Capital City College Group Data Protection Policy and Procedures

Author:	Graham Drummond	**Approved by:**	GLT and Audit Committee
Version:	3	**Date of Approval**:	(November 17 Audit Committee) Reviewed by GLT November 18
Equality Impact Assessed	November 17	**Review Date:**	November 21

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.

2. In line with article 5 of the General Data Protection Regulation, 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;
    - Processed in a manner that ensures appropriate security of the personal data

3. CCCG staff and others who process or use any personal information 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

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

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

6. 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 information has been used for personal gain). 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.

B. Designated Data Controllers and the Data Protection Officer

7. As a public authority as defined by data protection legislation the Group is required to comply with the General Data Protection Regulation (GDPR). Whilst ultimate responsibility for compliance rests with the CCCG Board, the day to day compliance to GDPR is the responsibility of all members of staff and the management of the Group.

8. In order to ensure ongoing compliance with data protection legislation there is a steering group which oversees the management and control of data. This steering group is chaired by the Director of Governance who also serves as the Group's Data Protection Officer (dataprotection@capitalccg.ac.uk). The remaining members of this group consist of designated data controllers for key areas of the Group's operations. The table below gives details of these data controllers:

Department / Division within the Group	Designated Data Controllers
WKC teachers / lecturers	College Director for Learner Experience
CIC teachers / lecturers	Deputy Director, Learner Experience
CONEL teachers / lecturers	The Principal
CCCT	Operations Director
Management Information Services / Registry / Examinations	Director Management Information
Finance	Director of Financial Services
Marketing	Director of Marketing
Human Resources	Head of Human Resources

9. Under the GDPR legislation it is mandatory to appoint a data protection officer. This role is performed by the Director of Governance for the Group 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
- Chair the Group's data protection steering group

C. Rights of Students and Staff

10. 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 staff and students and other users for whom the Group may hold personal information (data subjects) are entitled to the following rights:

- the right to ask what personal information CCCG holds about them and to have access to a copy of their personal information;
- the right to ask to correct any errors in their personal information;

- the right, in certain circumstances such as where personal information is no longer needed, to request that CCCG restricts the use that is made of the personal information;
- the right, in certain circumstances, to ask CCCG to review and explain the legitimate interests in processing the personal data.

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/.

11. The Group provides all staff and students and other relevant users with privacy notices. The notices inform the individuals of the types of data the Group holds and processes about them and the reasons for which it is processed.

D. Responsibilities of Staff

12. All staff are responsible for:

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

13. 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 1. A separate privacy notice is available for staff and this gives details of what staff can expect from the Group in relation to dealing with their personal information and can be found HERE.

14. Staff should not pass personal information 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.

15. Staff must note that it is a criminal offence to use personal data that they have access to as part of their work and use it for their own personal or commercial reasons and can lead to prosecution.

Security of personal data

16. All staff are responsible for ensuring that any personal data which they process is kept securely (**personal data** is defined as any information relating to an identified or identifiable natural (living) person).

17. Personal information 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 the Group's ID card system and the CCTV security system. Personal information 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

18. CCTV images must be kept securely and be password protected – the appropriate documentation must be provided by Police and other Government Agencies quoting the DPA section.

19. 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.

E. Student Obligations

20. Students must ensure that all personal data provided to the Group 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 Group's computer facilities may from time to time have access to personal data about themselves. The Group can bear no responsibility for the sharing of personal information if this is carried out by the student themselves.

F. Lawful basis for using Personal Data

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

    Most commonly, we will use personal information in the following circumstances:

    - We will use and process personal data and special category data when 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.
- 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. Where we do so we always provide the individual with the choice as to whether or not to opt in to such processing.

G. Processing Special Category Data

22. **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. Special Category personal data is subject to additional controls in comparison to ordinary personal data.

    In some cases the Group has a legal obligation to process special category data; for example the funding agency requires the Group 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 and the Group decides that special category data should be processed, this will be done on the basis of consent and the individual has the choice as to whether or not to opt in to such processing. The Group adheres to the definition of consent as defined within the GDPR legislation 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.."

