your enrolment form.

F. Automated decision making

The college does not make any automated decisions about you using your personal data.

G. Who we share your personal data with

Your data will be shared internally within the college with staff and departments that require the use of the data in order to administer your study and provide college services to you.

Data including your personal and sensitive data will be shared externally where the college has a legitimate need to do so in fulfilling the contract the college has with you or has a legal obligation to provide data. The following list provides examples of the most common occasions on which it is necessary to share your data.

- We will share some personal data (including your name, date of birth, email address, programme and level of study, start and end date and gender) with the college Students' Union if you have provided your consent at registration for your first year of study of your current programme. The Union use this information to communicate with you to provide services to you as a member of the Union. The sharing of data between the college and the Union is covered by a data sharing agreement. You can opt out at any time from the Student Union holding your data through our online student system.
- Other regulatory bodies that the college is legally required to provide data to including (HESA), Office for Students (OfS), Education and Skills Funding Agency (ESFA), Greater London Authority (GLA), Department for Education (DfE), National college for Teaching and Learning (NCTL), Student Loans Company, Quality Assurance Agency for Higher Education (QAA), Office for Standards in Education (OFSTED) and subject specific accreditation organisations. This may also include providing details to

third party organisations representing those bodies e.g. OfS use Ipsos Mori to conduct the National Students' Survey for which the college is required to provide the contact details of its students.

- Other third party organisations, covered by a data sharing agreement, where the college has a legitimate need to do so in fulfilling the contract it has with you.
- We will provide information to the police and other enforcement agencies in the event of an emergency or where required to assist the prevention or detection of crime.
- The college may also pass information about a student to an appropriate third party where there is concern about the welfare of a student to safeguard the interests of the student.
- We will provide information to UK Visas and Immigration (UKVI) where required in relation to students holding Student Route visas.
- Employers and organisations with whom placements are arranged as part of your programme of study in order to facilitate the placement.
- Employers of students studying on Apprenticeships programme.
- Other institutions when delivering provision in collaboration with CCCG.
- References to potential employers and other education institutions where the student has named the college or a staff member as a referee.
- Professional bodies where appropriate for the programme of study to validate and accredit qualifications.
- If you are aged under 18, or under 24 with an Education and Health Care Plan, a responsible adult you have nominated on your enrolment form, for the purposes of parents' evenings and other parents' communications regarding the progress of your study.
- We will share some personal data with our external supplier for the purpose of providing graduation gowns required for attendance at graduation ceremonies.

[1] HESA Student Collection Notices can be found at: https://www.hesa.ac.uk/about/regulation/data-protection/notices

H. Changes to your personal data

It is the responsibility of the student to notify the college as soon as possible if any of the data held about them needs to be updated or is incorrect. The college provides an opportunity annually for you as a student to check your details through the registration process and also requires students to notify changes more promptly directly to student services.

I. Will your data be sent or stored abroad?

Some of the personal data we process about you may be transferred to, and stored at, a destination outside the European Economic Area (EEA), for example where personal data is processed by one of our software suppliers who is based outside the EEA or who uses data storage facilities outside the EEA.

In these circumstances, your personal data will only be transferred where the transfer is subject to one or more of the appropriate safeguards for international transfers prescribed by applicable law (e.g. standard data protection clauses adopted by the European Commission); a European Commission decision provides that the country or territory to which the transfer is made ensures an adequate level of protection.

J. How long do we keep your personal data?

The college will retain personal data for no longer than is necessary to fulfil its contractual and regulatory obligations in line with the retention schedule in appendix 3 of the data protection policy which can be found here.

K. How you can access your personal information we hold, and other rights you have

1. The right to be informed

You have the right to be informed about the collection and use of your personal data and this privacy notice is part of the transparency requirements of data protection legislation.

2. Right of access

You have a right of access to your own personal data held by the college. Most data held about you is available for you to view online through our online student system whilst a student of the college. Furthermore, a request to see the personal data held by the college can be made through a Subject Access Request.

3. The right to rectification

You have the right to have inaccurate personal data held by the college rectified or completed if it is incomplete. This can be done through our online student system or by contacting the Student Administration teams at:

courseinfo@candi.ac.uk
courseinfo@westking.ac.uk
courseinfo@conel.ac.uk
employer@capitalcct.ac.uk

4. The right to erasure

Once personal data collected by the college is no longer necessary for the purpose for which it was collected and processed, you may have the right to have the data erased. The college manages the retention period of data held through its retention schedule.

