

City College Peterborough

Data Protection Policy

**Contents**

|  |  |
| --- | --- |
| 1. Basic Dos and Don’ts | 3 |
| 1. Position Statement | 4 |
| 1. Scope | 4 |
| 1. Responsibilities | 4 |
| 1. Policy | 4 |
| 1. Implementation | 6 |
| 1. Monitoring & Impact Assessment | 7 |
| Document Control | 7 |
| **Appendix: Staff Guidance** | **8** |
| 1. Definitions | **8** |
| 1. Roles and Responsibilities | **8** |
| 1. Training & Induction | **11** |
| 1. Individual Rights | **11** |
| 1. Data Breach | **14** |
| 1. Sharing data | **19** |
| 1. Data Retention & Deletion | **20** |
| 1. Additional Documents | **20** |
| Confidentiality Agreement and Policy Acceptance | **21** |

# Basic Dos and Don’ts

**Do** think about the person behind the data as though it were you.

**Do** ask for only the information you need to do the job and only keep it for as long as you need to and in accordance with the Document Retention Schedule.

**Do** be clear about why you are collecting the data.

**Do** make sure you have accurate data.

**Do** only use information for the reason it was collected.

**Do** dispose of paper records and emails securely.

**Do** use strong passwords to protect devices and data and **NEVER** share them with anyone else.

**Do** use secure and encrypted devices.

**Do** make sure you know who you are talking to and check their identity if you need to.

**Do** check someone’s email or address before you send anything.

**Do** check what is in an envelope or email before you send.

**Do** report all breaches suspected or real immediately.

**Do** check that you have a completed Legitimate Impact Assessment to process data.

**Do** check that there is an information sharing agreement if you need to share data externally.

**Do** ask for advice if at all unsure and always when someone asks to see information held about them or wants their information deleted.

**Don’t** share personal information unless you are sure you can and you know who is asking.

**Don’t** assume that someone’s consent lasts forever and covers everything.

**Don’t** leave PCs, laptops and phones unlocked when unattended or share your passwords.

**Don’t** leave personal information on show on desks or in vehicles - make sure it's secure.

**Don’t** open emails or click on links if you don’t recognise the sender - speak to IT Support.

**Don’t** write comments about an individual that we cannot defend - they have a right to see them.

**Don’t** ignore a possible data breach - the sooner it is reported, the sooner it can be dealt with.

1. **Position Statement** 
   1. The purpose of this policy is to make sure that we:
      1. comply with the law in respect of the data we hold about people
      2. protect our learners, supported people, employees, volunteers and other individuals
      3. protect the organisation when a data breach happens
      4. follow good practice.
   2. We recognise that we have a responsibility to make sure we comply with all of our data protection duties. We also have to ensure that all of our employees and suppliers not only understand but comply with data protection legislation.
   3. Data protection means that when we record and use personal information, we must be open about how the information is used and keep it secure. It applies to how we collect, use, share, keep, delete and destroy personal information.
   4. This policy applies to all personal data held by or on our behalf. It includes manual/paper records and personal data that is electronically processed by computer systems or other means such as CCTV systems.
2. **Scope** 
   1. This policy applies to anyone accessing or using personal information, including for example: employees, temporary or contract staff, volunteers, work placements, contractors, suppliers, services providers or other partners or agencies.
   2. We have to make sure that anyone delivering a service on our behalf complies with this policy and others to make sure the data is safe.
3. **Responsibilities** 
   1. There are six Data Protection Principles with which we must comply in relation to personal information. In summary these are that personal information will be:
      1. processed fairly and lawfully in a transparent way
      2. obtained only for one or more specified and lawful purpose(s) and not further processed in a manner incompatible with that purpose
      3. adequate, relevant and limited to what is necessary
      4. accurate and where necessary, kept up to date
      5. not be kept for longer than is necessary
      6. protected by appropriate technical and organisational measures
   2. This means that we will ensure:
      1. that when we ask for information that we are fair to the people whose information we ask for and use
      2. that we explain why we are asking for the information and what we will do with it
      3. we will only ask for the information we need
      4. the information we hold is up to date and accurate
      5. we only keep it for as long as we need to
      6. we have processes in place to protect the information whether it is on paper or electronic.
      7. we won’t send information abroad unless there are the proper safeguards
      8. that people can exercise their data protection rights.

* 1. In addition we will also:
     1. have someone with specific responsibility for data protection (a Data Protection Officer)
     2. make sure that all employees know their responsibilities under data protection and know what good practice is
     3. train and support staff to manage and handle information correctly
     4. respond to any queries about handling personal information promptly and courteously
     5. review how we use personal information to make sure we are always complying
     6. ensure staff know when they can share information with others and how to do so.

# What are your responsibilities?

All of us, whether permanent or temporary, are required to read, understand and accept any policies and procedures that relate to the personal data that we may handle in the course of our work.