23. In order to ensure a safe work place and that the Group complies 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 personal data is a condition of acceptance of a student onto a course and is a condition of employment for staff.

24. The Group 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. The Group will only use the information in the protection of the health and safety of the individual and in the event of a medical emergency.

25. Some jobs or courses will bring staff and applicants for posts at the Group, and some students, into contact with children including young people between the ages of 16 and 18 years. The Group has a duty under the Children Act and other legislation to ensure that they are suitable for the job and students for the courses offered. The Group also has a duty of care to all staff and students and must therefore ensure that employees and those who use the Group's facilities do not pose a threat or danger to other users.

H. Data Sharing

26. CCCG will comply with the relevant legislation with respect to the sharing of personal information. For example, if the Police make a request for personal information associated with carrying a criminal investigation the Group will share personal information as long as a legitimate reason is provided and assurance is confirmed that the request is legitimate. Also CCCG is required to supply personal information if requested to the relevant local child protection / safeguarding Board in line with its duty of care to those students who are under the age of 18 or are classified as a vulnerable adult. In all cases the designated controller for the relevant area of the Group must agree to the request and authorisation must be sought by the member of staff who is sharing the information.

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

I. Subject Access Request

28. Individuals have the right under the GDPR to access the personal data that CCCG holds in relation to them 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 2).

29. 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.

J. Examination Marks

30. 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. The Group 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

31. 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.

32. 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
- copies of any references given

33. Details of retention periods for different categories of personal information are available in our retention policy. A retention of records schedule is attached.

L. Contact us

The Group (as The WKCIC Group) is registered with the Information Commissioner's Office as a data controller under the reference A8187792.

Our address is Longford Street, London NW1 3HB

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

APPENDIX 1

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 information 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
   - 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 only be collected and processed with the students' express 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 and
   - disposed of safely and in accordance with the Group 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.

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

- 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 does the processing of the 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 consent for CCCG to process and store this information.

8. Staff should never share personal information 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.

APPENDIX 2

SUBJECT ACCESS REQUEST FORM FOR ACCESS TO PERSONAL DATA (STUDENTS)

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 Data that the CCCG has about me in the following categories:

- **Academic marks or course work details**
- **Academic or employment references**
- **Disciplinary records**
- **Health and medical matters**
- **Any statement of opinion about my abilities or performance**
- **Personal details including name, address, date of birth etc.**
- **Other information (Please specify)**

Name (in full) _____

Student number _____:

College course attended _____

Date of Birth _____

Address to which information is to be sent:

_____

_____

_____

_____

Daytime contact telephone number:

_____

For Office Use Only

Request for information received on ……..

Information sent to enquirer on ……..

Signed (Designated Data Controller ……

APPENDIX 3

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	3 years after the end of the financial year to which the records relate	Director of Financial Accounting
1.2	Statutory maternity pay records and calculations	3 years after the end of the financial year to which the records relate	Deputy Group Director, HR and OD
1.3	Statutory sick pay records and calculations	3 years after the end of the financial year to which the records relate	Director of Financial Accounting
1.4	Wages and salary records	6 years from the last date of employment	Director of Financial Accounting
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	Deputy Group Director, HR and OD
1.7	CRB Disclosures	Short as possible and no longer than 6 months	Deputy Group Director, HR and OD
1.8	Medical records as specified under the control of substances hazardous to health regulations	40 years	Director of Estates and Facilities
1.9	Personnel Files: training records; notes of grievances and disciplinary hearings	6 years from the end of employment	Deputy Group Director, HR and OD
1.10	Facts relating to redundancies (less than 20)	3 years from the date of redundancies	Deputy Group Director, HR and OD
1.11	Facts relating to redundancies (20 or more)	12 years from the date of redundancies	Deputy Group Director, HR and OD
1.12	Health records	During employment	Deputy Group Director, HR and OD