5. The rights to restrict processing and to object to processing

In certain circumstances you have the right to restrict the processing of your personal data. This is likely to arise when there is an issue concerning the accuracy or the legitimate grounds for processing of the personal data.

6. The right to object to processing

You have the right to object to:

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

The college will stop processing the personal data unless there are compelling legitimate grounds for the processing, which override your interests, rights and freedoms.

7. Rights to data portability

You have the right to receive the personal data concerning you in a structured, commonly used and machine-readable format. The college will respond to any Subject Access Requests in compliance with this. You have the right to obtain information which the college holds about you by making a subject access request – by completing appendix 2 of the data protection policy which can be found here.

In line with its policy the Group aims to comply with requests for access without undue delay and at the latest within one month of receipt unless there is a good reason for delay. In such cases, the reason for delay should be explained, in writing, to the data subject making the request.

Note:
Detailed guidance on all of the rights you have with regard to the personal data that we hold and process about you is available on the ICO website here - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/.

L. Contact us

If you have any queries about this privacy notice or how we process your personal data you can contact us at: dataprotection@capitalccg.ac.uk.

If you are not satisfied with how we are processing your personal data, please in the first instance contact our Data Protection Officer by email at: dataprotection@capitalccg.ac.uk. You can also report a concern about how your information has been handled to the Information Commissioner - https://ico.org.uk/concerns/handling/.

CCCG Privacy Notice for Employees, Workers and Contractors

What is the purpose of this document?

The purpose of this notice is to explain to you how Capital City College Group ("CCCG") may use your personal data collected from you during and after your working relationship with us.

It applies to all employees, workers and contractors.

CCCG determines why and how your personal data is used and, as such, is the data controller of your personal data. This places specific obligations on CCCG including that personal data must be processed fairly and lawfully and in a transparent manner.

CCCG is registered with the Information Commissioner's Office as a data controller under the reference ZA254956.

Our address is 211 Grays Inn Road, London, WC1X 8RA

CCCG's Data Protection Officer can be contacted by email at: dataprotection@capitalccg.ac.uk

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

The kind of data we process about you

Personal data is any information relating to a living individual from which that person can be identified directly or indirectly. It does not include data where the identity has been removed (anonymous data).

There are special categories of more sensitive personal data which require a higher level of protection. Special category personal data includes information about your racial or ethnic origin, religious or other philosophical beliefs, biometric data, data concerning physical or mental health or data concerning an individual's sex life or sexual orientation.

We collect personal data about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, or other background check agencies e.g. Disclosure and Barring Service. We will collect additional personal data in the course of job-related activities throughout the period of you working for us.

We will collect, store, and use the following categories of personal data about you:

- Your name, title, address and contact details including your telephone numbers and personal email address, date of birth and gender;
- Marital status, next of kin, dependents and emergency contact information;
- National Insurance number;
- Bank account details, payroll records and tax status information;
- Salary, annual leave, pension and benefits information, e.g. sick pay;
- Terms and conditions of your employment, start and end dates with previous employers and with CCCG, and details of your qualifications, skills and experience;

- Location of employment or workplace;
- Copy of driving licence (where applicable);
- Recruitment information (including copies of right to work documentation, references and other information included in an application or CV or cover letter or as part of the application process);
- Employment records (including job titles, work history, working hours and working hours, attendance at work, training records, professional memberships, nationality and entitlement to work in the UK);
- Compensation history;
- Assessment of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- Disciplinary and grievance information, including any warnings issued, and related correspondence;
- CCTV footage and other information obtained through electronic means such as swipecard records;
- Information about your use of our information and communications systems; and photographs.

We may also collect, store and use the following special category personal data:

- Information about your race or ethnicity, religious beliefs, sexual orientation and
- political opinions;
- Trade union membership;
- Information about your health, including any medical condition, health and sickness records including whether or not you have a disability for which CCCG needs to make reasonable adjustments;
- Genetic information and biometric data; and
- Information about criminal convictions and offences.

How will we use your personal data?

We will only process your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest (or for official purposes).