All of us must:

* Understand the main points of the Data Protection legislation.
* Identify and report any risks their line manager.
* Make sure that customers (including but not limited to learners and supported people) understand their rights.
* Identify any breaches or loss of data and report them.
* Identify and report any rights requests to the Data Protection Officer and their team.

1. **Policy**
   1. 3.1 It is the policy of CCP that it will be fully compliant with all aspects of the Data Protection Act 2018, which details the requirements and safeguards which must be applied to personal data to ensure the rights and freedoms of living individuals are not compromised.
   2. CCP will ensure that appropriate measures are in place to guarantee compliance with the law. These include but are not limited to Legitimate Impact Assessments, staff training, staff declarations, document control and retention and audit.
   3. It is the policy of CCP to take advice as needed and follow guidance laid out by the ICO (Information Commissioners Office) and to report significant breaches swiftly through this office.
2. **Implementation**

CCP will:

* 1. Apply a legitimate interest assessment (LIA) to all business areas where data is collected, used and retained where legitimate interest is used as the basis for processing. This will:
     + Identify the legitimate interest
     + Show processing is necessary
     + Show balance with individuals rights
  2. Assign responsibility to every department manager / task group representative involved in processing data to ensure there is a relevant LIA completed and authorised before processing any data.
  3. Obtain consent for marketing purposes or anything which might not reasonably be expected under our legitimate interests.
  4. Meet our legal obligations to specify the purpose for which information is used and the basis under which it is processed.
  5. Collect and process appropriate information restricted to the extent that it is needed to fulfil operational needs or to comply with legal requirements.
  6. Document our data processing
  7. Ensure the quality and accuracy of information processed.
  8. Take action to ensure retention thresholds are complied with.
  9. Take appropriate technical and organisational security measures to safeguard personal information.
  10. Ensure that personal information is not transferred abroad without suitable safeguards.
  11. Ensure that the rights of people about whom the information is held can be fully exercised under the legislation.
  12. Have a committee of trained staff known as the Data Protection Group who will meet regularly under the direction of the DPO.
  13. Provide everyone managing and handling personal information appropriate training and appropriate supervisions.
  14. Clearly communicate to relevant stakeholders to ensure contractual responsibilities for following good data protection practice are fully understood.
  15. Ensure that clear instructions exist for the handling of data including easy-read guides.
  16. Ensure that methods of handling personal information are regularly assessed and evaluated.
  17. Ensure that guidance is in place for robust governance of sharing data with partners and third parties.
  18. Ensure that data is stored digitally in accordance with its IT policy including system controls to prevent the downloading and storage of information and data to removable and transferrable media devices, as well as enforcing prohibition on the use of these devices. All staff accounts will require 2 factor authentication to access CCP systems and all data contained on these devices will be password protected and encrypted.

## Disclosures permitted by law

There will be occasions where the disclosure of personal information will be permitted in law such as for the prevention and detection of crime or safeguarding of vulnerable individuals.

1. **Monitoring and Impact Assessment** 
   1. As with all CCP policies this policy will be assessed to ensure that there is no negative impact on anybody in terms of the nine protected characteristics.
   2. Compliance with this policy and related standards and guidance will be monitored as part of the work of the Data Protection Group, chaired by the Data Protection Officer.
   3. A review of this policy will take place every three years or in conjunction with updates to the law. Each review will take account of any new or changed legislation, regulations or business practices.
   4. The Data Protection Group will be responsible for completing a risk-based audit plan for CCP. Internal audits will be undertaken by the task group and external audit and review by the Information Governance Team at Peterborough City Council.
   5. Incidents and breaches will be reported in line with the Data Breach and Incident Reporting Procedure. The Data Protection Group will maintain a central record and will ensure that CCP responds in accordance with its policies.
   6. Not following this policy by employees will be treated as misconduct with proportionate disciplinary response. Where a serious incident or breach occurs due to neglect of the policy, this may be treated as gross misconduct and lead to dismissal. In the case of contractors, partner representatives, agency workers and volunteers, disregard of this policy may be grounds for termination of that relationship with CCP. Disregard for this policy by members of Peterborough City Council may be regarded as a breach of the Code of Conduct.

**Document control**

|  |  |
| --- | --- |
| Revision issue date: | May 2024 |
| Next Review Due Date: | May 2027 |
| Date of most recent Equality Impact Assessment: | 04/06/24 |
| Document Lead and Author: | Adele Fender (DPO) |
| Approvers and dates: | Leadership team June 2024 |
| Purpose of the review: | Scheduled |
| Dissemination: | Intranet and website |

This document can only be considered valid when viewed via the City College Peterborough internal web pages on the intranet. If this document is printed into hard copy or saved to another location, you must check that the version date on your copy matched that of the intranet version. The date will always appear on the footer.

|  |  |
| --- | --- |
| Revisions | |
| *26/09/23* | Additions:  Amendments:   * Changed all references to ultimate accountability from Governing Board to Peterborough City Council * Changed reference to Principal to Executive Principal and Deputy Principal to Principal. |
| *04/06/24* | Amendments:   * Changed reference to ‘Executive Principal’ to ‘Head of the Organisation’ * Significant changes to the layout of the policy to be more standardised with others. * Simplified much of the language of the policy itself * Added Dos and Don’t guidance * Removed list of documents referenced but that don’t exist! * Removed bulk and added in as an appendix for Staff Guidance |

# Appendix: Staff Guidance

1. **Definitions**

**Data Controller**

City College Peterborough is the data controller and is fully responsible for ensuring compliance with legislation. The College has registered with the ICO reference Z5456707.

