

City College Peterborough

Data Protection Policy

This document has been produced by City College Peterborough. Any Comments or queries regarding the content of the document should be referred to: [dpo@citycollegepeterborough.ac.uk](mailto:dpo@citycollegepeterborough.ac.uk)

Contents

[1. Introduction 3](#_Toc530653194)

[2. Purpose 4](#_Toc530653195)

[3. Scope 5](#_Toc530653196)

[4. Application of the Policy 5](#_Toc530653197)

[5. Data Protection Principles 6](#_Toc530653198)

[6. Application of Principles 7](#_Toc530653199)

[7. Individuals Rights 7](#_Toc530653200)

[8. The Right to be Informed 7](#_Toc530653201)

[9. The Right of Access 8](#_Toc530653202)

[10. The Right of Rectification 8](#_Toc530653203)

[11. The Right to Erasure 9](#_Toc530653204)

[12. The Right to Restrict Processing 9](#_Toc530653205)

[13. The Right to Data Portability 10](#_Toc530653206)

[14. The Right to Object 10](#_Toc530653207)

[15. Rights related to automated decision making including profiling 11](#_Toc530653208)

[16. Rights of Employees 11](#_Toc530653209)

[17. Data Breach and Incident Reporting 11](#_Toc530653210)

[18. Recognition of Data Breach 12](#_Toc530653211)

[19. Detecting a Data Breach 13](#_Toc530653212)

[20. Reporting of Data Breach 13](#_Toc530653213)

[21. Investigating a Data Incident or Breach 14](#_Toc530653214)

[22. Recording of Data Breach 14](#_Toc530653215)

[23. Assessment and Escalation of Data Incidents 15](#_Toc530653216)

[24. Breaches by Other Organisations 16](#_Toc530653217)

[25. Third party complaints to the ICO 17](#_Toc530653218)

[26. Sharing Data 17](#_Toc530653219)

[27. Data Sharing Agreements 18](#_Toc530653220)

[28. Data Retention & Deletion 18](#_Toc530653221)

[Appendix 19](#_Toc530653222)

# Introduction

* 1. The European General Data Protection Regulation (GDPR) has been implemented into UK law by the Data Protection Act 2018, hereafter called Data Protection Legislation, which comprehensively 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. Personal data is defined as any type of information that can be used to identify or can be linked to an identified living person (data subject). Information to identify a living person is not limited to names and contact details, and part or incomplete information, if it could be collected together with other information to lead to identification, constitutes personal data.
  3. In the UK, Data Protection Legislation is upheld by the Information Commissioners Office (ICO) as the Data Protection Authority. This policy is subordinate in all instances to the ICO.
  4. City College Peterborough (CCP) is a data controller as defined by the ICO as an organisation which determines the purposes and means of the processing of personal data.
  5. CCP acts as data controller for the majority of its activities. There are certain functions where CCP delivers a commissioned service on behalf of other organisations where it processes data it is not defined as the controller of. In this capacity CCP is the data processor. This policy applies equally and where relevant on all data held as the data processor, however there should be due referral to relevant data sharing agreements in place to apply further requirements of assurance from the data controller.
  6. CCP needs to collect and use different types of information about people with whom it engages operational relationships and associations with in order to carry out its purpose and objectives. These include current, past and prospective employees, contractors, suppliers, service users, learners and other customers.
  7. There are 6 lawful bases for processing data. At least one of these must always apply when data is being processed and an organisation must process data under a predetermined basis governed by this policy.
     + Consent
     + Contract
     + Legal Obligation
     + Vital Interests
     + Public Task
     + Legitimate Interests
  8. CCP will use as default the lawful basis of Consent for all of its processing, however has opted to use primarily, but not necessarily exclusively, the lawful basis of Legitimate Interests to process data. CCP will not assume legitimate interests is appropriate for all of its data processing in compliance with ICO guidance and will use its default where legitimate interests is inappropriate.
  9. Data protection legislation stipulates that those who record, use and have access to personal information must be transparent about how the information is used and must follow approved data handling processes. It applies to the collection, use, disclosure, retention, access, accuracy, erasure and destruction of data.
  10. It is the obligation of CCP, as a data controller and processor, to ensure full compliance with data protection legislation. This policy applies to all personal data held by or on behalf of CCP and includes manual/paper records and personal data that is electronically processed by computer systems or other means such as CCTV systems.
  11. It is the intent of CCP to apply data policies to its operational functions which are compatible and consistent with the data policies of Peterborough City Council while applying full due consideration to the legal responsibility CCP has toward the data it controls.