If you fail to provide personal data

If you fail to provide certain personal data when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance

with the above rules, where there is a lawful basis for it in accordance with data-protection law.

Do we need your consent?

We do not need your consent if there are other lawful bases justifying the processing of your personal data as provided by data-protection law. For example, we do not need your consent when we use special category personal data in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data, where there is no other lawful basis justifying that processing. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us and you have the right to withdraw consent at any time.

How we use special category personal data

Special category personal data require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations or exercise rights in connection with employment.
- Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. (We may also process such information about members of staff or former members of staff in the course of legitimate business activities with the appropriate safeguards).

Information about criminal convictions

We may only use personal data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our legal obligations, for example safe recruitment of staff who have regular contact with learners who are under 18 in the normal course of their duties and provided we do so in line with our Data Protection Policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such personal data about members or former members in the course of legitimate business activities with the appropriate safeguards.

We do not envisage that we will hold personal data about criminal convictions.

We will only collect personal data about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect personal data about criminal convictions as part of the recruitment process or we may be notified, where appropriate, directly by you in the course of you working for us.

We are allowed to use your personal data in this way to carry out our legal obligations. We have in

place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal data to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request a reconsideration.
- Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal data, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

The legal basis on which we collect and use your personal data

We collect and use your personal data in the list above on the basis that it is necessary for performing our employment contract with you, or it is necessary to take steps before entering into the contract with you. We also collect and use your personal information on the basis that we need to do so in order to comply with our legal obligations.

In some cases we may use your personal data to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal data are listed in the table below as well as indicating which categories of data are involved:

Purpose	Legal basis/justification
To make a decision about your recruitment or appointment.	Necessary prior to entering into an employment contract and to comply with Employment Law.
To enter into and perform our obligations under our employment contract with you and exercise our rights.	Necessary for the performance of the employment contract and to comply with Employment Law.
To provide references on request.	Necessary for the performance of the employment contract or where consent has been given.
To monitor equality, diversity and inclusion.	Necessary in our legitimate interest to promote an inclusive work environment and to comply with employment law and our other legal obligations.
Immigration matters.	Necessary for us to comply with our legal obligations. Such processing may also be in the public interest and your consent may be required in some cases.
CCTV	Necessary for our legitimate interest in ensuring

	the safety of CCCG community and our property and assets.

How we use particularly sensitive personal data

Purpose	Legal basis/justification
We use information relating to your health to make decisions regarding reasonable adjustments.	Processing of health-related data is necessary so that we can meet our obligations under employment law.
We use information about your race or ethnicity, religious beliefs, sexual orientation and political opinions to conduct equal opportunities monitoring.	Processing is necessary in the public interest and so that we can meet our obligations under employment law (public sectory equality duty).
We use trade union membership information to pay trade union premiums, register that status of a protected employment and to comply with Employment Law obligations.	Processing is necessary so that we can meet our obligations under employment law.
We use information about your criminal convictions where the law allows us to do so and if it is appropriate given the nature of the role to assess your suitability to carry out the work for which you are being engaged.	Processing is necessary in the public interest and in the substantial public interest (e.g. preventing unlawful acts by safer recruitment of those working with learners who are under 18) .

Data sharing

Your data will be shared internally within CCCG only with staff and departments that require the use of the data in order to administer your employment and provide services to you. Data including your personal and special category personal data will be shared externally with third parties where required by law, where it is necessary to administer the contractual relationship with you or where we have a legitimate interest in doing so.

Why might you share my personal data with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the contractual relationship with you or where we have a legitimate interest in doing so.

Which third-party service providers process my personal data?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within CCCG. The following activities are carried out by third-party service providers: payroll, pension administration, occupational health assessment and absence recording.

How secure is my personal data with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal data in line with our policies (and data-processing contracts?). We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal data with other entities in the group?

We will share your personal data with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise,

for system maintenance support and hosting of data.

What about other third parties?

We may share your personal data with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal data with a regulator or to otherwise comply with the law.

Transferring information outside the EU

We do not transfer your personal data outside of Europe.

Data security

We have put in place measures to protect the security of your personal data.

Third parties will only process your personal data on our instructions and where they have agreed to treat your personal data confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

How long we keep your personal data for

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal data are available in our Retention Policy which is available on the intranet. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal data so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal data in accordance with Retention Policy.