**Data Processor**

A data processor is the person or organisation who processes personal data which has been shared with them legitimately by a data controller. A data processor does not own the data and cannot use it for purposes other than stated in the contract or where a legal gateway exists. Any use or sharing of data should not be done without the written consent of the data controller.

For the most part, CCP is the data controller and the data processor combined. In some instances it is just the data processor. For the purpose of processing the data CCP uses for the commissioned service of Day Opportunities, CCP is the data processor authorised to process the data on behalf of Peterborough City Council, the data controller.

**Data Controller/Processor Relationship**

Where the controller and processor are not the same i.e. the college and a partner organisation, the relationship must be underpinned by a contract. This contract must include a data sharing agreement detailing the schedules of the data to be processed as well as the clauses regarding the arrangements for the use, storage, retention and deletion of data by that external party. All contracts must be reviewed by the Data Protection Group to ensure that they meet requirements. Any contract between CCP and a third-party processor will make plain the liabilities and duties arising from data protection legislation that the processor must comply with.

**Special Category Data**

This is data identified as being more sensitive therefore requiring more protection. In general, any data which could create a greater risk to a person’s fundamental rights and freedom is considered special category. For example:

* Race
* Ethnic Origin
* Politics
* Religion
* Trade Union Membership
* Genetics
* Biometrics
* Health
* Sex Life
* Sexual Orientation

In addition, any data which if compromised could cause undue significant harm to an individual should be treated in the same way.

* Criminal Records
* Financial Information
* Disciplinary Information
* Credit card/debit card details pertaining to the data subject

It is important to emphasise that special category data is identified as such as it is data which could be used in an unauthorised way to cause significant harm to an individual. It is the duty of CCP to ensure that wherever data under these or similar categories is processed that suitable and effective safeguards are in place.

# Roles and Responsibilities

**The Head of the Organisation**

The Head of the Organisation has overall accountability and responsibility for all aspects of data protection in their capacity as the senior executive officer for CCP. This accountability is to Peterborough City Council, the ICO, third party data controllers, and all data subjects of CCP.

The Head of the Organisation is required to provide assurance to Peterborough City Council that all risks to CCP relating to data protection and information security are effectively managed and mitigated against.

The Head of the Organisation is supported in this responsibility in accordance with the normal operational structure and hierarchy of CCP. The Head of the Organisation will delegate responsibility for compliance with Data Protection Legislation (including the implementation of this policy and other related documents) to the DPO.

**Data Protection Officer (DPO)**

The DPO is responsible for internal compliance, informing and advising on data protection obligations at strategic level, providing advice on all aspects of data protection and being the primary point of contact for data subjects and the ICO. They run the Data Protection Group and hold responsibility for all outcomes of the group as well as ensuring the members of the group are adequately trained.

The DPO is also responsible for ensuring that the College is registered with the ICO for data processing, that the registration accurately reflects the data processing activities undertaken by CCP and that the registration is maintained and renewed as required.

**Data Protection Group**

The Data Protection Group is a body in place to give guidance and advice at organisational level on all data protection issues. The group is defined as a cross departmental working group representing all parts of the college who bring together working experiences and knowledge of data protection issues in order to progress and improve compliance across the organisation. The group acts as first contact for all data protection issues, including access requests and incidents, and acts to embed a positive culture for data protection across CCP. The group assesses training needs across the organisation and works with managers to deliver that training. The DPO, or in her absence an alternative member of the group will be responsible for assessing incidents. Group members are nominated by their senior manager and should demonstrate knowledge and competence around data protection obligations including this policy.

**Responsibilities of Each Department**

Each department, where practicable will delegate a member of staff to the Data Protection Group who will take responsibility for bringing departmental items for consideration. The DPO will approach any departments not represented.

Each department is responsible for ensuring it has completed LIAs for each unique type of data it processes or where relevant that necessary consent can be obtained.

Each department is responsible for ensuring that every opportunity for an opt out is offered where processing data for legitimate interests.

**Responsibilities of Managers**

All managers are required to ensure that they (and their staff) understand and adhere to this policy and any associated procedures. They are responsible for ensuring that staff are informed and updated on any changes made to this policy. They are also responsible for ensuring that their staff are aware of where data protection information is held and who their representative on the Data Protection Group is.

Managers must ensure that through the induction process or otherwise that all members of their team sign and return a copy of the confidentiality agreement as confirmation that they have read, understand, and will comply with this policy.

