

# CAPITAL CITY PARTNERSHIP



## Staff Handbook – September 2023

### Contents

Code of Conduct .....	2
Workplace Visitor Policy .....	6
Leave and Public Duties Policy .....	9
Flexible Working Policy .....	12
Sickness Absence Policy .....	15
Maternity, Adoption, Shared Parental and Partner Support Leave Policy .....	18
Expenses Policy .....	25
Volunteering Policy .....	27
Safeguarding Policy .....	29
Performance Review and Development Policy .....	33
Disciplinary Policy .....	36
Grievance Policy .....	40
Whistleblowing Policy .....	44
Internet, Email & Social Media Policy .....	47
GDPR Data Protection Policy (Business) .....	52
Cyber Security Policy .....	71
Equality and Diversity Policy .....	74
Health and Safety Policy .....	76
Anti-bribery and corruption Policy .....	79
Recruitment and Selection Policy .....	82
Notice Periods .....	85

## Code of Conduct

User group:	All employees
Policy category:	HR
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

The Capital City Partnership Code of Conduct outlines the standard of behaviour that employees are required to adhere to.

### Scope

This code of conduct applies to all paid employees of CCP, volunteers and those under our care on work experience, internships or other activity that requires supervision in our workplace.

### Policy elements

#### **Compliance**

CCP has a staff handbook which outlines a range of policies and procedures that employees must adhere to. Employees are required to ensure they have read and understood all policies within the handbook.

#### **Personal conduct**

Employees are always expected to behave professionally and courteously to all colleagues and customers and conduct themselves in a manner that maintains CCP's good reputation. Employees are expected to comply with the reasonable instructions of their line manager and other managers.

#### **Alcohol and drugs**

Consumption of alcohol or drugs is not normally permitted in the workplace during normal working hours. Exceptionally, alcohol may be permitted as part of an approved workplace event, with the prior approval of the Chief Executive Officer.

An employee who is found to be or becomes unfit to undertake the contractual duties of their post due to the consumption of alcohol or drugs will be sent home, and if necessary, may be accompanied. This matter will be dealt with by their line manager and/or Chief Executive Officer through CCP's Disciplinary Procedure when they are fit to return.

#### **Inappropriate conduct outside of work**

Inappropriate conduct outside of work may result in disciplinary action if it directly impacts on or affects the employee's ability to do their job or has the potential to damage CCP's reputation.

If an employee is charged by the police and is the subject of criminal proceedings, they must disclose this to the Chief Executive Officer as soon as practicable, except where the individual is directed by the criminal justice system not to disclose this.

### **Assets, systems and information**

Employees are responsible for safeguarding CCP's assets, systems and information under their control or accessed as part of their job. Assets can include but are not limited to property, equipment, vehicles, information and financial transactions. Employees may also be permitted to access telephones, internet, email and other business systems and encounter privileged and sensitive information. The use of these must be for legitimate company business and comply with relevant policies and procedures such as Data Protection and Cyber Security policies.

### **Conflict of interest**

A conflict of interest can arise if an employee's outside activities, private, personal or financial interests influence or interfere with the decisions that they make in the course of their work for CCP, or that they appear or can be perceived to influence or interfere with the decisions they make when working for CCP. Employees are responsible for declaring any actual or potential conflicts of interest to their line manager.

Employees of CCP must not misuse their position or any information obtained in the course of their employment to further their own interests or the interests of others who do not have the right to benefit under CCP's policies. Employees should never use their position to seek special favour or preferential treatment for themselves, relatives or personal contacts.

### **Personal relationships**

Employees should not be involved in appointments or decisions relating to discipline, grievance, promotion, expenses payments etc where they are related or have a close personal relationship out of work to the applicant or employee. Where such a relationship exists or develops between employees who either work together in the same area or where one employee is in a position of authority, the employees must declare this in confidence to their line managers, where there is the potential for a conflict of interest to arise.

### **Business integrity**

Employees are required to comply with all applicable legal requirements and regulations relevant to the work they undertake. These can include compliance with externally set registration requirements and professional standards of conduct.

CCP does not tolerate bribery of any kind and employees are liable to disciplinary action including dismissal, legal proceedings and imprisonment if they are either involved in bribery and corruption or do not report instances of bribery and corruption.

## **Media use**

Employees should only have contact with the media in the course of their employment where this has been approved in advance. Contact from the media in the first instance should be referred to the Business and Communications Officer. If an employee requires contact with the media to be made, they should contact the Business and Communications Officer for advice first.

CCP operates a range of social media platforms and the procedure for how these are used is detailed in the Social Media policy.

## **Political sensitivity**

CCP is an Arm's Length External Organisation (ALEO) of the City of Edinburgh Council with its board membership drawn from elected members and partners. CCP is chaired by an elected member.

CCP acknowledges that employees are also citizens and as such may have personal views and opinions on ideas and policies, and this is part of democratic debate. Employees are expected however, to take care to avoid situations where their personal views could be perceived as representing CCP's position. Within this context, employees should not release information that is not yet in the public arena or promote viewpoints that undermine CCP's position and that of its Board members. In their capacity as an employee, they should not criticise CCP and its Board members (and their organisations) through any form of media, in public online or at meetings, in written communication or in any context that would likely cause harm to CCP's reputation.

If an employee is in doubt about what actions they can or cannot take they can seek advice from their line manager.

## **Secondary employment**

CCP recognises that employees may wish to undertake secondary employment but expects that an employee's total working time should not exceed an average of 48 hours per week, considering all jobs that the employee undertakes. Secondary employment includes engaging in work on a fee paying or recognition in kind basis, self-employment, or engaging in any other business activity.

Where there may be a conflict of interest, or the possibility of an adverse effect on your role at CCP, such secondary employment must be declared to the Chief Executive Officer for approval.

Employees are not allowed to undertake secondary employment at their normal place of work (i.e. CCP) or use CCP equipment in undertaking secondary employment. Communications or the conduct of any business activity relating to secondary employment is not permitted during working hours.

## **Procedure**

### **Reporting concerns**

If an employee feels that theirs or another employee's conduct contravenes the code of conduct (or other employee policies in the CCP handbook), they should raise this immediately with their line manager. If their concerns relate to their line manager, they should be raised with their line manager's manager. If the circumstances where malpractice is taking place, CCP has a Whistleblowing Policy that should be referred to.

All concerns will be taken seriously and CCP will take the appropriate action to maintain confidentiality and ensure that employees are protected from victimisation. CCP will only involve other agencies and share information with the consent of the employee unless it relates to concerns around the protection of vulnerable people, or where due regard must be given to criminal processes.

Failure to raise concerns, without good reason, or raising false concerns maliciously or vexatiously may result in disciplinary action being taken against that employee.

### Disciplinary consequences

Failure to follow this code of conduct will be treated seriously and may lead to disciplinary action being taken, up to and including dismissal.

## Workplace Visitor Policy

User group:	All employees, partners and stakeholders
Policy category:	General Health and Safety
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

The workplace visitor policy outlines the rules for receiving visitors on Capital City Partnership's (CCP) premises at 14 Links Place.

We want to ensure that visitors will not:

- Pose threats to our premises and property
- Distract employees from their work
- Be exposed to danger

### Scope

This policy applies to all paid employees of CCP, volunteers and those under our care on work experience, internships or other activity that requires supervision in our workplace.

Workplace visitors can include, but not limited to:

- employees' friends and family (hereafter referred to as personal visitors);
- contractors;
- external vendors;
- employees of partner organisations;
- stakeholders; and
- members of the public.

This policy does not refer to remote employees or employees from other company locations e.g. Recruitment and Skills Centres. These employees should refer to the appropriate visitor policies in place in the premises that they work from.

For employees that are on leave e.g. parental, career break, whilst being employees of CCP at that time, the workplace visitor policy will apply.

### Policy elements

#### **All visitors**

The following applies for all visitors:

- Visitors must sign in the visitor book and show a form of identification
- Employees must always attend to their visitors when they are on the premises

- Our data protection and confidentiality policies temporarily cover all visitors whilst they are on the premises. Visitors must not misuse the internet connection, disclose confidential information or take photographs without permission from CCP. If a visitor is found not complying with CCP policies, they may be escorted off the premises and/or face prosecution if appropriate
- Visitors are allowed during normal working hours. Visitors who wish to gain access outside of these hours must have written permission from the Chief Executive Officer
- Visitors must adhere to the process and procedures as set out in CCP's Health and Safety policy.

### **Personal visitors**

The following applies for personal visitors:

- Employees may bring personal visitors to company events or to other events after obtaining permission from the Chief Executive Officer
- Common areas, such as lobbies, may be open to visitors, but this should be for a short period of time and for specific reason
- The main CCP office at Links Place is shared occupancy therefore the employee is responsible for their personal visitors at all times when on the premises
- Visitors under the age of 16 should be accompanied by an adult and should receive written permission from the Chief Executive Officer prior to gaining access to the premises.

Employees may not allow access to the premises to unauthorised personal visitors (exceptions can be made on a case-by-case basis with the written permission of the Chief Executive Officer).

### **Contractors and external vendors**

Contractors, suppliers and service vendors e.g. IT technicians, plumbers etc, can only enter the premises to complete job duties that have been notified/agreed in advance. It is the responsibility of the Chief Executive Officer (or in his/her absence a Senior Manager) to ensure these visitors use the visitor book.

### **Other visitors**

Other visitors that CCP may receive are, but not limited to, students, investors customers, job candidate, business partners etc. These visitors should always be accompanied by an employee of CCP whilst on the premises.

### **Unauthorised visitors**

Employees who come in to contact with an unauthorised visitor may ask them to leave. Visitors that misbehave (e.g. engage in hate speech, cause disruption or steal property) will be asked to leave and in some cases, where appropriate, be prosecuted.

## **Accidents**

CCP has a Health and Safety policy that applies to all staff and visitors of CCP. If a visitor has an accident, this must be reported to a member of the CCP management team and recorded in the accident book.

## **Procedure**

This policy directly relates to employees who have their working location at 14 Links Place, Edinburgh.

For CCP employees who work at a satellite office such as Fort Kinnaird, FUSE etc. they should adhere to the visitor policies in place in those locations.

## **Disciplinary consequences**

Employees who do not comply with this policy may face disciplinary consequences in proportion to their violation. The Chief Executive Officer will determine how serious an employee's offense is and take the appropriate action such as:

For minor violations (e.g. bringing in personal visitors without authorisation) employees may receive verbal reprimands

For serious violations (e.g. bringing in unauthorised visitors who rob or damage company property), employees may face severe disciplinary actions which could result in termination.



## Leave and Public Duties Policy

User group:	All employees
Policy category:	HR
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

This policy sets out contractual leave entitlements (paid and unpaid) of Capital City Partnership's (CCP) employees and the procedure to support employees who require time off to carry out public duties during their contractual working week.

### Scope

This policy is for all paid employees of CCP.

### Policy elements

#### Annual leave

The leave year is from 1 April to 31 March (inclusive). At the start of employment annual leave entitlement is 36 days for full time employees which is made up as follows:

- 26 days annual leave
- 6 floating days to cover public holidays
- 4 fixed days to cover public holidays at Christmas (2 days) and New Year (2 days).

Leave entitlement for part time employees is granted pro-rata.

Leave entitlement increases by one day per year of service to a maximum of five additional days i.e. until they have reached 30 days annual leave. The additional day will be added on to the next annual leave year only after a full year has been worked by the employee. For example, when an employee joins the organisation in August, the following August they will qualify for an additional day of leave as they have reached a year's continuous service; however, this additional day will be added to their leave entitlement when the next annual leave year commences the following April.

Leave should be taken within the current leave year. Where this is not possible a maximum of five days can be carried over to the new leave year but must be taken by 30 June, subject to agreement by the Chief Executive Officer. In exceptional circumstances, the Chief Executive Officer may give approval for additional leave in excess of 5 days to be carried over to the next leave year.

Illness occurring during a period of annual leave or public holiday will continue to be treated as annual leave unless covered by a medical certificate or agreed by the Chief Executive Officer. In these cases, the employee may be credited with their annual leave for the illness period that it relates to and allowed to take it later in the leave year. Information on CCP's sickness procedures is detailed in the separate 'Sickness Absence Policy'.

Annual leave will continue to accrue during maternity leave and can be taken after maternity leave ends. Leave entitlement must be confirmed with the employee's line manager prior to returning to

work. CCP's Maternity, Adoption, Shared Parental and Partner Support Leave Policy gives further detail on this process.

On termination of employment leave will be calculated pro-rata to termination date and any leave due to that date must be taken prior to termination date.

### **Requesting leave**

Leave requests will be authorised by the line manager. Employees should request leave using the Who's off system and give as much notice as reasonably possible. When the leave request is for one week or more, a minimum of two weeks' notice is required. Leave requests for three weeks or more can only be authorised by the Chief Executive Officer.

Where leave requests are for less than one week e.g. several days annual leave or lieu days, employees are required to give three working days' notice.

All leave requests will be subject to prior approval, and every effort will be made to meet the employee's requests; however, consideration will also be given to business need.

### **Special leave**

CCP acknowledges that through an employee's life there are changes that take place that may require employees to require additional time off to meet other demands placed on them. CCP has a range of special leave options in place to support employees at these times. These examples below are based on employees working a full-time working pattern and will be amended pro rata to reflect reduced working hour contracts.

- In the event of an employee requiring maternity, maternity support, paternity and/or adoption leave CCP has a separate policy to refer to
- Dependency leave: Five days paid leave and five days unpaid leave per year with prior approval from the Chief Executive Officer
- Funeral leave for:
  - Next of kin: Five days paid leave which may be extended at the discretion of the Chief Executive Officer. Five days unpaid leave may also be granted
  - Near relative: One day paid leave with additional leave at the discretion of the Chief Executive Officer
  - Other cases: Leave, paid or unpaid, may be granted at the discretion of the Chief Executive Officer
  - Leave of absence: Additional leave, paid or unpaid, may be granted in special circumstances at the discretion of the Chief Executive Officer.

### **Jury and witness service**

An employee receiving a summons to serve on a jury will be granted special leave with pay subject to deduction of allowances provided by the court of law under the jurors' allowances regulations.

Where an employee is cited to attend as a witness paid leave of absence will be granted. In these circumstances an employee should claim all allowances entitled under the jurors' allowances regulations and declare these claims to CCP in order that appropriate adjustments to salary payments can be made.

### Public duties

Employees who are local authority councillors shall be granted reasonable leave of absence with pay to undertake approved duties with the local authority concerned. Allowances claimed for these duties should be declared to CCP in order that appropriate adjustments can be made to salary payments.

Employees who are engaged by government departments in an advisory capacity shall be granted leave of absence with pay to undertake such duties. Allowances claimed for these duties should be declared to CCP in order that appropriate adjustments can be made to salary payments.

Employees who are appointed justices of the peace or as members of children's panels shall be granted leave of absence with pay limited in the first instance to 24 half days per year to undertake duties in connection with their appointments.

Where an employee is engaged in any other duties leave of absence will be subject to discussion and agreement by the Chief Executive Officer.

### Disciplinary consequences

All employees are obliged to comply. Any employee found to be in breach of the policy will be subject to disciplinary action which could lead to termination.

## Flexible Working Policy

User group:	All employees
Policy category:	HR
Last reviewed or modified:	September 2022
Review date:	March 2024

### Policy brief and purpose

Capital City Partnership (CCP) operates a system of flexible working hours. This policy ensures that flexible working arrangements are achieved with no negative impact on the overall efficiency of the organisation.