Your rights in connection with personal data - Rights of access, correction, erasure, and restriction

Under certain circumstances you have the right to:

- Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal data. This enables you to ask us to delete or remove personal

data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).

- Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal data for direct marketing purposes.
- Request the restriction of processing of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal data to another party.
- Withdraw consent to the processing of your personal data. In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Officer at dataprotection@capitalccg.ac.uk. Once we have received notification that you have withdrawn your consent, we will no longer process your personal data for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

If you want to review, verify, correct or request erasure of your personal data, object to the processing of your personal data, or request that we transfer a copy of your personal data to another party, please contact the Chief People Officer in writing.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

Your duty to inform us of changes

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

Data Protection Officer

We have appointed a Data Protection Officer (DPO) to oversee our compliance with data protection legislation. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Changes to this Privacy Notice

We reserve the right to update this Privacy Notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal data.

If you have any questions about this Privacy Notice, please contact the Data Protection Officer

APPENDIX 3

STAFF GUIDELINES FOR DATA PROTECTION

1. All staff will Process data about students on a regular basis when marking registers, writing reports or references or as part of a pastoral or academic supervisory role. You must only use Personal Data when there is a lawful basis for doing so. The information that you deal with on a day-to-day basis will be 'standard' and will cover categories such as:

    - general personal details such as name and address;
    - details about class attendance, course work marks and grades and associated comments; and
    - notes of personal supervision including matters about behaviour and discipline.

2 Information about a student's physical or mental health, ethnicity or race, is considered Special Category Data and can usually only Processed with the students' explicit consent. If you need to record this information, you should use the standard consent form (e.g. Student Services may want to keep information about dietary needs for religious or health reasons prior to taking students on a field trip, or that a student is pregnant).

3 All staff have a duty to make sure that they comply with the Data Protection principles which are set out in the Data Protection Policy. In particular, you must ensure that the Personal Data that you process is:

    - up to date and accurate;
    - being processed fairly;
    - kept securely;
    - adequate, relevant and limited to what is necessary and
    - disposed of safely and in accordance with the CCCG policy.

4. Staff must not disclose Personal Data to any student unless for normal or academic or pastoral purposes without authorisation or agreement from the Designated Data Controller or in line with CCCG's policy.

5. Staff shall not disclose Personal Data about staff or students to any other staff member except with the authorisation or agreement of the Designated Data Controller or line with the College policy unless it is necessary for legitimate educational or safeguarding purposes

6. Staff should understand their responsibilities for data protection and security when dealing with Personal Data on computers or in files away from the workplace or by means of remote access to CCCG's network from home or away from the work environment:

    - if the computer, laptop, tablet or mobile belongs to CCCG then it is not used by other household members;
    - only equipment designed to be portable is taken from the workplace;
    - if it is their own computer then CCCG data is not accessible to anyone else, i.e. password protected and all files are deleted when no longer needed;
    - virus protection is in place;
    - any print-outs are stored and disposed of carefully;
    - suitable transport is provided between home and work so that equipment data and manual files remain secure whilst in transit;
    - any loss, unauthorised destruction, or disclosure of data may result in disciplinary investigation

- computer files brought to work from outside the college environment are virus checked before loading onto CCCG's computer equipment;
- no personal files, containing information about staff or students, can be taken from the college environment without the express permission of the Line Manager and/or the designated Data Controller. Staff will be asked by their Line Manager/designed Data Controller to complete an authorisation form, which should be signed and dated by their Line Manager and/or the designated Data Controller. Personal Data files must not be left unattended at any time except when locked in a filing cabinet drawer or similar equipment; and
- Staff should not hold Personal Data belonging to students on their mobile phone, unless they have gained express permission from the student/s in question.

7. Before Processing any Personal Data, all staff should consider:
   a) whether the information needs to be Processed by CCCG and whether the Processing of the Personal Data fit within the purposes of providing education and training;
   b) if there is additional information that we are asking the student to supply (e.g. ethnicity), has the student / staff member given explicit consent for CCCG to Process this information.

8. Staff should never share Personal Data without being sure that they are permitted to do so. If in doubt staff should check with their data controller who in normal circumstances will be the Director of their service area.

9. If a staff member is asked by a student what Personal Data CCCG holds about them, then they should be directed to the student privacy notice which can be found on the CCCG website. This is particularly relevant at the time of enrolment.