All managers must clearly understand the requirements around reporting data incidents and ensure that they and their staff comply with those requirements. They must also embed a positive reporting culture and operate in a way that **incorporates data protection into everything that is done by default and design**.

All managers must ensure that their staff undertake training in data protection which is specific and relevant to their role, they must also uphold the element of personal responsibility for all staff around data protection.

**Responsibilities of Staff**

All staff, whether permanent or temporary, are required to read, understand and accept any policies and procedures that relate to personal data that they may handle in the course of their work.

All staff have a responsibility for data protection and are required to adhere to this policy, any associated procedures and to attend any associated training.

All staff must:

* Understand the main concepts within the Data Protection legislation
* Identify and report any risks to the security of data processed by CCP to their line manager or their Data Protection Group representative.
* Assist their customers/service users to understand their rights and CCP’s responsibilities in regard to data protection.
* Identify and report any requests relating to data to the Data Protection Officer or their Data Protection Group representative so that they can be processed in accordance with the Data Protection Act.

All staff including those on temporary contracts, agency staff, volunteers and work placement students, and their line managers, are required to read and sign the Confidentiality Agreement at the end of this document before access to any systems containing personal data is granted.

**Responsibilities of Peterborough City Council**

Accountability is one of the seven principles of data protection. Peterborough City Council are ultimately responsible for ensuring that data protection legislation is complied with in full at CCP.

Peterborough City Council delegate this responsibility to the Head of the Organisation and through doing so must:

* Take responsibility for complying with data protection legislation, at the highest management level and throughout the organisation
* Adopt and implement proportionate data protection policies
* Taking a ‘**data protection by design and default’** approach - putting appropriate data protection measures in place throughout the entire lifecycle of all processing operations
* Review and update accountability measures at appropriate intervals.

1. **Training & Induction**

Reading, understanding and signing to confirm conformity to this policy is a mandatory part of the induction process at CCP and must be documented as completed within the induction period. It will then need to be revisited whenever the policy is reviewed.

The Data Protection Group will lead on the development of staff training either through e-learning modules, face to face or third-party training. The training will be developed to meet the specific needs of individuals and the organisation.

It is the responsibility of individual line managers to ensure that they and their staff have sufficient training to ensure they are able to meet their obligations under this policy.

# Individual Rights

# The Right to be Informed

This means that people have a right to be told what we are doing with their information. We need to be clear and transparent about what we do because this helps build understanding and trust about what we do. The way we normally tell people about what we do is in a privacy notice. Our privacy notice is available on our website.

The privacy notice will be reviewed in line with ICO guidance on the right to be informed as found here <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/>

# The Right of Access

If we hold information about a person then they have a right to see their own information. There are a few exceptions to this rule, such as data held for child protection or crime detection / prevention purposes, but most individuals will be able to have a copy of the data held on them. We may have to redact some of the information if we cannot share something with a person.

* + All requests are logged, acknowledged within a reasonable timeframe of the request being made and fully responded to normally within 1 month
  + All requests are coordinated by the DPO
  + Appropriate identification of a requesting individual is always obtained
  + CCP will follow the ICO guidance on handling SARs which can be found here <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/?q=privacy+notices>

# The Right of Rectification

If we have some information about someone which is inaccurate or not complete then they can ask to amend or rectify it. We have to respond with a month.

* + - All requests are logged, acknowledged within a reasonable timeframe of the request being made and fully responded to normally within 1 month
    - All requests are coordinated by the DPO
    - Appropriate identification of a requesting individual is always obtained
    - Inform third parties we have shared data with so that they can rectify what they hold
    - If asked, inform the requester who we have shared their data with
    - CCP recognises all requests whether verbally or in writing.
    - CCP will follow the ICO guidance on handling requests for rectification which can be found here <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/?q=privacy+notices>

# The Right to Erasure

This is also known as the right to be forgotten and is the basis against which any request by the data subject to remove all or part of any data on them is considered. The reasons to erase may be as follows:

* + - Where the data is no longer necessary in relation to the purpose it was collected for
    - It is being unlawfully processed
    - The individual withdraws consent where consent was given.
    - It must be erased to meet a legal obligation
    - The individual objects to the processing and there is no overriding legitimate interest

CCP retains the right to override any requests made under the right to erasure where the legitimate interests of CCP justify the override. There will always be data that we need to keep to comply with legal requirements and funding contracts.

* + - All requests are logged, acknowledged within a reasonable timeframe of the request being made and fully responded to normally within 1 month
    - CCP recognises all requests whether verbally or in writing.
    - All requests are coordinated by the DPO
    - Where data has been shared CCP will inform the recipient of the erasure
    - If asked, inform the requester who we have shared their data with
    - CCP will follow the ICO guidance on handling requests for erasure which can be found here <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure>

Relevant guidance and information is available as a separate information sheet accessible on the CCP intranet.

# The Right to Restrict Processing

A person has the right to block or suppress the use of their information. If someone does ask us to restrict the use of their information then it means that we can retain the information but not use it any further. We will need to keep some information to ensure that we maintain the restriction.