### Scope

This policy applies to all paid employees of CCP.

### Policy elements

Employees are entitled to request flexible working arrangements and will be supported by CCP if their job duties permit it. The Chief Executive Officer has discretion to exclude employees from the scheme or to restrict the extent of flexible working to meet the organisation's needs e.g. employees that come into direct physical contact with customers.

#### Hours of employment

The normal working week consists of 35.75 hours. This is broken down as:

- Monday to Thursday 9.00am – 5.30pm
- Friday 8.30am – 3.15pm

with a daily break of one hour for lunch.

#### Core hours

The working day is divided into core time and flexible bands. Core time is from 10.00am to 12noon and 2.00pm to 4.00pm daily [except for Friday where core time is 2.00pm to 3.15pm]. During these times all employees, except those with prior written permission from the Chief Executive Officer, must be on duty.

The working week has a provision for one hour per day for lunch; but employees can choose to increase this to two hours or reduce this to 30 minutes.

The flexible bands are from 7.00am to 10.00am and 4.00pm to 7.00pm on Monday to Thursday and 7.00am to 10.00am and 3.15pm to 7.00pm on Friday.

### **Compressed working hours**

CCP supports flexible working including compressed working where this does not have a negative impact on the service delivery of the organisation.

If an employee wishes to be considered for changing their working pattern to a compressed one, they must discuss this with their line manager in the first instance to determine whether this would be practically possible. All requests must then be submitted in writing to the Chief Executive Officer and approved in advance of any changes to the working pattern being actioned.

Employees who work a compressed working pattern are excluded from the flexi time system during this time. Where an employee was previously part of the flexi time system, all debit or credit that has been accumulated must be cleared prior to the start of an agreed compressed working pattern.

### **Monitoring hours**

CCP operates a self-monitoring flexible hours system whereby the individual employee is responsible for monitoring their working hours in consultation with line managers. Hours of attendance should be recorded and managed by the individual employee for each week (net of lunch breaks). If an employee works longer hours one day, they can balance out their hours by working a shorter day the following day.

Normal visit such as doctor or dentist appointments will be accounted for under the terms of flexible working and should be debited as appropriate out of core hours. However, where there are exceptional circumstances such as hospital appointments, these will require the prior permission of the Line Manager and only with a corresponding medical appointment letter.

Staff leaving the organisation must clear their debit or credit time by the final working day. Uncleared debit will be regarded as unpaid absence and final salary will be deducted accordingly. Unclear credit will be forfeited.

The Chief Executive Officer has the authority to terminate or suspend the system or to exclude individuals from the system and if so, this change will be made with no less than 24 hours notification either verbally or in writing.

### **Overtime/weekend duty**

It is not the policy of CCP to pay for additional hours worked but where an episode of late or weekend work is necessary it must be approved in advance by the Chief Executive Officer.

The employee will be compensated by time off in lieu as follows:

- Time and a half for Saturdays and after 7.00pm on weekdays
- Double time for Sunday working.

### **Home working**

Home working is defined as where an employee works from home or when they complete their work at a place located outside of the company's premises. Working from home arrangements can be occasional, temporary, or permanent. Employees should note that CCP retains the right to alter an employee's working from home arrangements where business need supersedes in this

arrangement i.e. to cover for staff holidays or illness, or where the employee is required to attend a meeting.

Normal working hours should apply while off site unless exceptional arrangements are specifically authorised by the Chief Executive Officer. While home working, staff are expected to remain contactable during working hours. CCP has a Data Protection Policy and Cyber Security Policy which also applies to all employees who are homeworking.

### Disciplinary consequences

Anyone found abusing any part of the flexible working policy may have their participation suspended either temporarily or indefinitely, and whilst under suspension will be required to work normal fixed hours on site at a CCP office identified by the Chief Executive Officer.

## Sickness Absence Policy

User group:	All employees
Policy category:	HR
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

This policy outlines Capital City Partnership's (CCP) processes and procedures for sickness absence and pay.

### Scope

This policy is for all paid employees of CCP.

### Policy elements

#### Sick pay

CCP pays more sick pay than the statutory minimum (£99.35 per week), so your sick pay includes any Statutory Sick Pay (SSP) that you might be entitled to:

Length of service when sickness absence starts	You will get full pay for:	You will get half pay for:
Less than 1 year	1 month	1 month
1 year but less than 2 years	2 months	2 months
2 years but less than 3 years	4 months	4 months
3 years but less than 5 years	5 months	5 months
5 years or more	6 months	6 months

Where sick pay is awarded CCP will continue to make contributions to the pension scheme in order to preserve continuity of employee's membership and benefits within the scheme.

#### Absences due to injury

Instances of absence which are as a result of an injury will be considered with due regard to any relevant legislation and individual circumstances. Additional sick pay may be awarded at the discretion of the Chief Executive Officer.

#### Sickness during annual leave

If an employee falls sick during a period of annual leave, they should telephone their line manager on the first day of sickness. The period of sickness absence shall be treated as sick leave and not annual leave. The normal process for certification should still be followed.

Where sickness prevents an employee taking their annual leave entitlement this may be carried forward to the following leave year provided it is taken within a reasonable time agreed by the Chief

Executive Officer. The Chief Executive Officer will also consider the length of absence and annual leave already taken to date.

### **Out-patient attendance**

Employees attending hospital or clinic for treatment as an out-patient must provide evidence such as appointment card, letters etc.

## Procedure

### **Notification of an absence**

Employees prevented from reporting for duty owing to illness must inform their line manager before 10am on the first day of absence. Employees must inform their manager of:

- Why they are off
- How long they think they will be off
- Any work that urgently needs to be completed whilst they are off.

### **Logging sickness absence**

All staff must record their sickness leave on the Who's Off system. This must be done on the first day of absence and updated each sick day thereafter. If a member of staff is physically unable to log the sickness themselves, they must inform their line manager who will ask a member of the HR team to log the leave on their behalf.

In exceptional circumstances, where an employee cannot contact their line manager themselves due to their absence, they should ensure that someone else makes contact on their behalf.

CCP has a duty of care to all its employees. If the line manager has not heard from an employee when an employee was due to start work, they will try to contact the employee to find out why they are not at work and ensure that they are safe. If they are unable to contact the employee or the employee's designated emergency contact and the employee fails to contact the company, this absence will be treated as unauthorised until a reasonable explanation is provided.

### **During the absence period**

Employees should maintain reasonable contact with their line manager during a period of absence, typically around the first, fourth and last day of a short period of absence (7 days or less).

Where an absence is longer than 7 days, employees should maintain regular contact as agreed by them and their manager, typically weekly contact.

All absences must be supported by a [self-certificate](#) or medical certificate as follows:

- Absences of 1-7 calendar days: employee must complete a CCP self-certificate on return to work
- Absences of more than 7 calendar days: Employees must consult a doctor before or after seventh day and submit a medical certificate signed by a doctor/GP/medical professional



In cases of prolonged illness i.e. more than 14 calendar days, employees should, where practicable, give at least three working days' notice of their intention to return to work.

### **Returning to work**

Employees should inform their line manager prior to returning, when their expected return to work day will be. Line managers will arrange a return to work (RTW) interview with the employees, usually on the first day of return, to review their absence and return to work, including support or adjustments that are needed. A [RTW form](#) will be completed.

Prior to the RTW interview, line managers will review the employee's absence history over the last 12 months. If there are patterns seen to be emerging such as multiple regular periods of absence after annual leave, weekends etc line managers will arrange further discussions with the employee to look at these patterns and what interventions may be required to support the employee.

### **Termination of employment through illness**

Where it is necessary to terminate employment through illness, an employee will be given notice in accordance with their entitlement. Payment will be made at full rate during the notice period.

### **Death in service**

In the event of death in service, payment will be made to the employee's next of kin at full salary to the end of the current pay period i.e. to the end of the month.

### **Disciplinary consequences**

Failure to comply with this policy or submission of falsified information may result in sick pay being withheld and could lead to disciplinary action.

Unauthorised absence(s) may result in disciplinary action and termination. An example of unauthorised absence would be sickness absence over 7 days without providing a medical certificate.

# Maternity, Adoption, Shared Parental and Partner Support Leave Policy

User group:	All employees
Policy category:	HR
Last reviewed or modified:	March 2022
Review date:	March 2024

## Policy brief and purpose

This policy sets out contractual entitlements of Capital City Partnership's (CCP) employees and the procedure to support employees who are undertaking parental responsibilities.

## Scope

This policy is for all paid permanent employees of CCP. Employees on fixed term contracts will be entitled to statutory maternity/paternity/adoption support as defined in legislation at the time that a request for such support is made.

## Policy elements

### **Maternity leave and pay**

All employees have a legal entitlement to reasonable time off, with pay, for antenatal care, regardless of length of service or hours worked. It is also important to attend classes in preparation for the birth. Reasonable paid leave will be granted to attend these. For all appointments, confirmation should be sought at the first appointment and shown to their line manager to request time off for further appointments.

Employees may also be entitled to government incentives, schemes or benefits when expectant such as Statutory Maternity Pay (SMP), maternity allowance, child benefit etc. Further information on these government benefits can be found on the gov.uk website: <https://www.gov.uk/maternity-pay-leave>. CCP provides enhanced maternity benefits if employees meet specific eligibility criteria.

### Employees with less than 26 weeks continuous service

Employees who have less than 26 weeks continuous service with CCP by the beginning of the 15th week before their expected week of childbirth (EWC) will be entitled to take up to 52 weeks of maternity leave:

- Maternity leave can start any time after the 11th week before the EWC right up to the date of childbirth and can be decided by the employee.
- Further unpaid leave up to a maximum of 63 weeks may be granted at the discretion of the Chief Executive Officer.
- In accordance with health and safety legislation, the first two weeks starting from the date of childbirth are known as compulsory maternity leave and must be taken off.

Employees are entitled to 39 weeks of paid leave which is made up as follows:

- The first 14 weeks at full pay – inclusive of any Statutory Maternity Pay (SMP).
- The following 25 weeks at the flat rate of SMP.

Further information on SMP can be found on the Government website:

<https://www.gov.uk/maternity-pay-leave>

#### Employees with at least 26 weeks continuous service

Employees who have at least 26 weeks continuous service with CCP by the beginning of the 15th week before their expected week of childbirth (EWC) will be entitled to take up to 63 weeks of maternity leave:

- Maternity leave can start any time after the 11th week before the EWC right up to the date of childbirth and can be decided by the employee.
- Maternity leave, however, cannot continue longer than 52 weeks from the week of childbirth, which means that if an employee wishes to take the full 63 weeks, this is only possible if they take the 11 weeks prior to the week of childbirth.
- In accordance with health and safety legislation, the first two weeks starting from the date of childbirth are known as compulsory maternity leave and must be taken off.

During maternity leave all contractual benefits except remuneration must be maintained.

Employees are entitled to 39 weeks of paid leave which is made up as follows:

- The first 26 weeks will be paid at full pay (inclusive of any SMP)
- The following 13 weeks at the current flat rate of SMP or 90% of your average weekly earnings (whichever is lower).

Any further leave will be unpaid.

SMP is paid in the same way as your wages (for example monthly or weekly). Tax and National Insurance will be deducted.

Payments are made on the understanding that employees will be returning to CCP employment for a period of at least three months after maternity leave ends. If they do not return to work for the required period, they will be required to refund to CCP, at its discretion, the equivalent of 8 week' maternity pay issued at normal pay less any SMP paid as part of the 8 weeks' pay.

Employees whose contract of employment is due to end either during maternity leave or at the end of maternity leave period will continue to receive the appropriate pay and leave as detailed above until the end of maternity leave or the end of their contract of employment, whichever happens first. Any employee who has received maternity pay and does not return to CCP employment as a result of their contract of employment ending during or shortly after maternity leave will not be required to repay any payment made during maternity leave.

If an employee is unsure whether they will return to work, they can choose to receive 8 weeks normal pay and defer payment of any remaining entitlement until a later date. If an employee does not intend to return to work, the maternity pay above will be restricted to 8 weeks normal pay plus any entitlement to SMP.

### Returning to work

Employees have the right to return to work following maternity leave to the same job on the same terms and conditions of employment.

Annual leave will continue to accrue during maternity leave and can be taken after maternity leave ends. Leave entitlement must be confirmed with the employee's line manager prior to returning to work.

Keeping In Touch (KIT) days are designed to assist the employer and employee to plan for the employee's return. An employee can use a maximum of 10 KIT days in the lead up to returning to work, if they are used for specific purposes e.g. attendance at key meetings or training sessions, undertaking a specific piece of work etc. KIT days are not mandatory and must be agreed in advance by both the employer and employee and will be regarded as a work day and the employee will be paid appropriately.

Informally, other arrangements such as social events, meeting for coffee, telephone calls or emails can be used to reintegrate employees. These informal arrangements are voluntary and unpaid.

CCP is committed to encouraging parents to return to work after they have had a baby. It is recognised that parents may wish to alter their patterns of working to be able to combine their work and family responsibilities and CCP's 'flexible working policy' outlines alternative working arrangements. Requests by employees to change their existing arrangements are entirely voluntary and there will be no automatic right for employees to have a request approved.

### Choosing not to return

Employees who decide not to return to work at the end of their maternity leave should resign in writing to their line manager. If appropriate, they may be invited to a meeting to discuss the reasons for resigning and whether there are any alternative measures or support that can be put in place by CCP to help them stay at work.

If an employee takes full maternity pay and does not return to work for at least three months after their maternity leave, they will be required to pay 8 weeks maternity pay issued to them at normal pay less any SMP paid as part of this 8 weeks' pay.

### **Adoption leave and pay**

CCP acknowledges that the selection process for becoming adoptive parent(s) involves several assessment visits at home. CCP will give employees reasonable paid leave to attend those meetings. Employees are asked to give their line managers reasonable notice of the meetings and copies of the appointment letters from the adoption agency to confirm, the meeting times/dates.

All employees are entitled to up to 52 weeks adoption leave which can start up to 14 days before the expected date of the placement. They may also be entitled to adoption pay such as Statutory Adoption Pay (SAP) and other government benefits. For further information on this visit <https://www.gov.uk/adoption-pay-leave/pay>

### Employees with at least 26 weeks continuous service

CCP pays enhanced adoption pay as they want employees to return to work after the adoption leave ends. Employees who have at least 26 weeks continuous service with CCP by the date they are notified that they have been matched as adoptive parent(s) will be entitled to enhanced adoption pay:

- The first 26 weeks will be paid at full pay - inclusive of any Statutory Adoption Pay (SAP)
- The following 13 weeks at the flat rate of SAP.

If an employee does not return for a minimum of three months after the adoption leave ends, they will be requested to pay back the equivalent of 6 weeks' adoption pay (this will be their normal weekly pay less any Statutory Adoption Pay paid). If an employee is sick during the three months return period, the length of sickness absence will not count towards the return period.

Please note that only 1 person in a couple can take adoption leave. The other partner could get partner support leave (detailed below).

### Contact with work

Employees and their line manager should maintain reasonable contact during the adoption leave. This allows opportunities to discuss plans for returning to work, other vacancies in CCP, development opportunities or significant workplace developments and changes during the time off.

Before going on adoption leave, the employer and employee must agree what the contact arrangements will be – how often and how it will happen e.g. office visits, home visits, telephone, email etc. Any changes should be mutually agreed, and this contact does not constitute work therefore does not count towards KIT days.