Data Breach Policy and Procedures

1. Introduction

1.1 Every care is taken to protect Personal Data from incidents (either accidental or deliberate) to avoid a data protection breach that could compromise security.

1.2 Compromise of information or confidentiality may result in harm to staff or students, reputational damage or legislative non-compliance, and ultimately a fine from the ICO.

2. Purpose and Scope

2.1 CCCG's Data Breach Policy should be read in conjunction with its Data Protection Policy and has been designed to ensure the security of all Personal Data during its lifecycle. It sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across CCCG.

2.2 This Policy relates to all Personal Data and Special Category Data held by CCCG regardless of format.

2.3 This Policy applies to all staff and students at CCCG. This includes temporary, agency staff, contractors, consultants, suppliers and data processors working for, or on behalf of CCCG.

2.4 The objective of this Policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure Personal Data and prevent further breaches.

3. Types of Data Breaches

3.1 For the purpose of this Policy, data security breaches include both confirmed and suspected incidents.

3.2 An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to CCCG's information assets and / or reputation.

3.3 An incident includes but is not restricted to, the following:

- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record);
- equipment theft or failure;
- system failure;
- unauthorised use of, access to or modification of data or information systems;
- attempts (failed or successful) to gain unauthorised access to information or IT system(s);
- unauthorised disclosure of sensitive / confidential data;
- website defacement;
- hacking attack;
- unforeseen circumstances such as a fire or flood;
- human error; and
- cases where information is obtained by deceiving the organisation who holds it.

4. Reporting an incident

4.1 Any individual who accesses, uses or manages CCCG's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer.

4.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

4.3 The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. A Data Breach Report form should be completed as part of the reporting process (refer to Appendix 5).

4.4 All staff should be aware that any breach of data protection legislation may result in CCCG's Disciplinary Procedures being instigated.

5. Containment and recovery

5.1 The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

5.2 An initial assessment will be made by the DPO in liaison with the relevant designated data controller to establish the severity of the breach and will decided whether an investigation needs to take place or not. If the DPO decides that the severity of the case requires an investigation then an investigating officer (IO) will be appointed; this will usually be a designated data controller from another department within CCCG.

5.3 The IO will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

5.4 The DPO (and the IO, if an investigation is warranted) will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

5.6 The DPO (and the IO, if an investigation is warranted) in liaison with the Designated Data Controller will determine the suitable course of action to be taken to ensure a resolution to the incident.

6. Investigation and risk assessment

6.1 If a decision is made to appoint an IO, they will undertake an investigation immediately, if possible, within 24 hours of the breach being discovered / reported.

6.2 The IO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

6.3 The investigation will take into account the following:

- the type of data involved;
- its sensitivity;
- the protections in place (e.g. encryptions);
- what has happened to the data (e.g. has it been lost or stolen);
- whether the data could be put to any illegal or inappropriate use;
- data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s); and
- whether there are wider consequences to the breach.

7. Notification

7.1 The DPO in liaison with the IO (if appointed) and the Designated Data Controller will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach.

7.2 Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under data protection legislation;

- Individual Rights as defined by the ICO: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/
- whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks);
- whether notification would help prevent the unauthorised or unlawful use of Personal Data;
- whether there are any legal / contractual notification requirements; and
- the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

7.3 An individual or individuals whose Personal Data has/have been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting their rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact CCCG for further information or to ask questions on what has occurred.

7.4 The DPO (and IO if appointed) will consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

7.5 The DPO, in consultation with the Group Leadership Team will consider whether communications and marketing team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

7.6 A record will be kept of any Personal Data breach, regardless of whether notification was required.

8. Evaluation and response

8.1 Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

8.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

8.3 The review will consider:
- where and how personal data is held and where and how it is stored;
- where the biggest risks lie including identifying potential weak points within existing security measures;
- whether methods of transmission are secure; sharing minimum amount of data necessary;
- staff awareness; and
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

8.4 If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Group Leadership Team.

8.5 The Audit Committee will be informed of any data breaches that have occurred since their last meeting. If no data breaches have occurred to a year the audit committee will informed of a nil return on annual basis (usually at their October meeting).