The right applies when a request is made under the following conditions:

* + - There is a question over data accuracy or a request is received to rectify data
    - Data has been processed unlawfully where erasure is not requested
    - There is an objection to lawful data processing while legitimate grounds are considered
    - Data may be required for future legal reasons

CCP will:

* + - Ensure all requests are logged, acknowledged within a reasonable timeframe of the request being made and fully responded to normally within 1 month
    - Inform third parties we have shared our data with so that they can apply the same restriction on what they hold
    - If asked, inform the requester who we have shared their data with
    - CCP will follow the ICO guidance on handling requests to restrict processing which can be found here <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/>

*CCP will automatically restrict the processing of data where it receives a request for erasure, request for rectification, request for restriction or any objection to processing for the duration of the time given to consider each request, which is normally one month.*

# The Right to Data Portability

This is a right which allows people to obtain and reuse their data for their own purposes. It allows them to move, copy or transfer personal data from one IT system to another securely.

It applies to:

* + - data provided by the subject
    - where it is based on consent or in performance of a contract and
    - if carried out by automated means

CCP currently doesn’t operate a system of capturing data compatible with the requirements to comply with requests under the rights of data portability. In any event of compatibility, the college will apply ICO guidance on data portability as found here <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/>

# The Right to Object

An individual can object to what we are doing with their data where if it is based on::

* + - Our legitimate interests of lawfully processing
    - Public interest or exercise of official authority
    - Direct marketing
    - Purposes of scientific/historical research and statistics.

CCP will stop processing data instantly on receiving an objection unless we have compelling legitimate grounds which override the objection.

* + - The Right to Object will be made clear to all individuals from whom CCP will collect and process data. This includes CCTV and other image capturing.
    - All requests are logged, acknowledged within a reasonable timeframe of the request being made and fully responded to normally within 1 month
    - All requests are responded to by the DPO
    - CCP will follow the ICO guidance on handling objections which can be found here <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/>

# Rights related to automated decision-making including profiling

An individual has the right to not be the subject of a decision if it is based on automated processing and it results in a legal or similar impact on the subject.

CCP currently does not operate any decision making or profiling by ways of automated software. This policy will be reviewed periodically, and data protection legislation relevantly applied in any instances where the above requires updating.

In any eventuality, CCP will follow the ICO guidance on handling requests to grant the right related to automated decision making including profiling which can be found here <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/>

# Rights of Employees

Relevant guidance and information is available as a separate information sheet accessible in the Data Protection folder on the CCP intranet.

# Data Breach

# 5.1 Data Breach and Incident Reporting

* + 1. Data Breach is the descriptive term used for a data incident where the following might occur:
    - Intentional or unintentional release of secure or private/confidential information to an untrusted environment
    - Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to protected data transmitted, stored or otherwise processed
    - Any action taken by CCP or its employees and associated parties which is not compatible or compliant with data protection legislation
    - Unauthorised cross-departmental access to data and especially special category data
    - An identified incident which might lead to any of the above.
    1. City College Peterborough holds a large and varied amount of data which includes personal and special category data and information.
    2. CCP commits to ensuring that every care is taken to avoid a data breach by protecting personal information and following authorised processes to avoid the breach of any data.
    3. In the unlikely event of a data breach, CCP will always ensure that appropriate action is taken to mitigate any repercussions, minimise any associated risk, and comply with data protection legislation requirements around reporting of the breach within the timescales stipulated.
    4. CCP has incorporated into this policy its approach to Data Incident Reporting which covers the process of recognition, reporting, recording and escalation of all data incidents without exception.
    5. All data incidents are ultimately the responsibility of CCP as an organisation however CCP will apply its disciplinary policy proportionately in all instances of data incident or breach.

# Recognition of Data Breach

* + 1. A data breach is an escalation of a data incident which is any incident where data is involved which may be evaluated as contrary to the ordinary business operations of CCP under data protection legislation and this policy. All data breaches originate in a data incident.
    2. A data breach is generally considered to be any event, or risk of event which results in perceived or actual damage to an individual’s rights and freedoms, where data is a factor in the event.
    3. A data breach also refers to any non-compliance with data protection regulation and for the purpose of this policy is not restricted to events which are likely to cause damage to an individual.
    4. A breach will generally be attributed only to data that CCP is either the data controller of, or data that it is in the power of CCP to be disclosed.
    5. Data received by CCP from external organisations which is in appearance a breach of ICO rules on lawful processing is dealt with in the Breaches by Other Organisations section (section 24).
    6. CCP recognises a data breach where a data incident occurs which is systematically evaluated to be a breach and can be recognised as any of the following:
    7. Any data controlled by CCP where that control is lost, intentionally or not
    8. Data is processed or held contrary to general ICO guidance
    9. Any part of this policy on data protection is not adhered to or complied with
    10. Any activity occurs not in good faith of CCP’s policies, guidance and information
    11. Any processes designed to communicate, embed, report and monitor data protection at CCP are not followed appropriately.