### **Shared parental leave**

Employees will be eligible to apply for shared parental leave if both parents are employees of CCP. CCP will consider requests for shared parental leave on an individual basis.

### **Partner support leave and pay**

Employees can take partner support leave and pay if they are taking time off to look after a child if they are:

- The partner of someone who is about to give birth
- The partner of someone who is taking adoption leave/pay.

### Before birth

If the employee is the child's parent, or the partner/nominated carer of a person expecting a baby, they are entitled to paid time off to accompany the birth parent to up to three antenatal appointments. For all appointments, confirmation should be sought at the first appointment and shown to their line manager to request time off for further appointments.

### Before adoption

If the employee is adopting a child, they are entitled to a maximum of three working days paid partner support leave to attend meetings as part of the adoption process. Employees are asked to give their line managers reasonable notice of the meetings and copies of the appointment letters from the adoption agency to confirm, the meeting times/dates.

### After birth/placement

Partner support leave is only applicable if their partner is taking maternity or adoption leave. Employees are not entitled to partner support leave or pay if they are already in receipt of maternity leave and pay or shared parental leave and pay.

If the employee is matched with more than one child at the same time (e.g. siblings) or there is a multiple birth (e.g. twins), they are only entitled to one period of leave.

Partner support leave can only be taken as one whole block. Leave must be taken within 56 days (8 weeks) of the child's birth/placement.

### Employees with less than 26 weeks continuous service

Employees who are employed with less than 26 weeks continuous service up to the 15th week before EWC or date of notified match:

- 2 weeks at full pay.

### Employees with at least 26 weeks continuous service

CCP offers employees with at least 26 weeks continuous service up to the 15th week before EWC or date of notified match:

- 4 weeks at full pay.

### **In the event of a still birth or death of a child**

If the baby is born after 24 weeks of pregnancy the employees right to maternity leave/pay and the right to return to work are unaffected. If the baby dies before 24 weeks of pregnancy the employee will be entitled to sick pay/leave in accordance with the CCP absence policy.

If the employee resigns from CCP to have a baby, but the child does not live, the employee will be entitled to return to work but not necessarily to their previous post. Any return to work under these circumstances must be within the maximum period allowed for maternity leave.

### **Birthday Leave**

If an employee's birthday lands on a working day, they can take the day off as an additional day's leave, outside of their allocation.

### **Once in a Lifetime Leave Allowance**

CCP offers 1 week (pro-rata) leave with full pay for a special event in your life.

This one-off allowance is available to all staff who have a minimum of 5 years continuous service.

The offer can only be used once and does not repeat after an additional 5 years.

### **Procedure**

#### **Maternity leave**

To qualify for maternity leave, at least 15 weeks before the EWC or as soon as reasonably possible, CCP must be notified of:

- The fact that an employee is pregnant (not necessarily in writing)
- The EWC through a MAT1 form which is available from GP/midwife
- When the employee wishes to start maternity leave, in writing (which can be altered by giving 28 days' notice of the amended date in writing).

#### **Adoption leave**

To qualify for adoption leave, when the employee has been notified that they have been matched, they should inform their manager within 7 days of being told by the adoption agency, or as soon as reasonably possible. CCP should be given:

- Confirmation in writing that they have been matched by the adoption agency
- The date the child will be placed with the adoptive parents
- The date that the employee wishes to start their adoption leave (which can be altered by giving 28 days' notice of the amended date in writing)
- The adoption certificate from the adoption agency (CCP acknowledges that this may not be available immediately)

Once the line manager has received the above (acknowledging that the adoption certificate may not be available immediately), they will write to the employee within 28 days confirming the latest date that they can return to work (if the full entitlement of adoption leave is being taken).

Employees will not get adoption leave if the child is already living with them, for instance, if they are adoption their partners' child(ren).

If employees are adopting more than one child at the same time (e.g. siblings) they will only get one period of adoption leave.

If the child's placement ends for any reason while an employee is on adoption leave, they can continue their adoption leave for up to 8 weeks after the placement ends.

#### **Partner support leave**

When an employee has decided that they would like to take partner support leave, they must notify their line manager immediately in order to discuss when leave will be taken. Once dates have been agreed, the employee must confirm in writing:

- The EWC or the expected week of placement

- Whether they are taking one- or two-week's partner support leave
- The date they wish to start their leave (which can be altered by giving 28 days' notice of the amended date in writing)
- That they will be supporting the mother or adopter
- That the child is under 18 years old (in the case of adoptions).

In the case of birth, the employee must confirm this in writing no later than the 15th week before the EWC.

### **Birthday Leave**

Birthday leave can only be taken on the day of the employee's birthday and must be booked on WhosOff under 'Birthday Leave'.

### **Once in a Lifetime Leave Allowance**

Employees must complete the Once in a Lifetime Leave Request Form which must be signed off by line management before being submitted to HR for approval.

### **Disciplinary consequences**

All employees are obliged to comply. Any employee found to be in breach of the policy will be subject to disciplinary action which could lead to termination.



## Expenses Policy

User group:	All employees
Policy category:	HR
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

Capital City Partnership (CCP) will reimburse business related spend that is incurred by an individual employee when proof of purchase is provided.

### Scope

This policy applies to all paid employees of CCP.

### Policy elements

#### **Mobile phone allowances**

CCP will provide employees a mobile phone for work purposes upon request and the employee will claim the costs of running the phone through their expenses. If an employee requires a mobile phone but chooses to use their own device instead of obtaining a phone from CCP, then employees are entitled to claim a set fee of £10 per month towards mobile phone costs. No receipts are required to claim this.

Each employee must discuss this first with their line manager who will decide if there is a viable business case for either a CCP purchased mobile phone or contribution towards personal mobile costs. This business case must be approved by the Chief Executive Officer via the line manager prior to purchases or expenses claims being made.

#### **Subsistence allowances**

Subsistence expenses incurred whilst carrying out company duties will be reimbursed at the actual rate of expenditure provided this is reasonable and supported by documentary evidence.

Prior authority from the Chief Executive Officer should be sought where an overnight stay is involved. Where an overnight stay is required, hotel receipts should be attached to any claim for reimbursement. Evening/morning meals and soft drinks will be reimbursed for the individual employee only and upon production of receipts. CCP will not pay for the cost of alcoholic beverages.

## Travel

CCP will reimburse for travel costs that are incurred during work but not for the cost of travel from an employee's home to their place of work as part of their regular commute. Payment will only be made on approved travel costs from designated base to place of business.

Home to designated base travel costs will only be paid where the following conditions operate:

- During normal office hours: the actual travel costs should be claimed where a journey is from office base to place of business and back to office base. Where the employee travels from home directly to place of business, or travels from office base to place of business and finishes at home, then the actual costs for the journey or the costs between base and place of business and return (whichever is less) should be claimed
- Evening or weekend work: Where the journey undertaken is from home to place of business and return to home, the actual costs for the journey should be claimed. Exact details of the journey or legs of a journey should be shown on claims as should the purpose of the journey.

CCP promotes the use of public transport where reasonable and practical to reduce the impact on the environment. When using public transport copies of travel tickets/receipts must be submitted with an expense claim.

If an employee chooses to use a personal vehicle for business purposes, they must ensure that such use is covered by the terms of their insurance policy and provide evidence of this prior to use.

In claiming mileage allowance mileage should be shown as whole miles – fractions of a mile should be rounded to the nearest whole number. Mileage allowances are shown below and reviewed annually:

### Cars and vans:

- 45p per mile for the first 10,000 business miles
- 25p per mile thereafter.

### Bicycles:

- 20p per mile for the first 10,000 business miles
- 20p per mile thereafter.

## Procedure

It is not encouraged for employees to incur expenses regularly out with of travel and mobile phone costs. If purchases are required to be made for the business by an individual employee, they should consult with their line manager or the Finance Manger as far in advance as possible prior to incurring expenses.

An expenses form must be completed quarterly and submitted to the line manager for approval with relevant copies of receipts attached.

## Disciplinary consequences

It is an offence to knowingly claim expenses that have not been incurred and any employee found to be in breach of the policy will be subject to disciplinary action which could lead to termination and/or prosecution.

## Volunteering Policy

User group:	All employees
Policy category:	HR
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

This policy outlines CCP's approach and the principles and practices by which CCP involves volunteers in the organisation.

### Scope

This policy is for all individuals that are volunteers for CCP and includes those that are based in CCP's satellite locations e.g. Recruitment and Skills Centres. For all CCP employees who would like to undertake volunteering elsewhere, please refer to the Performance and Development policy.

### Policy elements

Capital City Partnership recognises that voluntary work brings benefits to the volunteers themselves and to those that they work alongside with.

CCP will:

- ensure that all volunteers are properly integrated into the organisation
- not use volunteers to replace paid employees
- foster a positive working environment for volunteers and expects all employees to work positively with volunteers
- support volunteers to meet their personal development goals whilst in placement.

### Procedure

#### Recruitment

Recruitment of volunteers will generally be from all sections of the community and will be reflective of CCP's Equality and Diversity policy. Individuals that are interested in becoming a volunteer for CCP should in the first instance contact the Chief Executive Officer, explaining what they would like to volunteer to do and why. If the Chief Executive Officer identifies that there may be a role suitable

for the individual, then they will be invited to meet with the Chief Executive Officer and/or other relevant managers to discuss this further.

Volunteers will be given a [volunteer agreement](#) before commencing their volunteering role, which will outline the role that they are expected to undertake and the expected duration of the volunteering placement. In some cases, volunteers may be subject to reference checks dependant on the role that they are undertaking.

Volunteers will be given induction and training appropriate to the specific tasks that will be undertaken by them.

### **Support**

During the placement, volunteers will be assigned a name contact in the organisations who will provide regular support. Dependant on the volunteer role, this could be in the form of face to face meetings or via email.

### **Expenses**

CCP will meet all out of pocket expenses.

### **Data protection**

CCP will keep minimal data on volunteers and further information on CCP's data retention is outlined in the Data Protection policy.

All volunteers will be subject to the data protection principles as outlined in CCP's data protection policy. Volunteers will not have access to confidential and sensitive data in order to carry out their volunteering role and will always be made aware of adhering to confidentiality during their volunteering placement.

### **Ending a placement**

Volunteers will agree with the Chief Executive Officer how long their placement will be before they start. CCP reserves the right to terminate this earlier in exceptional circumstances.

Where placements have been completed CCP will support a volunteer's request for a reference.

### **Work experience placements**

Work experience requests must be made in writing to the Chief Executive Officer, clearly stating what the individual would be expecting to gain from a work experience placement and what expectations they have. All work experience requests will be considered on an individual basis and will also be assessed against the company's insurance, health and safety and other relevant policies to ensure compliance. All work experience placements must have the approval of the Chief Executive Officer before commencing.

### **Disciplinary consequences**

Volunteers are expected to comply with the policies in the staff handbook that are relevant to them, and these are identifiable in the scope of each policy. If volunteers breach these policies, CCP has the right to terminate their placement with minimal or no notice (dependant on the seriousness of the breach).

## Safeguarding Policy

User group:	All employees
Policy category:	Health and safety
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

Capital City Partnership (CCP) supports a range of projects which, at times, work with vulnerable adults and/or children. The safeguarding policy aims to ensure the welfare and protection of adults and children that access services provided on or behalf of CCP by:

- Promoting good practice and work in a way that prevents harm, abuse and coercion occurring
- Ensuring that allegations of abuse or suspicions are dealt with appropriately and the person experiencing abuse is supported
- Preventing abuse from occurring or continuing

In this context, vulnerable adults are defined as:

- People aged 18 or over
- Who are receiving or may need support services because of learning, physical or mental disability, age, illness
- Who are or may be unable to take care of themselves, or unable to protect themselves against significant harm or exploitation.

### Scope

This policy applies to all paid employees of CCP, volunteers and those under our care on work experience, internships or other activity that requires supervision in our workplace. This policy also applies to CCP Board Directors.

### Policy elements

In order to implement the policy CCP will work:

- To promote the rights of all people to live free from abuse and coercion
- To ensure the safety and wellbeing of people who do not have the capacity to recognise or report abusive behaviour that they are experiencing
- To manage services in a way which promotes safety and prevents abuse
- To recruit staff and volunteers responsibly, ensuring all necessary checks are made
- To provide effective management for staff and volunteers through supervision, support and training.

CCP will:

- Ensure that all employees, Board Directors and other individuals working for CCP are familiar with the policy

- Notify the appropriate authorities if abuse is suspected or likely e.g. if the concern relates to a worker, volunteer or organisation who provide a service to vulnerable adults or children
- Inform service users that information may be passed to relevant authorities if deemed appropriate to safeguard the wellbeing of an individual or a group of individuals (this includes during investigation where sensitive and personal information will be treated with complete confidentiality but CCP will release information to the police and statutory agencies if required to assist formal investigations)
- Endeavour to keep information up to date with national developments relating to preventing abuse and maintaining the welfare of adults and children
- Ensure that staff are aware of their responsibility to refer incidents of adult and child abuse to the relevant statutory agencies including the Police (Appendix 1)
- Provide appropriate support to employees and volunteers working directly with service users who have, or are experiencing, abuse.

## Procedure

In this policy the definition of abuse includes (but is not limited to):

- Physical abuse: hitting, slapping, punching, burning, misuse of medication, inappropriate restraint
- Sexual abuse: rape, indecent assault, inappropriate touching, exposure to pornographic material
- Psychological or emotional abuse: belittling, name calling, threats of harm, intimidation, isolation
- Financial or material abuse: stealing, selling assets, fraud, misuse or misappropriation of property, possessions or benefits
- Neglect and acts of omission: withholding the necessities of life e.g. medication, warmth or food; ignoring medical or physical care needs
- Discriminatory abuse: racists, sexist, based on a person's disability; other forms of harassment, slurs or similar treatment
- Institutional or organisational: regimented routines and cultures, unsafe practices, lack of person-centred care or treatment
- Any of the above carried out either deliberately or unknowingly and as a single act or repeated acts.

## Reporting concerns

- If an act of abuse is witnessed, it should be reported directly to the police and the Chief Executive Officer of CCP should be informed
- If there are general concerns about an employee, volunteer or anyone working on behalf of CCP, or if a service user has raised concerns with an employee or volunteer, this should be reported to the Chief Executive Officer as soon as reasonably possible. The Chief Executive Officer will investigate immediately and seek advice from the appropriate authorities, and may notify the police if appropriate
- If the concern relates to the Chief Executive Officer, it should be reported to the Board of Directors
- If the concern relates to the organisation, it should be reported to the Office of the Scottish Charities Regulator (OSCR).

Any reports of abuse or concerns relating to possible abuse, made to CCP, will be fully investigated, clearly recorded using the [safeguarding reporting form](#) and reported to the CCP Board, and where necessary referred to the police and relevant statutory agencies.

CCP is committed to maintaining confidentiality wherever possible (see Data Protection Policy) and information relating to abuse or suspected abuse will only be shared with necessary individuals or agencies.

CCP will ensure that employees who have witnessed or reported abuse or suspected abuse will be kept informed of process, actions and outcomes, where this does not interfere with police and other relevant statutory bodies' investigations.

### **Receiving a report**

If you receive an allegation:

- Reassure the person concerned
- Listen to what they are saying
- Record what you have been told/witnessed as soon as possible using the [safeguarding reporting form](#)
- Remain calm and do not show shock/disbelief
- Tell the person concerned that the information will be treated seriously
- Do not start to investigate or ask detailed/probing questions
- Do not promise to keep it a secret.