APPENDIX 5

CAPITAL CITY COLLEGE GROUP

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify your line manager / head of department immediately.

Please complete this notification form and email to graham.drummond@capitalccg.ac.uk

Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

APPENDIX 6

SUBJECT ACCESS REQUEST FORM FOR ACCESS TO PERSONAL DATA

I **[insert name]** …….. wish to have access to either
(delete as appropriate):

1 All the data that CCCG currently has about me either as part of an automated system or part of the relevant filing system, or

2 Please specify what personal data you would like CCCG to supply – e.g. disciplinary records, academic marks or course work details. Providing dates will assist staff in locating the information – please also give names of the tutor / course manager:

Name (in full) _____

Student number _____:

College course attended _____

Date of Birth _____

Address to which information is to be sent (or provide email address):

_____

_____

_____

Daytime contact telephone number:

_____

For Office Use Only

Request for information received on ……..

Information sent to enquirer on ……..

Signed (Designated Data Controller ……

APPENDIX 7

Capital City College Group – Retention of Data / Information Schedule

Section 1 - Staff Related Data

No	Type of Data	Retention Period	Designated Data Controller
1.1	Income Tax and NI returns; correspondence with Tax Office	6 years after the end of the financial year to which the records relate	Director of Finance
1.2	Statutory maternity pay records and calculations	6 years after the end of the financial year to which the records relate	Director of Finance
1.3	Statutory sick pay records and calculations	6 years after the end of the financial year to which the records relate	Director of Finance
1.4	Wages and salary records	6 years from the last date of employment	Director of Finance
1.5	Records and reports of accidents	3 years after the date of the last entry	Director of Estates & Facilities
1.6	Records relating to events notifiable under the Retirement Benefits Scheme ie records concerning decisions to allow retirement due to incapacity, pensions accounts and associated documents	6 years from the end of the scheme year in which the event took place or the date upon which the accounts/reports were signed/completed	Director of Finance
1.7	Medical records as specified under the control of substances hazardous to health regulations	40 years	Director of Estates and Facilities
1.8	Personnel Files: training records; notes of grievances and disciplinary hearings	6 years from the end of employment	Chief People Officer
1.9	Facts relating to redundancies (less than 20)	6 years from the date of redundancies	Chief People Officer
1.10	Facts relating to redundancies (20 or more)	6 years from the date of redundancies	Chief People Officer
1.11	Health records	6 years from the last date of employment	Chief People Officer
1.12	Health Records where reason for termination of employment is concerned	6 years from the last date of employment	Chief People Officer

	with health, including stress related illness		
1.13	Sickness absence monitoring records	6 years from the last date of employment	Chief People Officer
1.14	Applications forms and interview notes (for unsuccessful candidates)	6 months from the date of the decision	Chief People Officer
1.15	Professional development records and files	6 years from the last date of employment	Chief People Officer
1.16	Parental leave	6 years from the last date of employment	Chief People Officer
1.17	Pension scheme investment policies	12 years from the ending of any benefit payable under the policy	Director of Finance
1.18	Pensioners' records	12 years after benefit ceases	Director of Finance
1.19	Trade union agreements	10 years after ceasing to be effective	Chief People Officer

Section 2 – Finance Data / Information

No	Type of Data	Retention Period	Designated Data Controller
2.1	Financial records including invoices, receipts, ledgers and accounts	7 years	Director of Finance
2.2	Inland Revenue approvals	permanently	Director of Finance
2.3	Pension scheme investment policies	12 years from the ending of any benefit payable under the policy	Director of Finance
2.4	Pensioners' records	12 years after benefit ceases	Director of Finance
2.5	Employers' liability certificate	20 years	Director of Finance
2.6	Payroll data	10 years following cessation of employment	Director of Finance
2.7	Published financial accounts	Indefinitely	Director of Finance
2.8	Tenders and time expired contracts	7 years	Director of Finance
2.9	Internal and external audit reports	7 years	Director of Finance

Section 3 – Student Related Data / Information

No	Type of Data	Retention Period	Designated Data Controller
3.1	Student MI records	7 years	Director of Integration and Information