# Purpose

The purpose of this policy is to:

* 1. Provide a framework for CCP to apply all relevant aspects of data protection legislation to its activities. Data protection legislation identifies specific rights in relation to data protection, these are codified in this policy and covered in more detail in the section headed individual rights. They are also referenced in separate information sheets. Accordingly, this policy must be considered in conjunction with the following additional documents:
     1. Legitimate Interest Assessments
     2. Data Breach and Incident Reporting Procedure
     3. Data Retention Schedule
     4. Privacy Notice (Right to be Informed)
     5. Right of Access – Information Sheet
     6. Right of Rectification – Information Sheet
     7. Right to be Forgotten – Information Sheet
     8. Right to Restrict Processing – Information Sheet
     9. Right to Object – Information Sheet
     10. Incident Reporting information Sheet
     11. Employee Rights – Information Sheet
     12. Data Sharing Agreements
     13. CCTV Code of Practice
  2. Communicate the policy of CCP in regard to all activities involving the collection, sharing, use and retention of data and ensure all relevant staff are aware of the policy and refer to it in all instances.
  3. Comply with the law in respect of the data CCP holds about individuals.
  4. Protect CCP’s customers, service users, staff and other individuals.
  5. Provide guidance on managing and protecting the organisation from consequences of a breach of its responsibilities.
  6. Follow best practice.
  7. Implement all duties in respect of the data protection legislation and ensure that all its relevant external stakeholders understand and can implement all the requirements of data protection legislation.
  8. Underpin any operational processes and procedures connected with the principles of the legislation.

# Scope

* 1. This policy will apply to anyone collecting, accessing or using personal information whilst acting on behalf of CCP or operating as a representative or associate of CCP.
  2. CCP requires that all third parties acting as Data Processors will comply with the terms of this data protection policy and other related policies and information.

# Application of the Policy

CCP is committed to ensuring this policy is upheld and embedded within the organisation. To that effect, CCP will:

* 1. Incorporate data protection by design and default into all of its operations.
  2. Process data using the lawful basis of legitimate interest. This does not preclude the processing of data by any other lawful method however must be considered as the primary requirement for processing.
  3. 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
  4. Assign responsibility to every staff member involved in processing data to ensure there is a relevant LIA completed and authorised before processing any data.
  5. Consider an opt out at every practicable opportunity.
  6. Obtain consent for marketing purposes or anything which might not reasonably be expected under our legitimate interests.
  7. Apply and comply with conditions regarding the fair collection and use of personal information.
  8. Meet our legal obligations to specify the purpose for which information is used and the basis under which it is processed.
  9. Collect and process appropriate information restricted to the extent that it is needed to fulfil operational needs or to comply with legal requirements.
  10. Document our data processing
  11. Ensure the quality and accuracy of information used.
  12. Apply robust methodology to ensure retention thresholds are complied with.
  13. Take appropriate technical and organisational security measures to safeguard personal information.
  14. Ensure that personal information is not transferred abroad without suitable safeguards.
  15. Ensure that the rights of people about whom the information is held can be fully exercised under the legislation.
  16. Name a person with specific responsibility for data protection in the organisation known as the Data Protection Officer.
  17. Have a committee of trained staff known as the Data Protection Group who will meet regularly under the direction of the DPO.
  18. Provide everyone managing and handling personal information appropriate training and appropriate supervisions.
  19. Clearly communicate to relevant stakeholders to ensure contractual responsibilities for following good data protection practice are fully understood.
  20. Ensure that clear instructions exist for the handling of data including Easyread guides.
  21. Ensure that methods of handling personal information are regularly assessed and evaluated.
  22. Ensure that guidance is in place for robust governance of sharing data with Partners and third parties.
  23. Demonstrate compliance.

# Data Protection Principles

* 1. There are seven Data Protection Principles with which CCP shall comply. In summary, these are that personal data will be:
     + Processed fairly and lawfully in a transparent way
     + Obtained only for specified lawful purposes and not further processed in a manner incompatible with that purpose
     + Adequate, relevant and limited to what is necessary
     + Accurate and where necessary, kept up to date
     + Not be kept for longer than is necessary
     + Protected by appropriate technical and organisational controls
     + Processed in a way with appropriate measures and records to demonstrate accountability
  2. This information is available as a separate information sheet available on CCP’s intranet.