If an incident of abuse has just taken place the priorities will be to:

- Call an ambulance if required
- Call the police
- Preserve evidence
- Keep yourself, employees, volunteers and service users safe
- Inform your manager or Chief Executive Officer
- Record what happened including names, dates, locations and details of the abuse
- If the individual experiencing abuse does not have the capacity to consent a referral will be made to the appropriate statutory services without the individual's consent to promote and safeguard their interests.

### **Managing allegations made against an employee or volunteer**

CCP will ensure that all allegations made against an employee or volunteer will be dealt with swiftly. Where the individual accused is thought to have committed a criminal offence the police will be informed immediately.

A risk assessment will be undertaken immediately to assess the level of risk to the individual accused and all other individuals that they will encounter. This will include whether it is safe for them to continue in their role or any other role within the service whilst an investigation is ongoing.

The Chief Executive Officer will liaise with the relevant statutory agencies to discuss the appropriate course of action and ensure that CCP's disciplinary procedures are coordinated with any other enquiries taking place as part of an ongoing process to manage the allegation.

## Disciplinary consequences

All employees are obliged to comply with this policy. Any employee that is discovered to have been aware of an incident of abuse and failed to report this will face disciplinary consequences.

### Contact details for reporting concerns

#### Capital City Partnership

Chief Executive Officer – Tel: 07566230608

Email: [rona.hunter@capitalcitypartnership.org](mailto:rona.hunter@capitalcitypartnership.org)

#### Edinburgh

Social Care Direct - Tel: 0131 200 2324

Email: [socialcaredirect@edinburgh.gov.uk](mailto:socialcaredirect@edinburgh.gov.uk)

#### East Lothian

Tel: 01875 824 309 - Mon-Thurs 9am-5pm and Fri 9am-4pm

Email: [communityaccess@eastlothian.gov.uk](mailto:communityaccess@eastlothian.gov.uk)

Emergency Social Care service (for out of normal hours, weekends and public holidays) Tel: 0800 731 6969 (freephone)

#### Midlothian

Tel: 0131 271 3900 (Mon-Thurs 9am-5pm, Fri 9am-3.30pm)

Emergency Social Care service – Tel (freephone): 0800 731 6969 at any time outside normal office hours

#### National

Police Scotland: Tel 101 for non-emergencies and 999 for emergencies

Office of the Scottish Charities Regulator (OSCR): <https://www.oscr.org.uk/contact-oscr/charity-concern-form>



## Performance Review and Development Policy

User group:	All employees
Policy category:	HR
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

This policy outlines Capital City Partnership’s approach and process to performance review and development (PRD). The PRD scheme governs the ability of employees to progress incrementally within the grade of their post, through a regular review process.

### Scope

This policy is for all paid employees of CCP.

### Policy elements

#### **The PRD process**

Employees upon completion of a successful PRD can move incrementally within the grade of their post. Once they have reached the top point of a grade, there is no further incremental progression although they will still receive any ‘cost of living’ award that is agreed annually. This will take effect from 1 April each year and any delay in applying this will be backdated.

The PRD year is from 1 April – 31 March of the following year (in line with the holiday and financial year). Progress against agreed objectives is assessed, as well as the identified core competencies for the grade of the post.

#### **The PRD meeting**

Employees should gather evidence over the 12-month period that can be used to demonstrate how they have achieved their objectives and competencies. Evidence can be gathered in many ways such as keeping a log of progress and examples of when competencies have been displayed, feedback from colleagues etc. This should then be summarised for the PRD meeting in the [PRD form](#). Behaviour descriptions for the core competencies are summarised in [PRD guidance note](#).

After the meeting, the employee and their line manager will sign the completed PRD form to reflect that they both agree on the year’s performance, and whether an incremental rise is appropriate. If an agreement cannot be reached, the form should remain unsigned and be referred to the Chief Executive Officer who will review the form and meet with the employee and line manager to mediate and seek a resolution.

If no resolution can be reached the Chief Executive Officer will make the final decision and sign the form.

Objectives for the next 12 months should then be set for the employee.

Employees will progress incrementally through development zones if they have not been subject to any disciplinary action in the preceding PRD year. Staff members recruited in Q4 (January – March)

will not receive their development zone increment until the following April. Anyone at end of a development zone, moving into contribution zone will move one SCP only as staff can only move up one contribution zone point per year and must do this through passing objectives set out in the PRD process. Progression through contribution zones will be by assessment and recommendation by the line manager, and increments will only be made if it can be demonstrated that the employee has met their objectives and the core competencies of their grade.

### Personal development plan

The personal development plan helps the employee to achieve their objectives and meet the desired behaviours for their role. The form should be completed with their line manager and should detail the:

- Development objectives that identify which of the employee's competencies or skills (technical/specialist/other) would benefit from further development
- Development activities/descriptions that identify how the employee is going to develop and should fall into one of following categories:
  - E-learning
  - Guided reading
  - On the job training
  - Workplace visits
  - Projects
  - Coaching
  - Mentoring
  - Secondments
  - Conferences
  - Training events
  - Shadowing/exchanges
  - Vocational/academic qualifications
  - Other.

Support for employee learning and development may range from adjusting working pattern to accommodate studies, additional leave and / or unpaid leave. In some instances, limited financial support may also be provided. Priority will be given to learning and development that is identified as essential and all offers of financial assistance will be subject to budget constraints. Each request will be considered on merit and any costs £500 or over must be supported by a [business case](#). Certified courses must be evidenced.

### **Time off work**

Time off work to undertake a learning and development course must be approved by the employee's line manager and/or the Chief Executive Officer.

Time off will be granted only if it is deemed to be beneficial to the employee's role and does not negatively impact the work of CCP.

### **Financial support**

CCP may pay up to £1,000 towards/for a learning and development course if:

- It is directly relevant the employees' post

- The time commitment will not be detrimental to the workload of the employees' team
- There is sufficient budget for it.

CCP may contribute 50% of the cost of a learning and development course, up to a maximum of £800, if:

- It is somewhat relevant to the employee's post
- The time commitment will not be detrimental to the workload of the employees' team
- There is sufficient budget for it.

Each financial contribution is based on a financial year, up to a maximum of three financial years and will be reviewed annually. The maximum financial contribution any single employee can receive for a learning and development course is £3,000 in total.

### Procedure

For all learning and development opportunities, in the first instance this must be identified through PRD discussions and agreed by line managers.

Training or learning courses under £500, can be approved by line managers provided they have the necessary budget.

For training or learning courses £500 or over, managers must put a [business case](#) forward to be authorised by the Chief Executive Officer prior to enrolment.

Volunteering opportunities will be assessed on the same criteria and given appropriate support dependant on the level of relevance those opportunities have to an employee's individual job and/or personal development.

### Disciplinary consequences

All employees are obliged to comply.

Any employee found to be in breach of the policy will be subject to disciplinary action which could include:

- withdrawal of participation on the learning course/programme
- repayment of financial assistance to CCP
- termination of employment contract.

Poor standard of work performance is termed unsatisfactory conduct and will lead to warnings short of dismissal (unless repeated). Further information is detailed in the CCP 'disciplinary policy'.

## Disciplinary Policy

User group:	All employees
Policy category:	HR
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

The disciplinary policy is intended to be used to correct and improve standards of behaviour. The Chief Executive Officer and Senior Managers are responsible for management and discipline within Capital City Partnership (CCP). An employee has the right to be represented at all stages of the disciplinary process by an accredited trade union representative or another employee of CCP.

Action taken will be based on investigation of the incident or circumstances in question, considering any witness statements.

### Scope

This policy applies to all employees of CCP.

### Policy elements

#### **Decisions, representations and appeals**

In the first instance, the Chief Executive Officer or Senior Manager will arrange to interview the employee. The employee will be:

- Advised of the nature of the interview
- Advised of their right to be accompanied by a representative of their choice
- Allowed reasonable time to consult their representative
- Given the opportunity to make a statement
- Able to discuss the matter in full in the interview
- All reasonable measures will be taken to arrive at a true and accurate position.

If the investigation gives grounds for the Chief Executive Officer/Senior Manager to believe that the outcome would be disciplinary action against the employee, the Chief Executive Officer/Senior Manager will advise the employee and their representative. A decision can be deferred for a period not exceeding 7 working days from the date of notification to allow the employee and/or their representative to carry out consultation with a trade union official. Within that period, the trade union official representing the employee can meet with the Chief Executive Officer/Senior Manager to discuss the case further, to hear the outcome of the investigation and to make representation before disciplinary action is taken.

In reaching a decision the Chief Executive Officer/Senior Manager will consider all the circumstances, such as the employee's length of service and past performance, the nature of the misconduct and/or the standard of performance that may require disciplinary action.

If the employee remains aggrieved after these representations, they have the right to formal appeal as outlined in the procedure section of the policy within each stage.

### **Summary suspension or dismissal**

Employees will not normally be dismissed for a first offence but there are exceptional circumstances of gross misconduct which could lead to summary dismissal with no prior oral or written warning.

Examples of gross misconduct are (this list is not exhaustive):

- Serious offences against the interests of CCP include wilful injury to others and wilful damage to CCP property
- Incapacity on duty because of alcohol or substance use
- Fraudulent salary claims; including falsification of expenses claims
- Gross insubordination
- Neglect of duty resulting in serious consequences
- Fighting in the work place
- Theft from CCP or an employee of CCP
- Theft from the public
- Falsification of information to CCP to secure employment
- Failure to declare criminal convictions during employment with CCP that may impact on the employees' ability to carry out their role or bring CCP into disrepute
- Exceptionally grave or repeated offences of the types listed under the unsatisfactory conduct section.

The line manager will pass details of a case of gross misconduct to the Chief Executive Officer and inform the employee and their line manager that this action has been taken.

No decision on disciplinary action will be taken until the Chief Executive Officer has interviewed the employee and they have been given the opportunity to present an explanation of the matter.

Consideration will be given to mitigating circumstances. A lesser penalty may be imposed which may take the form of a final written warning instead of dismissal. In any event, the decision will be confirmed in writing, together with a clear statement of the reasons. Copies of this will be given to the employee and the employee's representative.

### **Records**

Where an offence warrants summary dismissal but the Chief Executive Officer, due to mitigating circumstances, imposes a lesser penalty (which will include a final written warning) this will be noted on the employee's personnel record (where appropriate).

### **Unsatisfactory conduct**

Instances of failure to observe and maintain CCP discipline which are less serious than offences of gross misconduct are termed unsatisfactory conduct and will lead to warnings short of dismissal (unless repeated). Examples of these are:

- Bad time keeping
- Absences without reasonable cause
- Poor standard of work performance
- Negligence
- Refusal to carry out a reasonable instruction.

## Procedure

### **Verbal warning**

Can be applied in situations where an employee's work performance and/or conduct is unsatisfactory, and despite having received support to improve this from their manager they have been unable to demonstrate improvement over a reasonable period. The employee will be interviewed within fourteen days, having been informed of the nature of the interview. If appropriate, the employee may be issued with a verbal warning which will be recorded and retained on their personnel file for 3 months, after which it will be removed. The employee will be informed of their right of appeal.

### **First written warning**

If, following the employee receiving a verbal warning, a further related offence occurs, or their work performance does not improve, the circumstances will be investigated. A manager will arrange to interview the employee, advising them of the nature of the interview their rights. If it is decided that disciplinary action is appropriate, a first written warning will be issued within 7 days and will confirm:

- Any previous verbal warning
- The employee's offence or details of the unsatisfactory performance
- What action/improvement is required
- The consequence of a further related offence/lack of improvement in performance.

The written warning is recorded on the employee's personnel file and retained for 6 months. If there is no further cause for concern during that period, the warning will be considered as lapsed and reference to it in the personnel file will be removed. The employee has the right to appeal a first written warning within 7 days of receiving written notice of the warning.

### **Final written warning**

If a further related offence occurs or the employee fails to undertake the actions/improvements identified from the first written warning, the circumstances will again be investigated. The manager will arrange to interview the employee advising them of the nature of the interview and their rights. If it is deemed appropriate, a final written warning will be issued and will confirm:

- Any previous verbal and written warnings
- The employee's offence or details of the unsatisfactory performance
- What action/improvement is required
- The consequence of a further related offence/lack of improvement in performance.

The written warning is recorded on the employee's personnel file and retained for 12 months. If there is no further cause for concern during that period, the warning will be considered as lapsed and reference to it in the personnel file will be removed. The employee has the right to appeal a first written warning within 7 days of receiving written notice of the warning.

### **First and final warning**

In certain circumstances an employee's misconduct may be significantly serious that the first stages of the policy are bypassed and a first and a final warning is issued.

### **Dismissal**

If a further related offence occurs or the employee fails to undertake the actions/improvements identified from the final written warning within 12 months of the warning being issued, the circumstances will again be investigated. The manager will arrange to interview the employee

advising them of the nature of the interview and their rights. In certain circumstances it may be necessary to suspend the employee on full normal pay pending completion of the investigation and decision.

Employees may be dismissed for disciplinary reasons in situation such as:

- Persistent misconduct and/or continuous unsatisfactory performance after previous reference to the written warning system
- Gross misconduct – an employee may be summarily dismissed without previous reference to the written warning system.

If dismissal is identified to be the appropriate disciplinary action, the employee will be made aware in writing of:

- Any previous valid warnings
- The reason for the decision
- The effective date of termination of employment.

The employee has the right to appeal against the decision in writing within 7 days of receiving written notice of the dismissal.

### **Precautionary suspension**

Managers have delegated powers to apply precautionary suspension to an employee who is posing a threat/danger to themselves or others e.g. being under the influence of alcohol. In this situation, the employee will be asked to leave the workplace and the required to report to the Chief Executive Officer (or nominated senior manager) no later than 12noon of the next working day (unless they can provide a medical certificate). At this point, the circumstances will be considered by the Chief Executive Officer/manager and disciplinary action may be taken.

### **Levels of authority**

<b>Stage</b>	<b>Initiated by</b>	<b>Notification to</b>	<b>Actioned by</b>	<b>Redress to</b>
Verbal warning	Line manager	CEO	Line Manager	CEO
First written warning	Line manager	CEO	Line manager	CEO
Final written warning	Line manager / CEO		CEO	
Suspension	CEO		CEO	
Dismissal	CEO		CEO	

When disciplinary action is taken against a manager, redress will be to the next highest level of management.

### **Disciplinary consequences**

The disciplinary consequences of not following this policy are described throughout the policy.

## Grievance Policy

User group:	All employees
Policy category:	HR
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

Capital City Partnership (CCP) recognises the importance of creating a working environment in which all employees feel confident about raising matters of concern relating to their employment. The Grievance Policy provides a process to deal with these concerns wherever possible at an early stage, through discussion and agreement.

It should also be noted that CCP has a separate Whistleblowing Policy for all employees if they believe that they have discovered malpractice or impropriety, to be able to voice their concerns in a responsible and effective manner.

### Scope

This policy applies to all paid employees of CCP, volunteers and those under our care on work experience, internships or other activity that requires supervision in our workplace.

This policy is designed to deal with employment related concerns, such as:

- Work or working arrangements
- The office and its equipment (including health and safety concerns)
- The employment contract
- Equal opportunities issues.

This policy cannot be used to challenge decisions that are made outside CCP, such as tax, national insurance matters or legislative changes.