# Detecting a Data Breach

* + 1. Data is processed by a number of different departments and staff at CCP. Generally, it is the responsibility of all staff employed by CCP to be aware of this policy and their individual responsibilities under this policy for reporting a data incident or where there is perceived risk of an incident occurring.
    2. All staff are responsible for the detection of a potential breach by ensuring that they take any awareness they have of a data incident under any circumstances and follow the Data Breach and Incident Reporting Procedure.
    3. This applies to perceived actions of others but also a requirement for self-reporting.
    4. On detection of an incident, immediate appropriate action must be taken to mitigate or remedy the situation.

# Reporting of Data Breach

* + 1. Any member of staff who is party to identifying a potential or actual data incident must refer to and comply with the procedures on Data Breach and Incident Reporting found [HERE](https://citycollegepeterboroughac.sharepoint.com/:w:/r/sites/NewHome/Shared%20Documents/File%20Server/Data%20Protection/Task%20Group/GDPR/Incident%20Reporting/Data%20Incident%20Reporting%20Infosheet.docx?d=wc226996284e84df9b7114c58d55afb38&csf=1&web=1&e=9AMKfV). In all instances the following will apply:
    - All incidences must be reported to an appropriate line manager
    - The manager must ensure the incident is contained
    - All incidences involving data are assumed to be a data incident
    - All data incidences are assumed to be a data breach until fully evaluated
    - An individual observing (discovering or committing) an incident will not be responsible for evaluating the incident
    - **An individual observing an incident is critically and personally responsible for reporting the incident as soon as they are aware of it**
    - All data incidences are reported to the Data Protection Group and/or DPO using the authorised Incident Reporting Form found [HERE](https://citycollegepeterboroughac.sharepoint.com/:x:/r/sites/NewHome/Shared%20Documents/Intranet/Data%20Protection/Data%20Incident%20Reporting%20Form.xlsx?d=wee2881dd60604a2fa8802ef46707f7f8&csf=1&web=1&e=4J8Rzf), or in person or by phone to the DPO.
    - All data incidences are evaluated by the Data Protection officer, or in her absence, another member of the Data Protection Group and will include a full risk assessment without exception.
    - **All data incidents involving special category data, specifically those which relate or might relate to safeguarding must always be notified to the safeguarding lead officer**
    - The DPO holds responsibility for escalating an incident
    1. The Data Protection Group can be contacted at [DPO@citycollegepeterborough.ac.uk](mailto:DPO@citycollegepeterborough.ac.uk)

# Investigating a Data Incident or Breach

* + 1. All data incidents and breaches will be subject to proportional investigation. This investigation will be co-ordinated by a member of the Data Protection Group in conjunction or collaboration with management of any relevant or involved departments or parties.
    2. In all instances the investigation must by led by an appropriate senior manager who will be the investigating manager. This requirement will be advised on by the DPO in all instances.
    3. Any member of the Data Protection Group, including the DPO, who is associated with or party to an incident is not permitted to participate in the investigation, recording or advising on the incident other than providing information.
    4. All evidence and findings will be recorded and held by the Data Protection Group.
    5. Any consequences of the investigation in relation to any individuals involved will be the responsibility of an appropriate line manager to implement as per CCP’s disciplinary procedure.
    6. The investigation into the breach is a separate investigation to that of the involved individual’s conduct.
    7. The investigation of the circumstances of a breach should always lead to documented learning from the incident and positive change to ensure a similar incident cannot happen again.

# Recording of Data Breach

* + 1. All data incidences are recorded appropriately by a member of the Data Protection Group. The record will include a description of the nature of the personal data breach including:
    - The categories and number of individuals concerned
    - The categories and number of personal data records concerned
    - the name and contact details of the investigating manager and other individuals involved and a report of their investigation
    - Data Incident Reporting Form
    - Assessment of seriousness of breach
    - A description of the likely consequences of the data incident
    - A description of the measures taken, or proposed to be taken, to deal with the data incident
    - The measures taken to mitigate any possible adverse effects
    - Details on escalation or other actions
    - Confirmation that the data subject has been informed of the ongoing right to complain to the ICO as appropriate
    - Final outcome, process/policy changes and learning.