3.2	Student files, including academic achievements and conduct	6 years from the last day of the course; 10 years with the consent of the student for personal and academic references	Heads of Quality / CCCT Managing Director
3.3	Examination and assessment records, including pass lists/awards lists and correspondence with examination bodies	Termination of relationship with student + 6 years	Director of Integration and Information
3.4	Student surveys/feedback from students, including complaints	Current year plus 3 years	Director of Performance and Quality
3.5	Student records: eg Learner support, Access Fund payments, Childcare etc	Completion of student's programme + 6 years	Heads of Quality / CCCT Managing Director
3.6	Confidential student records eg referral to external agencies	2 years	Heads of Quality / CCCT Managing Director
3.7	Tutorial records	Completion of student's course plus 3 years (NB excluding summaries extracted for reference purposes – see 4.2 above)	Heads of Quality / CCCT Managing Director
3.8	Coursework samples	Current academic year plus 1 year	Heads of Quality / CCCT Managing Director
3.9	Assignments/course log	Life of course	Heads of Quality / CCCT Managing Director
3.10	Handouts, WebPages, learning resources	Life of course	Heads of Quality / CCCT Managing Director
3.11	Course grade/mark sheets	Termination of relationship with student + 6 years	Heads of Quality / CCCT Managing Director
3.12	Course induction programme/course handbooks	Life of course	Heads of Quality / CCCT Managing Director

Section 4 – College Performance Data / Reports

No	Type of Data	Retention Period	Designated Data Controller
4.1	College development plans including retention and achievement date	4 years	Director of Governance

4.1	External inspection reports and reviews	4 years	Director of Performance and Quality
4.2	EV reports and action plans	Current academic year plus 3 years	Director of Performance and Quality
4.3	Course submissions/approvals (external)	Life of course plus 4 years	Head of Examinations
4.4	Any/all individual course review documentation	Current academic year plus 3 years	Heads of Quality / CCCT Managing Director
4.5	Curriculum SARs and action plans	Current academic year plus 3 years	Heads of Quality / CCCT Managing Director
4.6	Divisional/Centre SARs and action plans	Current academic year plus 3 years	Heads of Quality / CCCT Managing Director
4.7	College SARs and action plans	Current academic year plus 3 years	Director of Performance and Quality

Section 5 – Corporate Data / Reports

No	Type of Data	Retention Period	Designated Data Controller
5.1	Data protection registration	10 years	Director of Governance
5.2	Software licenses and hardware registers	5 years	Director of IT
5.3	Minutes of the Governing Body and its committee	In perpetuity	Director of Governance
5.4	Agendas and papers of Corporation and Committees	10 years	Director of Governance
5.5	Policies approved by the Corporation	In perpetuity or until updated/superseded	Director of Governance
5.6	Deeds and titles relating to property	In perpetuity	Director of Governance

Data Privacy Impact Assessment Framework – Addendum to the Data Protection Policy

1. Introduction

1.3 A Data Protection Impact Assessment (DPIA) is a process which assists CCCG identify and minimise risks associated with the implementation of projects which involve personal data, including the use of new technologies..

1.4 A DPIA must be carried out for all projects where there is a risk to the rights and freedoms of Data subjects, including the risk of a personal data breach.

2. Purpose and Scope

2.1 This framework should be read in conjunction with the CCCG's Data Protection Policy and its Data Breach Policy which has been designed to ensure the security of all personal data during its lifecycle. It sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the CCCG.

2.2 This Policy relates to all personal and Special Category Data held by the CCCG regardless of format. Its aim is to provide guidance to those that need to carry out a DPIA for projects involving Personal Data.

3. The Assessment

3.1 If a project involves Personal Data, then a DPIA must be included within the project brief / proposal and be approved by the Group Leadership Team. The writer of the project proposal should discuss the potential implications for data protection with CCCG's DPO.

3.2 The following headings should be used as part of the DPIA:

- the nature, scope, context and purpose/s of the Processing;
- assessment of the necessity, proportionality and compliance measures;
- identification and assessment of the risks to individuals, with details of:
  - identification of measures to mitigate those risks
  - the likelihood and the severity of any impact on individuals (e.g. high risk could result from either a high probability of some harm, or a lower possibility of serious harm)

3.3 If the risk is high then the lead staff members must consult with the DPO and where appropriate, individuals and relevant experts. If a high risk is identified which cannot be identified then ICO may need to be contacted. The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, the ICO may issue a formal warning not to Process the data, or ban the Processing altogether.