CCP is confident that most grievances raised by staff are genuine and in good faith. However, if a grievance is found to be deliberately vexatious or malicious this will be treated as a serious disciplinary offence and may constitute gross misconduct. A vexatious or malicious grievance includes one that:

- Is not made in good faith e.g. is based on deliberate misrepresentations or untruths
- Can be considered unreasonable e.g. where an individual continues to raise the same issues that have been formally addressed previously.

### Policy elements

#### Roles and responsibilities

All employees are responsible for:

- Making sure they understand the grievance policy
- Trying to deal with grievances informally in the first instance
- Raising a grievance in writing if it has not been settled at the informal stage
- Stating the outcome that they are seeking.



All managers are responsible for:

- Making sure they understand the grievance policy
- Making sure their employees are aware of, and understand, the grievance policy
- Dealing with grievances promptly and informally where possible
- Handling grievances sensitively and confidentially, making sure standards of fairness, objectivity and consistency are followed in all cases.

Grievance processes must be treated as a high priority by managers, employees and trade representatives so they can be completed as quickly as possible.

### **Representation**

At any formal meeting held under the grievance policy, an employee will have the right to be accompanied by:

- An accredited workplace trade union representative
- A CCP employee
- A full time official employed by a trade union.

If the representative is a CCP employee, they will be allowed reasonable time off with pay to attend grievance meetings. Separate arrangements will apply if the representative is a trade union official. The representative cannot answer any questions put directly to the employee however they can help the employee to present their case. Employee and representative may talk privately at any time during the meeting.

## Procedure

### **Stage 1 – Informal grievance**

The employee should raise any grievance informally in the first instance with their line manager. Both employee and line manager should aim to resolve the grievance at this stage. Grievance(s) may be raised by:

- Discussing concerns with the line manager
- Discussing concerns with the line manager's manager or Chief Executive Officer if the concern is either about the line manager, or if the employee feels uncomfortable discussing concerns with the line manager
- Speaking directly to the individual concerned, if the concern relates to another employee and the individual feels it is appropriate to do so.

During the informal discussion(s), the grievance should be discussed in detail with the employee:

- What the employee is concerned about and why i.e. what impact is it having on the employee
- The outcome the employee is seeking and whether this is possible and appropriate
- The implications of adopting a course of action.

Often a resolution can be met through discussion and clarification, but if the issue is more complex, the individual with whom the grievance has been raised with may require time to investigate the circumstances of the grievance. This will be done without unreasonable delay.

At the conclusion of an investigation, or within five working days of the grievance being raised, the manager/Chief Executive Officer should inform the employee verbally of any action that will be

taken. The manager/Chief Executive Officer will then monitor the situation to ensure that any action/decision taken is effective.

### **Stage 2 – Formal grievance**

If the grievance is not resolved at the informal stage, the employee should raise the matter within 10 working days in writing. The employee should set out the details of the grievance and submit this to the line manager who will hear the grievance with the Chief Executive Officer. If the grievance is about the line manager, formal written grievance should be sent to the Chief Executive Officer.

Following receipt of the grievance and any supporting documents, the appropriate manager will arrange a Stage 2 meeting to consider the grievance. The meeting will be arranged within 10 working days of receiving the written grievance unless there is joint agreement to extend this timescale. The manager conducting the grievance meeting will make sure all relevant information is presented and considered. Where appropriate, other managers/employees involved at an earlier stage will attend the meeting to aid discussions. In particularly complex cases, the manager conducting the meeting may seek appropriate external support and advice from qualified bodies.

After the grievance meeting, a decision will be sent to the employee in writing, with 10 working days. There are five possible outcomes to a grievance:

#### Grievance upheld

The manager who heard it will explain any action that will be taken to resolve the concern(s) raised. This may include:

- Clarifying or changing working practices
- Providing additional training and/or support
- Agreeing to correct any identified failing
- An action plan to resolve the issues raised.

#### Grievance partially upheld

The manager who heard the grievance decides that only some of the concern(s) raised require action. They will explain which parts of the concern(s) have been upheld and the action that will be taken to resolve them.

#### Grievance not upheld

The manager who heard the grievance decides the concern(s) that have been raised cannot be supported.

#### Further investigation required

The manager who heard the grievance decides that further information is required before a decision can be made.

- The manager will adjourn the meeting and start an investigation. The manager will explain this verbally and in writing, indicating how long the investigation will take
- If another employee is the subject of the grievance, they will be provided with a copy of any relevant information being considered
- When the investigation is finished the manager will decide the outcome of the grievance and provide written confirmation of the findings.

#### Vexatious grievance

The manager hearing the Stage 2 grievance decides that the grievance is vexatious. They will decide whether to take disciplinary action.

### **Stage 3 – Appeal**

The employee may appeal the stage 2 decision by submitting a written request to the Chief Executive Officer within 10 working days of receiving the written outcome of the stage 2 process. An appeal will only be considered based on one or more of the following:

- The process followed was unfair and not followed the grievance policy
- Additional evidence was presented at the time and not considered
- Evidence was considered but misinterpreted
- The conclusion reached was incorrect given the evidence that was presented.

A Stage 3 appeal must include:

- Details of what the employee is concerned about and why
- Why the employee is making an appeal
- Why the employee disagrees with the Stage 2 outcome
- The outcome that the employee is seeking
- Any other relevant information.

No new issues or concerns can be added at this stage. The concerns raised must be the same as those originally raised at Stage 2. If new issues or concerns are raised a new grievance process must begin.

If considered, the appeal will be held with 20 working days of receipt of the written request. The Chief Executive Officer will hear the appeal alone or with selected individuals of authority or expertise, as they deem appropriate.

### [Disciplinary consequences](#)

Any employee found to be making vexatious grievances will be subject to disciplinary action which may result in termination of contract.

## Whistleblowing Policy

User group:	All employees
Policy category:	HR
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

The Public Interest Disclosure Act (which came into effect in 1999), gives legal protection to employees against being dismissed or penalised by their employer as a result of publicly disclosing serious concerns.

Capital City Partnership (CCP) is committed to the highest standards of openness, probity and accountability. This policy is intended to support employees and other members of CCP who believe that they have discovered malpractice or impropriety to voice their concerns in a responsible and effective manner.

This policy is not designed to be used to question financial or business decisions taken by CCP, nor should it be used to reconsider any matters that have already been addressed under complaint, disciplinary or other policies of CCP.

It should also be noted that CCP has a separate Grievance Policy for all employees to raise matters of concern relating to their employment and it may be advisable to read this prior to submitting a concern.

### Scope

This policy applies to all paid employees of CCP, volunteers and those under our care on work experience, internships or other activity that requires supervision in our workplace.

### Policy elements

This policy is intended to cover concerns which are in the public interest and may initially be investigated separately but further on may lead to the invocation of other policies e.g. disciplinary.

Concerns could include (but are not limited to):

- Financial malpractice, impropriety or fraud
- Failure to comply with a legal obligation
- Danger to Health and Safety
- Criminal activity
- Improper conduct or unethical behaviour
- Attempts to conceal any of the above concerns.

### Protection

This policy is designed to offer protection to those employees of CCP who disclose concerns provided the disclosure is made:

- In good faith

- In the reasonable belief of the individual making the disclosure that it shows malpractice or impropriety.

It is important to note that no protection from internal disciplinary procedures is offered to those who choose not to use this procedure. In an extreme case, malicious or wild allegations could result in legal action against the employee.

### **Confidentiality**

CCP will treat all such disclosures in a confidential and sensitive manner. The identity of the individual making the disclosure may be kept confidential if it does not hinder or frustrate any investigation. However, the investigation process may reveal the source of the disclosure, and in some cases the individual making the disclosure may be required to make a statement as part of the evidence for the investigation.

### **Anonymous allegations**

This policy encourages individuals to identify themselves when making a disclosure. Concerns expressed anonymously are much less credible, and it will be at the discretion of CCP whether these progressed, considering the following factors:

- The seriousness of the issues raised in the disclosure
- The credibility of the concern
- The likelihood of confirming the allegation from attributable sources.

### **Untrue allegations**

If an individual makes an allegation in good faith which is not upheld upon investigation, no action will be taken against that individual. In making the disclosure the individual should exercise due care to ensure the accuracy of the information.

If, however, an individual makes malicious or vexatious allegations, particularly if they persist with making them, disciplinary action may be taken against that individual.

## **Procedure**

### **Receiving a complaint**

On receipt of a disclosure, the individual who receives the disclosure must pass this information (as soon as is reasonably possible) to the appropriate designated investigating officer as follows:

- Complaints of malpractice will be investigated by the Chief Executive Officer unless the complaint is against the Chief Executive Officer or is any way related to the actions of the Chief Executive Officer, in which case this will be passed to the Chair of the CCP Board for referral
- Where a complaint is connected to the Chief Executive Officer but not against them, the Chief Executive Officer will nominate a Senior Manager to act as the alternative investigating officer
- Complaints directly against the Chief Executive Officer will be passed to the Chair of the CCP Board to appoint an investigating officer.

The individual making the disclosure has the right to bypass the line management structure and take their complaint directly to the Chair of the CCP Board. The Chair has the right to refer the complaint back to the Chief Executive Officer if they feel that it can be investigated appropriately without any risk of conflict of interest.

If there is evidence of criminal activity, then the investigating officer should inform the police as soon as possible. CCP will ensure that any internal investigation does not obstruct a formal police investigation.

### **Investigating a complaint**

The investigating officer should:

- Obtain full details and clarification of the complaint
- Where the concern raised relates to another employee/member of CCP, inform the individual concerned as soon as practically possible, including their right to be accompanied by a trade union or other representative at any interview/hearing held during an investigation
- From the beginning, consider the involvement of the company auditors and the Police and consult with the Chair of the CCP Board
- Investigate the concerns fully and where appropriate with the assistance of other individuals/bodies
- Upon completion of the investigation, decide what the outcome is concerning the complaint and the validity of the complaint. This decision should be presented in a written report to include the findings of the investigation and reasons for the decision. The report should then be passed to the Chief Executive Officer or Chair of the CCP Board (whichever is appropriate dependant on the complaint). If appropriate, a copy of the outcome will be passed to the company auditors to enable a review of procedures.

The individual who made the disclosure will be kept informed of the progress of the investigation and if appropriate, the outcome. If they are not satisfied that their concern is being properly dealt with by the investigating officer, they have the right to raise it in confidence with the Chief Executive Officer/Chair of the CCP Board.

If the investigation finds the complaint to be unsubstantiated and all internal procedures have been exhausted, but the individual who made the complaint is not satisfied with the outcome of the investigation, they have the right to make disclosures to prescribed persons (such as the Health and Safety Executive, Audit Commission etc).

### **Disciplinary consequences**

The Chief Executive Officer/Chair of the CCP Board, upon review of the report, will decide what action should be taken. If the complaint is shown to be justified, the disciplinary or other appropriate CCP policies and procedures will be invoked.

## Internet, Email & Social Media Policy

User group:	All employees
Policy category:	Information and technology
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

This policy outlines Capital City Partnership's (CCP) processes and rules governing the use of internet, email and social media for both business and personal use, accessed via company or personal devices.

It sets out how employees must behave when using the company's social media accounts. It also sets out how employees must behave when using their personal social media accounts, especially when they can be linked back to CCP and could have an impact on the reputation of the company.

### Scope

This policy applies to all employees of CCP. This policy applies to both business and personal use of social media.

### Policy elements

Guidance on accessing internet sites and use of company email addresses is provided. Employees may be able to access social media services and social networking websites at work. CCP acknowledge that social media can bring great benefits to the company, particularly for building relationships with current and potential stakeholders and partners. However, it is important that employees who use social media do so in a way that enhances the company. A misjudged status can generate complaints or damage the company's reputation, as well as security and data protection implications that should always be considered.

Social media sites can include (but are not limited to):

- Social network sites such as Twitter and Facebook
- Online review websites such as Trustpilot and TripAdvisor
- Sharing and discussion sites such as Reddit
- Photographic social networks such as Instagram and Flickr
- Question and answer social networks such as Yahoo Answers
- Professional social networks such as LinkedIn

### Responsibilities

Internet access and company email addresses must be used responsibly and with consideration. Content must not be abusive, offensive, inflammatory, obscene or in any way inappropriate. Everyone who operates a company social media account or who uses a personal social media

account is individually responsible for implementing this policy. In addition, the Chief Executive Officer has the following responsibilities:

- Ensuring that CCP uses social media safely, appropriately and in line with the company's objectives
- Providing apps and tools to manage the company's social media presence and track key performance indicators
- Proactively monitoring social media threats
- Working with employees to roll out marketing ideas and campaigns through the company's social media channels
- Ensuring requests for assistance and support received via social media are followed up.

### **Basic principles of social media use**

CCP recognises that social media offers a way for the company to market itself, stay connected online and build its profile. CCP believes that employees should be actively involved in industry conversations online and individually, social media helps employees to make useful connections, collaborate and be innovative. CCP encourages employees to use social media to achieve their professional and personal goals and objectives.

Regardless of which networks are being used and whether they are being used for business or personal use, following these principles will help avoid common pitfalls:

- Know the social network: employees should spend time becoming familiar with the social network before contributing. It is important to read any FAQs and understand what is and is not acceptable on a network before posting messages or updates or commenting on an ongoing discussion/post.
- If unsure, do not post it: Everyone should err on the side of caution when posting to social networks. If an employee feels an update or message may cause complaint or offense (or be unsuitable) they should not post it. Employees can always consult the Chief Executive Officer or line manager for advice.
- Be thoughtful and polite: Many social media users have got into trouble simply by failing to observe basic good manners online. Employees should adopt the same level of courtesy used as when communicating using other means such as email.
- Look out for security threats: Employees should be on guard for social engineering and phishing attempts. Social networks are also used to distribute spam and malware. Further information on staying secure online is detailed in CCP's 'cyber security policy'.
- Keep personal use reasonable: Although CCP believes that having employees who are active on social networks can be valuable both to the employees themselves and the company, employees should exercise restraint in how much personal use of social media they make during working hours.
- Don't make promises without checking first: Some social networks are very public, so employees should not make any commitments or promises on behalf of the company without checking that the company can deliver on these and that they have the appropriate authority to do so.
- Handle complex queries via other channels: Social networks are not the best place to resolve complicated enquiries or issues. Once a customer has made contact, employees should handle further communications through a more appropriate channel such as email or telephone.



- Do not escalate things: It is easy to get drawn into difficult discussions and post responses that retrospectively, may not have been the most appropriate posts. Employees should always take the time before posting and to hold back from responding if any doubt.

### **Company social media accounts**

This part of the policy covers all social media accounts owned and managed by CCP.

#### Authorised users

Only individuals that have been authorised by the Chief Executive Officer may use CCP's social media accounts. Authorisation is typically granted when the employee has social media related tasks as part of their core job. Allowing only dedicated individuals to use the accounts ensures the company's social media presence is consistent and cohesive.

#### Account safety

Company social media accounts should be protected by strong passwords that are changed regularly and shared only with authorised users.

Wherever possible, employee should use two-factor authentication (often called mobile phone verification) to safeguard company accounts.

Employees must not use a new piece of software, app or service with any of the company's social media accounts without receiving prior approval from the Chief Executive Officer.

#### New accounts

New social media accounts on behalf of the company must not be created without authorisation from the Chief Executive Officer. The company operates its social media presence in line with a strategy that focuses on the most appropriate social networks, given available resources. If an employee feels that the company should have a presence on a platform that CCP does not use, employees should raise this with the Chief Executive Officer in the first instance. All company social media accounts must be linked to a shared mailbox – not a personal email address.