# Assessment and Escalation of Data Incidents

* + 1. Assessment & escalation of data incidents refers to the reporting requirements for certain types of breach to the ICO, Data Controllers where we are the Data Processor, and to the Data Subjects involved.
    2. All incidents go through an assessment process to determine level of seriousness which then determines the level of escalation required. This is detailed in the Data Breach and Incident Reporting procedure and will comply with ICO guidelines.
    3. The assessment will be carried out with due attention to
    - Whether any control has been lost over personal data
    - The potential harm or risks to the data subject as a result of the incident, including any distress the data subject may suffer as a result of the incident.
    - The impact of the breach in relation to:
* Limitations of an individual’s rights & freedoms
* Discrimination against an individual
* Identity theft or fraud
* Financial loss
* Damage to reputation
* Loss of confidentiality
* Volume
* Sensitivity
* Severity of any other consequences
  + 1. Escalations may include:
    - Informing the data controller - As data processor, CCP is required to report any breach as soon as it is aware of the breach, regardless of the impact and risk, to the relevant data controller.
    - Informing the ICO
    - Informing the affected individual (data subject)
    1. The decision on the escalation of any data breach ultimately rests with the Head of the Organisation, or when absent, an alternative member of the leadership team, under the advice of the DPO.
    2. Consequently, CCP will not report any incidences to the ICO, data subjects or data controllers without the express permission and/or knowledge of the Head of the Organisation or alternative member as described above.
    3. All escalations will be co-ordinated and conducted by the DPO strictly in line with ICO requirements, timelines and guidelines found here <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>
    4. As far as is reasonable, CCP will err on the side of caution in deciding whether to report breaches.

# Breaches by Other Organisations

* + 1. This section refers to:
    - Data controlled by CCP that is shared with an authorised data processor where the data processor has disclosed that data unlawfully or experienced any kind of breach.
    - Data received by CCP from a third party organisation or individual which appears in breach of data protection legislation.
    1. Where a data processor processing data on behalf of CCP has a breach, it is their legal responsibility to report it to CCP as soon as they become aware. All processors must have clear breach reporting requirements written into a data sharing agreement (see sharing data section 26). CCP is thereafter responsible for treating the breach in accordance to this policy and **recognises the timeline in accordance with ICO guidance as commencing from the data processor becoming aware of the breach and not when the data processor notified CCP of the breach**. The processor takes no responsibility for reporting or escalating the breach to the ICO.
    2. CCP does not recognise any legal obligation towards data received which appears in breach of data protection legislation, however will take limited action depending on the circumstances.
    3. Examples might be:
    - Data or information including Special Category Data is received by the wrong person
    - Unprotected information is received
    - Shared or generic mailboxes receive unprotected data
    - Information received is excessive to requirements
    1. Where data is received by CCP from a third-party data controller which appears inconsistent with data protection legislation, the following applies:
    2. The incident is to be considered a data incident
    3. The incident must be reported following the Data Breach and Incident Reporting procedure
    4. The recipient **must not** respond unless under the instruction of the DPO.

# Third party complaints to the ICO

In the event of a complaint being made to the ICO in regard to how CCP is processing data, this complaint will be investigated by the DPO and a response provided in conjunction with the Head of the Organisation.

# Sharing Data

* 1. The sharing of data specifically means where CCP, as the data controller holding data for a legitimate interest, allows access to that data by either an external individual or organisation, or internal departments or members of staff who may or may not be part of the legitimate interest.
  2. Information can only be shared where CCP has a recognised and approved legitimate interest, or where that legitimate interest is not sufficient, by an appropriate lawful basis, ordinarily consent.
  3. Consent can only be granted by the data subject or by somebody acting on their behalf in a legal capacity. Consent cannot be granted by CCP as the data controller, nor by anybody else regardless of their trusted status with the data subject’s data in a non-legal capacity.
  4. Where CCP shares data, CCP remains the data controller whilst the recipient is the data processor. For data to be transferred between the two, there must always be a data sharing agreement in place.
  5. Examples of where CCP may share data include:
     + Data returns to funding bodies & government departments or agencies
     + Shared information with partners and examination boards
     + Sharing data with Local Authorities or Combined Authority
     + Internal cross-departmental sharing.
  6. Disclosures permitted by law:
     + Data sharing for safeguarding and prevent purposes
     + Requests by the police or other enforcement agencies.
  7. CCP will always seek a written request confirming the reason for the disclosure where consent has not been obtained and will evaluate that request before responding.
  8. The sharing of data must comply with the LIA for the processing and be in line with ICT policy of secure document sharing. Where practicable or available this must be by authorised secure means such as a secure file sharing system.
  9. Data that is authorised to be shared must:
     + Be shared in an authorised format and way
     + Only be sent to a confirmed designated and authorised recipient
     + Be In a protected format, physical or password
     + Never be sent in the same communication as the method of accessing the data.
  10. Circumstances where data cannot be shared:
      + Where it is sent to a personal mailbox belong to a staff member
      + Where it is sent to a family member or other associate of a staff member
      + Where it is sent to a generic or shared email address of an organisation or CCP
      + Where it cannot be sent in a secure way
      + While using unsecured Wi-Fi or other unsecure networks when off premises.
  11. Any sharing of personal information between CCP and other organisations will be subject to an information sharing protocol that commits the partners to an agreed data transfer process that meets the requirements of Data Protection legislation.
  12. Any data sharing agreements entered into must be approved by the Data Protection Group prior to the information being shared. Data Protection Impact Assessments will be carried out whenever there are projects, new or changed service activities, or new ICT that could potentially impact on the privacy of individuals. The results of assessments will be reported by the DPO to the project lead and other relevant staff.