# Application of Principles

* 1. CCP will apply these principles in accordance with this policy. Specifically, CCP will ensure that all data is processed on the authority of a relevant and legitimate LIA and provide access to its privacy notice at all points of collecting data, and grant access to other policies on request.
  2. CCP will 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 mobile devices will require 2 factor authentication to access CCP systems and all data contained on these devices will be password protected and encrypted.
  3. CCP will apply and abide by the rights granted to individuals by data protection regulation.
  4. CCP will seek to obtain consent for the purposes of direct marketing even where a legitimate interest exists

# Individuals Rights

Data protection legislation has mandated a set of rights for individuals. These are summarised below with the approach CCP has adopted in each case.

# The Right to be Informed

* 1. CCP will provide concise, transparent, intelligible and easily accessible information when processing personal data which will ensure that anybody we are collecting data from will be aware of the scope, purpose and retention of their data.
     + Provision of privacy information at the time of collecting data
     + Name and contact details of our organisation
     + Contact details of our DPO
     + The purposes of processing of personal data
     + The lawful basis for processing of the data
     + the legitimate interests for the processing
     + The categories of personal data obtained
     + The categories of recipients of personal data
     + Details of transfers to international organisations
     + Retention periods for the data
     + Individual rights in respect of processing
     + The right to withdraw consent
     + The right to complain to the ICO
     + the source of the personal data
     + The details of whether individuals are under statutory or contractual obligation to provide their data.
     + the existence of automated decision-making, including profiling
  2. This information is provided as a separate privacy notice which is available on CCP’s website and intranet.
  3. CCP will update and monitor this policy 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

* 1. Any person whose details are collected, processed and held by CCP has a general right to receive a copy of their own information. CCP recognises that there may be some exceptions to this rule, such as data held on safeguarding.
     + 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 issue a standard form for receiving Subject Access Requests (SAR) however recognises all requests whether the form is used or not.
     + 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>
  2. Relevant guidance and information is available as a separate information sheet accessible on the CCP intranet.

# The Right of Rectification

* 1. An individual has the right to have their data rectified if it is inaccurate or incomplete normally but not exclusively as determined by a completed SAR.
     + 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>
  2. Relevant guidance and information is available as a separate information sheet accessible on the CCP intranet.

# The Right to Erasure

* 1. 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 the data subject 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
  2. CCP retains the right to override any requests made under the right to erasure where the legitimate interests of CCP justify the override.
     + 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>
  3. Relevant guidance and information is available as a separate information sheet accessible on the CCP intranet.

# The Right to Restrict Processing

* 1. This is effectively an alternative to the right to erasure where a data subject may request that their data is restricted in use. Data may be processed in the authorised way but on granting this right, may only be used according to the restrictions.
  2. This right may also be exercised to extend the retention of data under certain circumstances such as where the processing activity is the destruction of the data etc.
  3. 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
  4. 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/>
  5. *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

* 1. 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.
  2. 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
  3. 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

* 1. An individual can object to the processing of their data where it is processed for the following:
     + Our legitimate interests of lawfully processing
     + Public interest or exercise of official authority
     + Direct marketing
     + Purposes of scientific/historical research and statistics.
  2. 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/>
  3. Relevant guidance and information is available as a separate information sheet accessible on the CCP intranet.

# Rights related to automated decision making including profiling

* 1. 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.
  2. 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.
  3. 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 on the CCP intranet.

# 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 indecent which might lead to any of the above
  2. City College Peterborough holds a large and varied amount of data which includes personal and special category data and information.
  3. 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.
  4. 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.
  5. 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.
  6. 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.
  7. This part of the policy must be considered in conjunction with the Data Breach and Incident Reporting Procedure.