#### Current accounts

CCP's social media accounts may be used for many different purposes. In general, employees should only post updates, messages or otherwise use these accounts when that use is clearly in line with the company's overall objectives. For instance, to:

- Respond to customer enquiries and requests for help
- Share blog posts, articles, and good news stories about the company
- Share insightful articles, media, and other content relevant to the industry that has been created by others
- Provide followers with an insight to the company
- Promote the company, market projects or events/initiatives.

Social media is always changing, and employees are encouraged and supported to think of new ways to use it and put those ideas to the Chief Executive Officer.

Company social media accounts must not be used to share or spread inappropriate content, or to participate in activities that could bring the company into disrepute. When sharing a post, employees should review the content thoroughly and should not post a link based solely on a headline.

## Acceptable use

Below are rules for acceptable use on social media relating to both company accounts and personal accounts:

- Employees may use their personal social media accounts for work-related purposes during regular hours but must ensure this is for a specific reason. Social media should not affect the ability of employees to perform their regular duties
- Use of social media for non-work purposes is restricted to non-work times such as breaks, lunch time etc
- Employees should ensure that their personal social media accounts do not represent CCP's views or opinions. They may wish to include a disclaimer in their profiles/bios such as 'the views expressed are my own and do not reflect the views of my employer'
- Employees must not create or transmit material that might be defamatory or incur liability for the company
- Employees must not post message, status updates or links to material or content that is inappropriate:
  - This includes pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling, and illegal drugs
  - This also covers text, images or other media that could reasonably offend someone based on race, age, sex, religious or political beliefs, natural origin, disability, sexual orientation, or any other characteristic protected by law
- Social media should not be used for illegal or criminal activities
- Employees should not send offensive or harassing materials to other via social media
- Unsolicited views on social, political, religious, or other non-business-related matters should not be broadcast on social media
- No messages or materials that could harm CCP's reputation should be posted or sent via social media
- Employees should not interact with CCP's partners, stakeholders or competitors in any way that could be interpreted as being offensive, disrespectful, or rude
- Social media should not be used to discuss colleagues, customers, stakeholders etc without their prior consent (see CCP's 'data protection policy' for guidance)
- Employees should not post, upload, forward or link to spam, junk email or chain emails and messages.

## Copyright

CCP respects and operates within copyright laws. Employees may not use social media to:

- Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party. If employees wish to share content published on another website, they are free to do so if that website has obvious sharing buttons/functions on it
- Share links to illegal copies of music, films, games, or other software.

## **Security and data protection**

Employees should be aware of the security and data protection issues that can arise from using social networks.

## Maintaining confidentiality

Employees must not:

- Share or link to any content or information owned by the company that could be considered confidential or commercially sensitive such as details of company accounts, future strategy etc
- Share or link to any content or information owned by another company or individual that could be considered confidential or commercially sensitive such as accounts for organisations funded by CCP, client lists for projects etc
- Share or link to data that could in any way breach the company's 'data protection policy'.

## **ICT acceptable use**

Company IT and internet resources – including computers, smart phones, and internet connections – are provided for legitimate business use. CCP therefore reserves the right to monitor how social networks are used and accessed through these resources. Any such examination or monitoring will only be carried out by authorised staff. Additionally, all data relating to social networks written, sent, or received through the company's computer systems is part of official CCP records. The company can be legally compelled to show that information to law enforcement agencies on request.

## **Disciplinary consequences**

Knowingly breaching this social media policy is a serious matter. Employees who do so will be subject to disciplinary action, up to and including termination of employment. They may also be held personally liable for violating this policy. Where appropriate, the company will involve the police or other law enforcement agencies in relation to breaches of this policy.

## GDPR Data Protection Policy (Business)

User group:	All employees
Policy category:	Information and technology
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

This policy sets out Capital City Partnership's (CCP) obligations and responsibilities in the handling, storage and use of all personal data in relation to applicable guidance and legislation which will include:

- the Data Protection Act 2018 (DPA),
- the General Data Protection Regulation ((EU) 2016/679) (GDPR),
- the Electronic Communications Data Protection Directive (2002/58/EC),
- the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) (as amended),
- and all applicable laws and regulations relating to the processing of the personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner or any other national supervisory authority for data protection, and the equivalent of any of the foregoing in any relevant jurisdiction.

### Definitions:

Key words	Definition
Controller	Refers to any person(s) or organisation(s) that exercise overall control over the purposes and means of the processing of an individual's personal data.
Data subject	Any living and identifiable person(s) to whom the personal data relates.
ICO	The Information Commissioner's Office, the UK supervisory authority for data protection.
Personal data	All information concerning a living individual who can be identified (directly or indirectly) from that information.
Processing	Any action that involves the deletion, disclosure, organisation, holding or obtaining of personal data.
Sensitive personal data (sometimes known as 'special categories of personal data')	Personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.
Third party	Any person(s), or organisation(s), other than the data subject or controller.

## Scope

This policy applies to the personal information of individuals with whom CCP engage, including partner organisations and clients.

This policy will also inform any Information Sharing Agreements that will be signed by delivery partners and organisations/projects that receive funding from CCP, both directly, and indirectly where CCP acts as the third-party grant administration and/or management body. When indirectly funded, the recipients may also be subject to the data protection policies of the core funding body and this will be outlined in funding agreements.

The GDPR sets out data protection principles which state that personal data shall:

- be obtained and processed lawfully, fairly and in a transparent manner
- be obtained for specified, explicit and legitimate purposes and not be processed in any manner incompatible with those purposes
- be adequate, relevant, and necessary for the relevant purposes
- be accurate and kept up to date
- not be kept for longer than is necessary for the relevant purposes; and
- be kept safe from unauthorised access, accidental loss, destruction, or damage by appropriate technical and organisational measures.

CCP needs to keep certain information about its partner organisations, clients and other users to allow it to monitor performance, achievements, health and safety, etc. It is also necessary to process personal data to comply with the legal requirements of funding bodies and legislation.

According to Article 6 of the GDPR at least one of the following legal bases must be met to ensure processing personal data is lawful:

- a) Consent: the data subject has given clear consent for you to process their personal data for a specific purpose.
- b) Contract: the processing is necessary for a contract you have with the data subject, or because they have asked you to take specific steps before entering into a contract.
- c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- d) Vital interests: the processing is necessary to protect someone's life.
- e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the data subject's rights and freedoms which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

As CCP is an organisation that will hold personal data on:

- partner organisations delivering services;
- clients receiving support directly - current examples would be FKRSC; and
- clients receiving support delivered as part of a contract which is managed by CCP.

It is likely that legal bases (a) or (b) will be the most applicable. However, CCP will look at the legal bases on a case by case basis and ensure that at least one legal basis applies before collecting and processing personal data.

## Policy elements

### **Notification of data held and processed**

All delivery partners, clients and other users are entitled to know:

- the name and contact details of CCP and our data protection officer;
- what personal data CCP holds and processes about them, and why;
- the purposes of CCP's processing and applicable legal bases;
- who personal data is shared with, including any transfers outside of the UK;
- how to exercise their rights under the GDPR, including how to gain access to this personal data;
- how long CCP keeps their personal data;
- how to lodge a complaint with the UK supervisory authority for data protection – the ICO;
- details of whether they are under a statutory or contractual obligation to provide personal data to CCP; and
- the source of the personal data if not obtained from the data subject.

CCP will issue privacy notices from time to time, which contain the above information. CCP will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

### **Responsibilities of staff**

When, as part of their responsibilities, employees collect information about other people (i.e. service users), they must comply with the guidelines for information handling as set out in Appendix 1.

CCP employees should contact the Chris Nicol (CCP Data Protection Officer) if they are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

- processing of personal data without a legal basis for its processing or, in the case of sensitive personal data, without one of the special conditions set out below being met;
- any personal data breach as set out below;
- access to personal data not without proper authorisation;
- personal data not kept or deleted securely;
- removal of personal data, or devices containing personal data (or which can be used to access it), from CCP's premises without appropriate security measures being in place; and/or
- any other breach of this policy of the data protection principles set out above.

### **Data security**

All employees are responsible for ensuring that:

- any personal data which they hold is kept securely; and
- personal data is not disclosed orally or in writing, accidentally or otherwise, to an unauthorised third party.

Personal data in hard copy should be kept in a locked space such as a filing cabinet, locked drawer, etc. Personal data which is stored online should be in an area that is password protected or on an external drive/disk that is then stored in a locked space. When SharePoint is used for operational purposes colleagues need to balance practical use with the potential risks of breaches. This should

include removal when task is complete, additional encryption if possible and most importantly ensuring only necessary staff have access.

Any employee accessing personal data from outside CCP and provided for a particular task will be required to follow procedures that have been sanctioned by their line manager. Essentially if personal data provided by a third party, e.g. to assist in an audit or a research task, then it should be treated in the same way as internally generated data, but it should also be disposed of securely when the need to hold the personal data has concluded.

### **Personal data breaches**

A personal data breach may take many different forms, e.g.:

- loss or theft of data or equipment on which personal data is stored;
- unauthorised access to or use of personal data either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

CCP will:

- make the required report of a personal data breach to the ICO without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- notify the affected individuals if a personal data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

If any employee becomes aware of any personal data breach, then this will need to be disclosed in the first instance to the Rona Hunter, CEO of CCP who will then inform the necessary authorities. An unauthorised disclosure will be dealt with as a disciplinary matter, and in some cases may be considered an act of gross misconduct.

### **Rights of data subjects**

All delivery partners, clients and other users of CCP have the following rights in relation to their personal data:

- to be informed about how, why and on what basis their personal data is processed as set out above in this policy – see CCP's privacy notice
- to access all personal data that is being kept about them
- to have personal data corrected if it is inaccurate or incomplete
- to have personal data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten')
- to restrict the processing of personal data where the accuracy of the data is contested, or the processing is unlawful (but they do not want the data to be erased), or where CCP no

longer needs the personal data but they require it to establish, exercise or defend a legal claim; and

- to restrict the processing of personal data temporarily where they do not think it is accurate (and CCP is verifying whether it is accurate), or where they have objected to the processing (and CCP is considering whether the organisation's legitimate grounds override their interests).

Any person who wishes to exercise any of the above rights should make a request to the Data Protection Officer, Chris Nicol. CCP aims to comply with requests to exercise data subjects' rights as quickly as possible and will ensure that a response will be provided no later than one month after the request has been received.

If there are exceptional circumstances where the month timescale cannot be met, the requestor will be notified of this within the initial one month period and the reason for the delay in writing. CCP may extend the period for responding by two months where a request is complex, or a number of requests have been received from the data subject.

### **Information supplied to external bodies**

CCP at times may be required to share details with external bodies such as funders, auditors, to demonstrate performance or evidence compliance with funding agreements. In these situations, details contained within an individual customer's record will not be passed to external bodies unless anonymised.

Where CCP uses external organisations to process personal data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. In particular, contracts with external organisations must provide that:

- the organisation may act only on the written instructions of CCP;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent of CCP and under a written contract;
- the organisation will assist CCP in providing access to personal data and allowing individuals to exercise their rights in relation to data protection;
- the organisation will assist CCP in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the organisation will delete or return all personal data to CCP as requested at the end of the contract; and
- the organisation will submit to audits and inspections, provide CCP with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell CCP immediately if it is asked to do something infringing data protection law.

Before any new agreement is entered into involving the processing of personal data by an external organisation, or an existing agreement is altered, the relevant employees must seek approval of its terms by the Data Protection Officer, Chris Nicol.



### **Processing sensitive personal data**

It may be necessary at times to process sensitive personal data about an individual. This may be to ensure that CCP is a safe place for everyone, to operate, other company policies or due to legislative requirements e.g. where employees may engage with children and young people and CCP must give due regard to the duties in the Children (Scotland) Act 1995.

CCP will only process sensitive personal data if:

- we have a legal basis for doing so as set out above, e.g. it is necessary for the performance of the employment contract, to comply with CCP's legal obligations or for the purposes of legitimate interests; and
- one of the special conditions for processing sensitive personal data applies, e.g.:
  - the data subject has given explicit consent
  - the processing is necessary for the purposes of exercising the employment law rights or obligations of CCP or the data subject
  - the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
  - the processing relates to personal data which are manifestly made public by the data subject
  - the processing is necessary for the establishment, exercise, or defence of legal claims; or
  - the processing is necessary for reasons of substantial public interest.

Before processing any sensitive personal data, CCP employees must notify the Data Protection Officer, Chris Nicol of the proposed processing, in order that he may assess whether the processing complies with the criteria noted above.

Sensitive personal data will not be processed until:

- the assessment referred to above has taken place; and
- the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

CCP will not carry out automated decision-making (including profiling) based on any individual's sensitive personal data.

CCP's privacy notice sets out the types of sensitive personal data that CCP processes, what it is used for and the legal basis and special condition for the processing.

In relation to sensitive personal data, CCP will comply with the procedures set out below to make sure that it complies with the data protection principles set out above.

### **Retention of data**

CCP will keep some forms of information longer than others. Due to limitations on data storage facilities, information about an individual will not be kept indefinitely unless there are specific requests to do so.

Contracted Organisations - records held for organisations delivering services on behalf of CCP will be held for a time period that is commensurate with the contract and the funder requirements.

### **Data protection impact assessments (DPIAs)**

Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where CCP is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal data.

Before any new form of technology is introduced, the manager responsible should therefore contact the Data Protection Officer, Chris Nicol, in order that a DPIA can be carried out.

During any DPIA, the manager responsible will seek the advice of the Data Protection Officer and the views of a representative group of employees and any other relevant stakeholders.

### **Documentation and records**

CCP will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve sensitive personal data or criminal records information, including:

- the name and details of CCP, including our data protection officer (and where applicable, of other controllers)
- the purposes of the processing
- a description of the categories of individuals and categories of personal data
- categories of recipients of personal data
- where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- retention periods; and
- where possible, a description of technical and organisational security measures.

As part of CCP's record of processing activities we document, or link to documentation, on:

- information required for privacy notices;
- records of consent;
- controller-processor contracts;
- the location of personal data;
- DPIAs; and
- records of personal data breaches.

If CCP processes sensitive personal data or criminal records information, we will keep written records of:

- the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose
- the legal basis (and special condition, where applicable) for our processing; and
- whether we retain and erase the personal data in accordance with our policy document and, if not, the reasons for not following our policy.

We will conduct regular reviews of the personal data we process and update our documentation accordingly.

## Disciplinary consequences

Compliance with the data protection laws is the individual responsibility of all employees of CCP. Whilst the policy does not form part of the formal contract of employment, it is a condition of employment (paid and voluntary) with CCP that employees will adhere to this policy and its procedures.

Any deliberate breach of this policy may lead to disciplinary action, access to CCP data being withdrawn and/or criminal prosecution.

## *Appendix 1 – Guidelines for information handling*

These guidelines set out how CCP and all its delivery partners, etc. should handle and transport data.

All information held should be classified as follows:

- Unclassified information: information which is not confidential or personal and which may be disseminated freely
- Information Technology and Media Services
- Personal information: information covered by the data protection laws which allows a living individual to be identified or which relates to an identifiable individual
- Sensitive personal data: information covered by the data protection laws which relates to an individual's ethnicity, political membership or opinion, religious beliefs, health, sexual orientation and preferences and criminal convictions or allegations of; or
- Confidential information: information which may or may not be personal and which may not be disclosed except to those with the explicit consent of the data owners and where disclosure without consent may constitute an actionable offence.