1.13	Health Records where reason for termination of employment is concerned with health, including stress related illness	3 years	Deputy Group Director, HR and OD
1.14	Sickness absence monitoring records	2 years	Deputy Group Director, HR and OD
1.15	Applications forms and interview notes (for unsuccessful candidates)	6 months from the date of the decision	
1.16	Professional development records and files	5 years	Deputy Group Director, HR and OD
1.17	Parental leave	5 years from the birth/adoption of the child or 18 years if the child receives a disability allowance	Deputy Group Director, HR and OD
1.18	Pension scheme investment policies	12 years from the ending of any benefit payable under the policy	Director of Financial Accounting
1.19	Pensioners' records	12 years after benefit ceases	Director of Financial Accounting
1.20	Trade union agreements	10 years after ceasing to be effective	Deputy Group Director, HR and OD
1.21	Line manager's staff files	Duration of the individual's employment then forwarded to HR Department for disposal	Deputy Group Director, HR and OD

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 Financial Accounting
2.2	Inland Revenue approvals	permanently	Director of Financial Accounting
2.3	Pension scheme investment policies	12 years from the ending of any benefit payable under the policy	Director of Financial Accounting
2.4	Pensioners' records	12 years after benefit ceases	Director of Financial Accounting
2.5	Employers' liability certificate	20 years	Director of Financial Accounting
2.6	Payroll data	10 years following cessation of employment	Director of Financial Accounting
2.7	Published financial accounts	Indefinitely	Director of Financial Accounting
2.8	Tenders and time expired contracts	7 years	Director of Financial Accounting
2.9	Internal and external audit reports	7 years	Director of Financial Accounting

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	Deputy Principal / CCCT Deputy Managing Director / Director Learner Experience
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 and College Principals for college specific feedback / complaints.
3.5	Student records: eg Learner support, Access Fund payments, Childcare etc	Completion of student's programme + 6 years	Deputy Principal / CCCT Deputy Managing Director / Director Learner Experience
3.6	Confidential student records eg referral to external agencies	2 years	Deputy Principal / CCCT Deputy Managing Director / Director Learner Experience / Director Learner Experience
3.7	Tutorial records	Completion of student's course plus 3 years (NB excluding summaries extracted for reference purposes – see 4.2 above)	Deputy Principal / CCCT Deputy Managing Director / Director Learner Experience
3.8	Coursework samples	Current academic year plus 1 year	Deputy Principal / CCCT Deputy Managing Director / Director Learner Experience
3.9	Assignments/course log	Life of course	Deputy Principal / CCCT Deputy Managing Director / Director Learner Experience
3.10	Handouts, WebPages, learning resources	Life of course	Deputy Principal / CCCT Deputy Managing Director / Director Learner Experience

3.11	Course grade/mark sheets	Termination of relationship with student + 6 years	Deputy Principal / CCCT Deputy Managing Director / Director Learner Experience
3.12	Course induction programme/course handbooks	Life of course	Deputy Principal / CCCT Deputy Managing Director / Director Learner Experience

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	Deputy Principal / CCCT Deputy Managing Director / Director Learner Experience
4.5	Curriculum SARs and action plans	Current academic year plus 3 years	Deputy Principal / CCCT Deputy Managing Director / Director Learner Experience
4.6	Divisional/Centre SARs and action plans	Current academic year plus 3 years	Deputy Principal / CCCT Deputy Managing Director / Director Learner Experience
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 Breach Policy and Procedures

1. Introduction

1.1 Every care is taken to protect personal data from incidents (either accidentally or deliberately) 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 The Group'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 the Group.

2.2 This policy relates to all personal and special categories (sensitive) data held by the Group regardless of format.

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

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. Definitions / Types of Breach

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 the Group'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;
- 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 the Group'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 the Group'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 the Group.

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 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);
- 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;
- 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 the Group 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;
- 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):	

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.

1.4 A DPIA must be carried out for all projects where there is a risk of a personal data breach.

2. Purpose and Scope

2.1 This framework should be read in conjunction with the Group'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 Group.

2.2 This policy relates to all personal and special categories (sensitive) data held by The Group 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 data protection impact assessment 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 the Group's data protection officer.

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 data protection officer 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.