# Data Retention & Deletion

* 1. This part of the policy must be considered in conjunction with the Document Retention Schedule.
  2. CCP will hold a clear schedule identifying all data processes and show the intended retention period for every processed data. CCP will complete a Legitimate Interest Assessment for each data stream it processes including an identification of the retention requirements and intention.
  3. It is the responsibility of all staff members processing data to ensure that the LIA for that data includes information on the retention of that data. Data must not be processed unless there is a clear retention period available. The retention will be determined by the periodical and time-based question, do we need this data? If yes, this might be due to:
     + Regulatory or legislative reasons
     + Public interest, archives, scientific or historical research
     + Statistical purposes
     + Operational reasons
     + Confirmation of existence of a relationship.
  4. There are 2 basic rules CCP will follow:
     + That we can justify the retention period internally
     + That we can explain the retention period externally.
  5. Where there is no fair and lawful basis for retaining data, it must be either deleted or anonymised securely and completely including archived or duplicated copies.

# Additional documents:

* 1. Legitimate Interest Assessments
  2. Data Retention Schedule
  3. Privacy Notice (Right to be Informed)
  4. Rights of Employees – Fact Sheet
  5. CCTV Code of Practice

**Confidentiality Agreement & Policy Acceptance**

Users of CCP services and members of staff are entitled to assume that any personal information which is collected or recorded during the course of their involvement with the organisation will not be disclosed inappropriately by any person or persons working within the organisation.

All staff, including permanent staff, temporary staff, agency staff, volunteers and work placement students hired by CCP are in a position of trust. Any abuse of this trust will be construed as gross misconduct and may result in disciplinary or legal action.

It is a requirement of CCP that all staff and all managers requesting access to systems for these staff members, should read, and undertake to comply with, these compliance guidelines in accordance with CCP’s Data Protection Policy.

It is the responsibility of managers and supervisors of all staff who have access to personal information (including sensitive personal information) to ensure that these workers understand and comply with the need for confidentiality under Data Protection legislation.

**Declaration** *page 1 of 2 (City College Peterborough Data Protection Policy V1.0)*

**As the signatory to this document I agree to abide this data protection policy and all relevant related document, and by the Good Practice Guidelines as stated below.**

* I will exercise caution in dealing with any requests involving personal information, I should refer such requests to my Manager or Supervisor.
* I will keep my desk clear of paper containing personal information unless the work is actually in progress and I will **never leave personal information unattended**.
* I will ensure that all papers containing personal information are locked in a filing cabinet or desk that is in a secure area away from public access, when I leaves for the day or a significant period of time. I will **never leave personal information unsecured.**
* I will allow proper supervision of my work when working with personal information.
* I will dispose of any scrap paper containing personal information carefully in the official confidential shredding bins or other secure shredding facilities.

When working on personal information held on electronic systems, I will ensure that-

* I do not attach or link any personal IT equipment or other IT equipment not owned and authorised by CCP to CCP’s IT network.
* The computer I am working on is locked before leaving the workstation, even for a short period of time or if in a secure office.
* I will close any open files and log out of the network if the workstation is to be left for longer periods.
* If working remotely I will only use encrypted laptops or encrypted recordable media issued by CCP on a secure network which must be used in line with relevant IT policies.

I will not discuss knowledge of any personal information of any type gained during the course of my employment at CCP with anyone, either internal or external to CCP, unless specifically requested to do so by my line manager in the course of their duties.

**All data and information including personal information and data which is obtained, accessed or accessible during the course of any type of employment with CCP remains the under the stewardship of CCP and I will not transfer or seek to transfer it in any form out of the control of CCP under any circumstances. I acknowledge that this action would be in contravention of the Data Protection Act 2018 and may result in legal proceedings against me.**

I understand that my continued contract of employment is subject to the following signatures of agreement. Unwillingness or refusal to sign will be dealt with as a disciplinary matter.

**Declaration** *page 2 of 2 (City College Peterborough Data Protection Policy V1.0)*

*One copy to be kept on personnel file with copy retained by staff member*

**For all members of staff.**

Your signature on this statement will explicitly acknowledge that you undertake to comply with this policy document and confidentiality agreement.

|  |
| --- |
| I have read and understand CCP’s data protection policy and agree to its terms in full. I acknowledge and understand the implications of not following this policy or data protection legislation in my employment at CCP. I have read and understood the Confidentiality Agreement and accept the terms and conditions stated therein.  Signature: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  Date: . . . . . . . . . . . . . . . . . . . . .  Full Name (Print): . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  Employed As: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  Employment Agency/School/College/Other. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . |

**Manager/Supervisor:**

Your signature on the statement will explicitly acknowledge that you undertake the following

|  |
| --- |
| I understand that I take responsibility for ensuring that the above staff member is aware of, and abides by, this policy and agreement and confirm that they will only be granted access to personal information which is necessary to allow them to fulfil their contract or agreed duties.  Signature: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  Date: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  Full Name (Print): . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  Department & Location: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  If access to special category data is authorised, please also sign here . . . . . . . . . . . . . . . . |