Before processing personal data, the following questions should be considered:

- Is it necessary to record the information?
- Is there a legal basis (and special condition, where applicable) to process the data?
- Has authorisation been obtained to collect/store/process the data?
  - If yes, has the information been checked with the data subject for accuracy?
  - If no, is it in the individual's best interests to collect and retain the data?
- Is the information standard or sensitive?
  - If the information is sensitive, has the data subject's express consent been obtained?
- Has the individual been informed that this type of data will be processed and given access to the relevant privacy notice?
- Is the data secure?

Security arrangements appropriate to the classification level must always be in place to ensure the integrity of the information. The retention period of each class of information will be determined by the Data Protection Officer and information should not be kept for longer than necessary for business use.

A full inventory will be held and maintained of all important information assets. Each asset will have a nominated owner, although responsibility for the security measures may be delegated to a nominated individual, accountability remains with the owner. An annual review of information assets will be undertaken.

Any paper documents with a classification of sensitive or above must be shredded. When permanently disposing of equipment containing storage media, all data and software must be irretrievably deleted using an in-house procedure or by another licensed organisation.

### **Keeping information safe**

When looking at information on a screen in an open room/office space, individuals should consider the possibility that this information may be viewed by others nearby and should try to minimise this as much as possible.

When handling confidential paper documents, the individual responsible must take appropriate action to avoid unauthorised disclosure. Procedures must be in place based on the nature of the document such as locking document away when not in use. When printing or copying confidential data, the device or printer must be physically secure or attended.

### **Exchanging information**

Generally, if information is to be shared where individuals can be identified or in the case of organisation's sensitive information being included in the transfer an Information Sharing Agreement (ISA) should be considered. An ISA will ensure that signatories agree to certain protocols and procedures which will alleviate risk of personal data breach:

- Intended third party recipients of classified information or documents must not only be authorised to receive such information, but have ensured they have appropriate information security policies and procedures in place to assure the confidentiality and integrity of the information
- Personal, sensitive or confidential data or information, may only be transferred across networks, or copied to other media, once it has been encrypted and password protected
- Transfer of information should only occur when the confidentiality and integrity of the data can be reasonably assured during the transfer
- All parties are to be notified in advance whenever telephone conversations or videoconference events etc are to be recorded; and
- Email addresses should be checked carefully prior to dispatch, especially where the information contained is sensitive; and where the disclosure of email addresses or other contact information to the recipients is a possibility.

The following measures aim to support individuals to implement these guidelines successfully:

- CCP will establish a continuous 'plan-do-check-act' cycle of activities which ensure that suitable practices are documented, reinforced, and improved with time
- Ensuring that all individuals who use information systems, or handle information in other ways, understand the policies that are relevant to them and the consequences for non-compliance
- Using physical security measures when deemed necessary

- Applying technology where considered appropriate and feasible, e.g. to control and log access to systems, data, and functionality
- Using various lawful forms of monitoring activities, data, and network traffic to detect policy infringements
- Considering relevant information security policy requirements when planning and undertaking activities uninvolving IT-based information systems
- Formal or informal risk assessment, to identify the probability and impact that various hazards could have on information systems
- Monitoring effectiveness of its information security policy implementation – this may involve review independent from those charged with its implementation
- CCP will retain a data security mitigation log which will annually inform reviews of this policy; and
- Individual database managers will consider whether a PIA is required for any data that they are gathering.

## *Appendix 2 - Employee Privacy Notice*

### **Privacy Notice for Employees**

This notice explains what personal data (information) we hold about you, how we collect it, and how we use and may share information about you during your employment and after it ends. We are required to notify you of this information under data protection legislation. Please ensure that you read this notice and any other similar notice we may provide to you from time to time when we collect or process personal information about you.

Data Protection Officer - Chris Nicol [Chris.Nicol@capitalcitypartnership.org](mailto:Chris.Nicol@capitalcitypartnership.org) / 07462432348.

### **Who collects the information?**

Capital City Partnerships is a 'controller' of personal data and gathers and uses certain information about you.

### **About the information we collect and hold**

The table set out in the schedule summarises the information we collect and hold, how and why we do so, how we use it and with whom it may be shared.

We may also need to share some of the categories of personal information set out in the schedule with other parties, such as external contractors and our professional advisers and potential purchasers of some or all of our business or on a re-structuring. Usually, information will be anonymised but this may not always be possible. The recipient of the information will be bound by confidentiality obligations. We may also be required to share some personal information as required to comply with the law.

We seek to ensure that our information collection and processing is always proportionate. We will notify you of any changes to information we collect or to the purposes for which we collect and process it.

### **Where information may be held**

Information may be held at our offices, and third party agencies, service providers, representatives and agents. We have security measures in place to seek to ensure that there is appropriate security

for information we hold [including those measures detailed in our [information security policies and/or guidance], which can be obtained on request by contacting our Data Protection Officer, Chris Nicol, who can be contacted at [Chris.Nicol@capitalcitypartnership.org](mailto:Chris.Nicol@capitalcitypartnership.org) or on 07462432348

### **How long we keep your information**

We keep your information during and after your employment for no longer than is necessary for the purposes for which the personal information is processed. Further details are available in our Employment Data Retention Policy which is in our employee handbook, if you would like to request a copy of this then please contact our Data Protection Officer.

### **Your right to object to us processing your information**

Where our processing of your information is based solely on our legitimate interests (or those of a third party), you have the right to object to that processing if you give us specific reasons why you are objecting, which are based on your particular situation. If you object, we can no longer process your information unless we can demonstrate legitimate grounds for the processing, which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.

Please contact our Data Protection Officer if you wish to object in this way.

### **Your rights**

Please contact our Data Protection Officer if (in accordance with applicable law) you would like to exercise any of your rights under applicable data protection legislation.

Your rights in relation to your information are:

- you have a right to request access to the information that we hold about you by making a "subject access request"
- if you believe that any of your information that we hold about you is inaccurate or incomplete, you have a right to request that we correct or complete your personal information
- you have a right to request that we restrict the processing of your information for specific purposes
- if you wish us to delete the information that we hold about you, you may request that we do so
- you have a right to object to our processing of your information in certain circumstances
- you may request information concerning you held by us, which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit such information to a third party in certain situations; and
- if applicable, you have a right to object to decisions being taken by automated means which produce legal effects concerning you or similarly significantly affect you.

### **Keeping your personal information secure**

We have appropriate security measures in place to prevent personal information from being accidentally lost or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

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

## How to complain

If you have any queries or concerns about this notice or about our use of your personal information, please contact our Data Protection Officer.

If our Data Protection Officer is not able to address your query or concern, you can contact the Information Commissioner at <https://ico.org.uk/concerns/> or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.

## Schedule

### About the information we collect and hold

The information we collect	How we collect the information	Why we collect the information	How we use and may share the information
<b>Your name, contact details (i.e. address, home and mobile phone numbers, email address) and emergency contacts (i.e.name, relationship and home and mobile phone numbers) <input type="checkbox"/></b>	From you	To enter into/perform the employment contract  Legitimate interests: to maintain employment records and good employment practice	To enter into/perform the employment contract
<b>Details of salary and benefits, bank/building society, National Insurance and tax information, your age <input type="checkbox"/></b>	From you	To perform the employment contract including payment of salary and benefits  Legitimate interests: to maintain employment records and comply with legal, regulatory and corporate governance obligations and good employment practice	To ensure you receive the correct pay and benefits  Information is shared with our payroll administrator and HM Revenue & Customs (HMRC)
<b>Details of your spouse/partner and any dependants <input type="checkbox"/></b>	From you	To perform the employment contract including employment-related benefits, for example, private medical insurance, life assurance and pension	To ensure you receive the correct pay and benefits  Information is shared with our payroll administrator and HM Revenue & Customs (HMRC)

The information we collect	How we collect the information	Why we collect the information	How we use and may share the information
<p><b>Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information</b> <input type="checkbox"/></p>	<p>From you and, where necessary, the Home Office</p>	<p>To enter into/perform the employment contract</p> <p>To comply with our legal obligations</p> <p>Legitimate interests: to maintain employment records</p> <p>To carry out obligations and exercise rights in employment law</p> <p>For reasons of substantial public interest (preventing or detecting unlawful acts)</p>	<p>To carry out right to work checks</p> <p>Information is shared with HR personnel and may be shared with the Home Office</p>
<p><b>Details of your pension arrangements, and all information included in these and necessary to implement and administer them</b> <input type="checkbox"/></p>	<p>From you, from our pension administrators and (where necessary) from your own pension fund administrators</p>	<p>To perform the employment contract including employment-related benefits</p> <p>To comply with our legal obligations</p> <p>Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice</p>	<p>To administer your pension benefits and/or to comply with our auto-enrolment pension obligations</p> <p>Information is shared with our pension administrators and with HMRC</p>
<p><b>Information in your sickness and absence records (including sensitive personal information regarding your physical and/or mental health)</b> <input type="checkbox"/></p>	<p>From you, from your doctors, from medical and occupational health professionals we engage</p>	<p>To perform the employment contract including employment-related benefits</p> <p>To comply with our legal obligations</p> <p>Legitimate interests: to maintain employment records; comply with legal, regulatory and corporate governance obligations and good employment practice; and ensure safe working practices</p> <p>To carry out and exercise obligations and rights in employment and social security law, such as to assess your working capacity as an employee</p>	<p>To maintain employment records, to administer sick pay entitlement, to follow our policies and to facilitate employment-related health and sickness benefits</p> <p>To comply with our legal obligations to you as your employer</p>



The information we collect	How we collect the information	Why we collect the information	How we use and may share the information
			<p>Information is shared with your doctors, with medical and occupational health professionals we engage</p> <p>For further information, see * below</p>
<b>Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs</b>	From you	To comply with our legal obligations and for reasons of substantial public interest	<p>To comply with our equal opportunities monitoring obligations and to follow our policies</p> <p>For further information, see * below</p>
<b>Information on grievances raised by or involving you</b>	From you, from other employees and from consultants we may engage in relation to the grievance procedure	<p>To perform the employment contract</p> <p>To comply with our legal obligations</p> <p>Legitimate interests: to maintain employment records; comply with legal, regulatory and corporate governance obligations and good employment practice; and to carry out obligations under employment law</p> <p>To establish, exercise or defend legal claims</p>	For staff administration, to follow our policies and to deal with grievance matters Information shared with relevant managers, HR personnel and with consultants and advisers we may engage
<b>Information on conduct issues involving you</b>	From you, from other employees and from consultants we may engage in relation to the conduct procedure	<p>To comply with our legal obligations</p> <p>Legitimate interests: to maintain employment records; comply with legal, regulatory and corporate governance obligations and good employment practice; and ensure safe working practices</p>	For staff administration and assessments, to follow our policies, to monitor staff performance and conduct and

The information we collect	How we collect the information	Why we collect the information	How we use and may share the information
			<p>to deal with disciplinary and grievance matters</p> <p>Information is shared with relevant managers, HR personnel and with consultants and advisers we may engage</p>
<p><b>Details of your appraisals and performance reviews</b></p>	<p>From you, from other employees</p>	<p>To comply with our legal obligations</p> <p>Legitimate interests: to maintain employment records; comply with legal, regulatory and corporate governance obligations and good employment practice; and ensure safe working practices</p>	<p>For staff administration and assessments, to follow our policies, to monitor staff performance and conduct and to deal with disciplinary and grievance matters</p> <p>Information is shared with relevant managers, and HR personnel, and with consultants and advisers we may engage</p>
<p><b>Details of your performance management/improvement plans (if any)</b></p>	<p>From you, from other employees</p>	<p>To comply with our legal obligations</p> <p>Legitimate interests: to maintain employment records; comply with legal, regulatory and corporate governance obligations and good employment practice; and ensure safe working practices</p>	<p>For staff administration and assessments, to follow our policies and to monitor staff performance</p> <p>Information is shared with</p>

The information we collect	How we collect the information	Why we collect the information	How we use and may share the information
			relevant managers, and HR personnel, and with consultants and advisers we may engage
<b>Details of your time and attendance records</b>	From you	<p>To perform the employment contract</p> <p>Legitimate interests: to monitor and manage staff access to our systems and facilities; record staff absences; and to carry out obligations under employment law</p>	<p>For payroll and staff administration and assessments, to follow our policies and to monitor staff performance and attendance</p> <p>Information is shared with relevant managers, HR personnel, our payroll administrator, and with consultants and advisers we may engage and with</p>
<b>Information in applications you make for other positions within our organisation</b>	From you	<p>To enter into/perform the employment contract</p> <p>To comply with our legal obligations</p> <p>Legitimate interests: to maintain employment records and comply with legal, regulatory and corporate governance obligations and good employment practice</p>	<p>To process the application</p> <p>Information is shared with relevant managers, HR personnel and with consultants and advisers we may engage</p>
<b>Information about your use of our IT, communication and other systems</b>	Automated monitoring of our websites and other technical systems, such as our computer networks and	Legitimate interests: to protect our networks, and personal data of employees and customers/clients, against unauthorised access or data leakage; ensure our business policies, such as those concerning security and internet use, are	To protect and carry out our legitimate interests (see adjacent column) Information shared with

The information we collect	How we collect the information	Why we collect the information	How we use and may share the information
	connections and our computer devices	adhered to; for operational reasons, such as quality control to ensure that commercially sensitive information is kept confidential; for security vetting and investigating complaints and allegations of criminal offences; and to prevent unauthorised access and modifications to our systems as part of investigations by regulatory bodies, or in connection with legal proceedings or requests	relevant managers, HR personnel, and with consultants we may engage  For further information, see ** below
<b>Your image, in photographic form</b>	From you	Legitimate interests: to monitor and manage staff access to our premises, systems and facilities	To protect and carry out our legitimate interests (see adjacent column) Information shared with other staff members and the directors
<b>Details of your use of business-related social media, such as LinkedIn</b>	From relevant websites and applications	Legitimate interests: to monitor and manage staff access to our systems and facilities; protect our networks, and personal data of employees and customers/clients, against unauthorised access or data leakage; ensure our business policies, such as those concerning security and internet use, are adhered to; for operational reasons, such as maintaining employment records, recording transactions, training and quality control  to ensure that commercially sensitive information is kept confidential; to check that restrictions on your activities that apply after your employment has ended (post-termination restrictions or restrictive covenants) are being complied with; and for security vetting and	To protect and carry out our legitimate interests (see adjacent column)  Information is shared with relevant managers and with consultants we may engage  For further information, see ** below

The information we collect	How we collect the information	Why we collect the information	How we use and may share the information
		investigating complaints and allegations of criminal offences as part of investigations by regulatory bodies, or in connection with legal proceedings or requests	
<p><b>Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within our organisation; you will be notified separately if this is to occur)</b></p>	From relevant websites and applications	<p>Legitimate interests: to monitor and manage staff access to our systems and facilities; protect our networks, and personal data of employees and customers/clients, against unauthorised access or data leakage; ensure our business policies, such as those concerning security and internet use, are adhered to; for operational reasons, such as maintaining employment records, recording transactions, training and quality control</p> <p>to ensure that commercially sensitive information is kept confidential; to check that restrictions on your activities that apply after your employment has ended (post-termination restrictions or restrictive covenants) are being complied with; and for security vetting and investigating complaints and allegations of criminal offences as part of investigations by regulatory bodies, or in connection with legal proceedings or requests</p>	<p>To protect and carry out our legitimate interests (see adjacent column)</p> <p>Information is shared with relevant managers HR personnel and with consultants we may engage</p> <p>For further information, see ** below</p>
<p><b>Details in references about you that we give to others</b></p>	From your personnel records, our other employees	<p>To perform the employment contract</p> <p>To comply with our legal obligations</p> <p>Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice</p>	<p>To provide you with the relevant reference</p> <p>To comply with legal/regulatory obligations</p> <p>Information shared with relevant managers and the recipient(s) of the reference</p>

You are required (by law or under the terms of your contract of employment, or in order to enter into your contract of employment) to provide the categories of information marked "☐" above to us to enable us to verify your right to work and suitability for the position, pay you, provide you with your contractual benefits, such as contractual sick pay, and administer statutory payments, such as statutory sick pay (SSP). If you do not provide this information, we may not be able to employ you, to make these payments or provide these benefits.