# 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 24).
     1. 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:
        + Any data controlled by CCP where that control is lost, intentionally or not
        + Data is processed or held contrary to general ICO guidance
        + Any part of this policy on data protection is not adhered to or complied with
        + Any activity occurs not in good faith of CCP’s policies, guidance and information
        + 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](file://ccp-srv-02/Departments/GDPR/CCP%20Policies%20%26%20Notices/Data%20Breach%20and%20Incident%20Reporting%20Procedure%20-%20Draft.docx). 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:/g/EcZehiz36DZJoY2R7w1f2PUBzKuyHkZo6MBkJz-D7_i8Lg?e=gQG2z0), or in person or by phone to the DPO.
     + All data incidences are evaluated by the Data Protection Group Breach Assessment Team (BAT), including 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
  2. The Data Protection Group can be contacted at [DPO@citycollegepeterborough.ac.uk](mailto:DPO@citycollegepeterborough.ac.uk) or via individual contact list found [HERE.](https://citycollegepeterboroughac.sharepoint.com/:w:/g/EdJPRy8_0XRJtb3sB_VCcQsBpA6qqdi_FWBS8I5OfAppHw?e=zIokEK)

# 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
     + 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)
  2. The decision on the escalation of any data breach ultimately rests with the Head of the Organisation (Executive Principal), or their deputy, under the advice of the DPO.
  3. Consequently, CCP will not report any incidences to the ICO, data subjects or data controllers without the express permission and/or knowledge of the Executive Principal.
  4. In the event the Executive Principal is not available, the authority is delegated to Principals in agreement.
  5. 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/>
  6. 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.
  2. 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.
  3. 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.
  4. 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
  5. Where data is received by CCP from a third party data controller which appears inconsistent with data protection legislation, the following applies:
     1. The incident is to be considered a data incident
     2. The incident must be reported following the Data Breach and Incident Reporting procedure
     3. 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 Executive Principal.

# 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:
     + In an authorised format and way
     + Only be sent to a confirmed designated and authorised recipient
     + In a protected format, physical or password
     + Never 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
      + Using a generic 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.

# Data Sharing Agreements

* 1. 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.
  2. 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 Data 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
     + And 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.

# Appendix

**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.

**Personal Information**

Personal information is defined as​ ​information relating to a living individual who can be identified directly or indirectly from that information. It may also be possible to identify an individual from that and other information which is in the possession of, or likely to come into the possession of CCP. It also includes any expression of opinion about the individual and any indication of the intentions of CCP or any other person in respect of the individual.

It is important to note that, where the ability to identify an individual depends partly on the information held and partly on other information (not necessarily data), the information held will still be personal.

**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

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**

**Executive Principal**

The Executive Principal 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 Executive Principal 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 Executive Principal is supported in this responsibility in accordance with the normal operational structure and hierarchy of CCP.

The Executive Principal 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. Within the group are three named members of a Breach Assessment Team (BAT) who act with, or on behalf of the DPO in 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 Executive Principal 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.

**Policy Review**

A review of this policy will take place annually to take account of any new or changed legislation, regulations or business practices.

**Monitoring Compliance**

Compliance with this policy and related standards and guidance will be monitored as part of the work of the Data Protection Group. Findings will be reported to the Data Protection Officer.

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.

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.

As part of the monitoring and evaluation, an action plan for continuous improvements in Data Protection practices will be promoted as required by the Data Protection Group.

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.

**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.

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.

**Basic Quick Rules**

* Check that you have a completed LIA to process data.
* Check that you have an information sharing agreement in place if you need to share data externally to CCP.
* Think about data as it were about you.
* Hold data only for as long as it is needed.
* Destroy files correctly and confidentially.
* Make sure you have accurate data.
* Keep your passwords safe and secure, they are **not** to be shared with anyone else.
* Lock your PC whenever you leave it unattended, even for a minute.
* Make sure any documents are not left on your desk if they contain personal or sensitive information.
* Do not disclose personal information unless you are **sure** you can, and you **know** who is asking for it.
* Suspect an incident? Report it straight away.
* Above all, if in any doubt, ask for advice.

**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.

Managers and Supervisors must make all staff aware of the Good Practice Guidelines below that must be followed during the handling of all personal information.

**Document control**

|  |  |
| --- | --- |
| Revision issue date: | May 2021 |
| Next Review Due Date: | May 2024 |
| Date of most recent Equality Impact Assessment: | ? |
| Document Lead and Author: | Original author – Graham Jones; lead – Adele Fender |
| Approvers and dates: | Governing Board |
| 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. |

**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 assessible 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 . . . . . . . . . . . . . . . . |