\* Further details on how we handle sensitive personal information are set out in our GDPR Data Protection Policy (Employment) contained within the Employee Handbook.

\*\* Further information on the monitoring we undertake in the workplace and how we do this is available in our internet, email, and social media policy contained within the Employee Handbook.

## Cyber Security Policy

User group:	All employees
Policy category:	Information and technology
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

Capital City Partnership's (CCP) cyber security policy outlines the guidelines and provisions for preserving the security of its data and technology infrastructure.

### Scope

This policy applies to all paid employees of CCP, volunteers and those under our care on work experience, internships or other activity that requires supervision in our workplace.

### Policy elements

Confidential data is secret and valuable e.g. unpublished financial information, customer/partner/vendor data, patents, formulas or new technologies etc. All employees are obliged to protect this data. This policy gives guidance on how to mitigate security risks to avoid security breaches.

#### **Digital devices**

When employees use digital devices to access company emails or accounts, they introduce security risks to the data. All employees are advised to keep their devices secure by:

- Keeping all company and personal devices password protected
- Using and upgrading antivirus and anti-malware software (see Appendix 1)
- Ensuring that they do not leave their devices exposed or unattended e.g. turning off screens and locking devices when leaving their desks
- Installing security updates of browsers/systems at regular intervals and/or as soon as updates are available
- Logging into company accounts and systems through secure and private networks only i.e. not using public wi-fi networks that are unsecure
- Not accessing internal systems/accounts from other people's devices e.g. individuals outside of the organisation; or lending their own devices to others where they may be able to view the browsing history and/or access company systems
- Reporting stolen or damaged equipment as soon as possible to their direct line manager
- Refraining from downloading suspicious, unauthorised, or illegal software to their company devices
- No software should be installed on company devices without approval
- Only using company devices for business use only,

## **Emails**

Emails often host scams and malicious software e.g. worms. To avoid virus infection or data theft, employees are advised to:

- Avoid opening attachments and clicking on links where the content is not adequately explained
- Be suspicious of clickbait titles – where subject lines offer prizes, advice etc
- Check email addresses and names of senders to ensure that they are legitimate
- Look out for inconsistencies or warning signs in emails such as grammar and spelling mistakes, capital letters, excessive use of exclamation marks.

If an employee is unsure if an email is safe, they should not open or forward it on to others and should report it to the IT specialist – Lee Hair (email support@leehair.co.uk, telephone 0131 516 4760). All scams, breaches and malware should be reported as soon as possible and will be investigated by the IT specialists.

## **Passwords**

Passwords should be secure and secret. Employees are advised to:

- Choose passwords with at least eight characters (using a mix of capital and lower-case letters, numbers and symbols) and avoid using combinations that can be easily guessed i.e. birthdays
- Remember passwords instead of writing them down. If passwords are written down, then employees must keep the paper or digital note confidential and destroy it when it is no longer required
- Exchange credentials only when necessary and in person. If it is not possible to exchange in person then the phone should be used instead of email and only if the employee is confident that the person that they are speaking to is who they say that they are
- Change passwords every two months or immediately when a device is stolen.

## **Management of data**

Employees should:

- Only store personal data when authorisation has been given to do so
- Only store personal data on the server shares
- Report any data breaches
- Only store data on laptops where encryption is in place
- Never store personal data on USB sticks or disks unless these are encrypted

Transferring data introduces security risks. Employees must:

- Avoid transferring sensitive data e.g. customer information, employee records) to other devices or account unless necessary. When there requires to be a mass transfer of data, employees should seek advice from the IT specialist before doing so
- Ensure that confidential data is only shared over the company network/system and not using public Wi-Fi networks or private connections
- Never send personal data by email or in the post unless encrypted
- Ensure that the recipients of the data are authorised to receive the data and have adequate security processes in place.



CCP has a Data Protection Policy that should be referred to when managing data.

### **Remote working**

Employees working remotely must adhere to this policy. Remote working requires employees to access the company's systems from a distance, so the employee has a duty to ensure that they follow process for data encryption, keeping data safe and secure at their remote location and only use a network that is secure. If an employee is concerned about the possible risks and how to mitigate these, they can seek advice from the IT specialists.

### **Disciplinary consequences**

All employees are expected to follow this policy. Any employee that causes a security breach may face disciplinary action as follows:

First time, unintentional, small-scale security breach: Employees may be issued with a verbal warning and receive cyber security training

Intentional, repeated, large-scale breaches (where financial or other damage is incurred): More severe disciplinary action which may result in termination. Each case will be examined on an individual basis.

Employees who are observed to disregard this policy and its processes/instructions may still face disciplinary action, even if their behaviour has not resulted in a security breach.

### *Appendix 1 – Anti-virus and anti-malware guidance*

CCP systems should only be accessed from approved CCP devices which have anti-malware software installed and activated with up to date anti-virus/malware definition files. All CCP devices have ESET Endpoint Antivirus software installed.

Every computer must have the appropriate operating system update service activated, and available operating system and application updates installed.

If a computer is infected with any type of malware it should be disconnected from any CCP network and not re-connected until it has been certified malware free by the IT specialist.

## Equality and Diversity Policy

User group:	All employees
Policy category:	HR
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

This policy reinforces Capital City Partnership's (CCP) commitment to providing equality and fairness to all in our employment and not provide less favourable facilities or treatment on the grounds of age, disability, gender reassignment, marriage and civil partnership, pregnancy or maternity, race, ethnic origin, colour, nationality, national origin, religion or belief, or sex or sexual orientation. CCP are opposed to all forms of unlawful and unfair discrimination in line with the Equality Act (2010).

CCP is a living wage and disability confident employer.

### Scope

This policy applies to all paid employees of CCP, volunteers and those under our care on work experience, internships or other activity that requires supervision in our workplace.

This policy applies to all individual who apply for a vacancy at CCP. Employee recruitment and selection processes involving selecting candidate for employment, training, promotion etc based on their aptitude and ability.

### Policy elements

CCP is dedicated to encouraging a supportive and inclusive culture amongst its workforce, promoting diversity and eliminating discrimination in the workplace. The company's aim is to ensure that all employees and applicants are given equal opportunity and that the organisation is representative of all sections of society. Each employee will be respected and valued and able to give their best as a result of being treated fairly.

All employees will be treated fairly and equally in the workplace, irrespective of their:

- Sex
- Gender Identity/Gender transition
- Marital/Civil Partnership Status
- Race/Ethnicity
- Disability
- Age
- Religion or Belief
- Sexual Orientation
- Pregnancy/Maternity status.

Employees should never assume any of the above regarding colleagues.

CCP will:

- Help and encourage all employees to develop to their full potential and utilise their unique talents
- Create an environment in which individual differences and the contributions of all team members are recognised and valued
- Foster a working environment that promotes dignity and respect for all employees
- Not tolerate any form of intimidation, bullying or harassment, and will discipline those that breach this policy
- Make training, development and progression opportunities available to all employees
- Actively promote equality in the workplace
- Support anyone who feels that they have been subject to discrimination to raise their concerns, so CCP can apply corrective measures
- Regularly review all its employment practices and procedures so that fairness is maintained always.

CCP does not tolerate:

- Direct discrimination/ Indirect discrimination: uniformly enforced rule or law that disproportionately adversely affects those with protected characteristic
- Associative discrimination: due to association with someone with a protected characteristic
- Perceptive discrimination: directed because it is believed someone has a protected characteristic
- Harassment: unwanted conduct relating to protected characteristic regardless of direction of behaviour and possession of characteristic.
- Third Party Harassment: not part of organization but discrimination should have been controlled by organization.
- Victimisation: mistreatment due to making or supporting complaint under this act.

Good practice tips for inclusivity:

- Mind your language – use inclusive language
- Do not assume gender identity/sexual orientation/race/disability/religion
- Ask people what pronouns they prefer
- Respect all self-identification
- Not a debate - No-one's identity is up for discussion
- Do not erase diverse identities – e.g. do not use 'gay' when you mean LGBT+
- Avoid intrusive and/or inappropriate questions
- Learn.

### Disciplinary consequences

All employees must comply with the policy and anyone who does not may be subject to disciplinary consequences and in some cases, legal prosecution, and termination.

## Health and Safety Policy

User group:	All employees / All visitors
Policy category:	Health and Safety
Last modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

This policy outlines Capital City Partnership's (CCP) approach to Health and Safety including the CCP Health and Safety Policy Statement, management approach and accident reporting procedure.

### Scope

This policy applies to all paid employees of CCP, volunteers and those under our care on work experience, internships or other activity that requires supervision in our workplace.

All visitors (such as but not limited to stakeholders, partners and independent contractors) are expected to comply with the Health and Safety Policy when on the premises and this policy should be read in conjunction with CCP's Workplace Visitor Policy.

### Policy elements

#### Policy statement

CCP's [Health and Safety Policy statement](#) has the following commitments:

- To provide adequate control of the health and safety risks arising from our work activities
- To consult with our employees on matters affecting their health and safety
- To provide and maintain safe equipment
- To ensure safe handling and use of substances
- To provide information, instruction, and supervision for employees
- To ensure all employees are competent to do their tasks, and to give them adequate training
- To prevent accidents and cases of work-related ill health
- To maintain safe and health working conditions; and
- To review and revise this policy as necessary at regular intervals.

#### Monitoring the policy statement

An [action plan](#) supporting the policy statement is monitored by the CCP Management Team with overall responsibility held by the Chief Executive Officer. This is also reviewed annually in line with the policy statement annual review.

#### Accidents

Whilst CCP has procedures in place to promote a safe working environment, it is acknowledged that not all accidents are preventable and can still occur. In these cases, all work-related accidents must be reported as soon as practically possible to allow for the circumstances to be fully investigated and where appropriate, preventative measures to be implemented.

Work related accidents include all accidents that may cause minor or severe injuries, or incidents that are as a result of negligence or inadequate safety precautions. The victims of these accidents may be employees or people that were on company premises or vehicles.

## Procedure

### Reporting an accident

CCP encourages employees to report all accidents no matter how minor. Accidents that involve very minor injuries such as small cuts, non-extensive bruises etc. and would not normally require any action on behalf of the company (e.g. the breaking of a drinking glass) do not have to be reported (although employees could report them if they want). Accidents that involve (or could have involved) more severe injuries and require investigation and action from CCP must be dutifully reported in accordance with RIDDOR - [Reporting of Injuries, Diseases & Dangerous Occurrences RIDDOR \(hse.gov.uk\)](https://www.hse.gov.uk/riddor/).

Employees are obliged to report:

- Fatalities
- Damage to the head, skull, and face
- Damage to any of the senses (e.g. partial or complete loss of hearing, sight)
- Incapacitation or dislocation of limbs that hinder functionality or movement (including paralysis and amputation)
- Damage to the skin (e.g. extensive burns, bruises, or cuts)
- Blows or injuries to the spine, back and ribs
- Harm to the nervous system or loss of consciousness through electrocution, hypothermia etc.
- Poisoning
- Contamination from hazardous substances or transmission of diseases
- Any other injury that requires hospitalisation or medical care.

If an employee needs medical coverage, the accident must be reported immediately as insurance claims may have to be approved after an investigation has taken place.

Employees are also required to report occurrences that may not have resulted in injuries but could be potentially dangerous if they happened again. These include but are not limited to:

- Explosions
- Slippery surfaces
- Water or gas leaks
- Inadequate insulation of circuits
- Collapse of walls, ceilings, other structures
- Breaking of window glass or frame.

When an employee witnesses or is involved in an accident they must report it to their line manager using the accident book. If the accident occurred remotely then it must be reported by telephone or email in the first instance, and then recorded within one week of the occurrence.

If the employee believes that that the accident has occurred (or has the potential to occur) due to negligence or inadequate safety (either by CCP or another employee) this must be reported to their line manager as soon as possible.

### Disciplinary consequences

All employees are obliged to comply with this policy. Any employee that is discovered to have been aware of a serious accident (or potential serious hazard which results in an accident) and failed to report this will face disciplinary consequences. If an employee is the cause of an accident, they must report this immediately to minimise the disciplinary consequences.

## Anti-bribery and corruption Policy

User group:	All employees
Policy category:	HR
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

This policy supports CCP's ethos of honesty, transparency and fairness and protects the reputation of the company.

### Scope

This policy is for all employees of CCP, volunteers and other individuals who may engage in work for CCP and / or who have access to CCP office, equipment and projects, regardless of physical location.

### Policy elements

#### Introduction

Bribery and corruption remain a major issue in world trade, despite the many dedicated efforts to prevent them. Our legal obligations are primarily governed by the Bribery Act 2010. That Act affects us, as a UK company, if bribery occurs anywhere in our business.

Involvement in bribery and corruption exposes the Company and relevant individuals to a criminal offence. It will also damage our reputation and the confidence of our funders and partners.

The Company's position is simple: the Company conducts its business to the highest legal and ethical standards. The Company will not be party to corruption or bribery in any form. Such acts would damage the Company's reputation and expose the Company, and its employees and representatives, to the risk of fines and imprisonment.

We run our business with integrity and in an honest and ethical manner. All of us must work together to ensure that CCP remains untainted by bribery or corruption.

This policy sets out the steps all of us must take to prevent bribery and corruption at CCP in order to comply with relevant legislation. It does not form part of any employee's contract of employment and we may amend it at any time.

#### What are bribery and corruption?

A 'bribe' is a financial or other advantage offered, promised, requested or given to induce a person to perform a relevant function or activity improperly, or to reward them for doing so. In this context, a 'financial or other advantage' is likely to include cash or cash equivalent, gifts, hospitality and entertainment, services, loans, preferential treatment in a tendering process, discounts etc. Whether or not an individual receives benefit from a bribe is irrelevant as is the timing of a bribe, therefore payment/inducement made before, during or after an event will constitute a bribe.

- 'Bribery' includes offering, promising, giving, accepting or seeking a bribe.
- 'Corruption' is the misuse of office or power for private gain.

All forms of bribery and corruption are strictly prohibited. If you are unsure about whether a particular instance constitutes bribery, you should raise it with the Chief Executive Officer.

This means that you must not:

- give or offer any payment, gift, hospitality, or other benefit in the expectation that a business advantage will be received, or to reward any business received
- accept any offer from a third party that you know or suspect is made with the expectation that a business advantage will be offered for them or anyone else [and/or]
- give or offer any payment (sometimes known as a 'facilitation payment') to a government official to facilitate or speed up a routine or necessary procedure
- provide or conceal information which would compromise the transparency and equity of a tendering process and which would result in a material advantage being gained by one entity over other entities involved in the process.

No person must threaten or retaliate against another person who has refused to offer or accept a bribe or who has raised concerns about possible bribery or corruption.

### **Who can be involved in bribery and in what circumstances?**

Bribery and corruption could be committed by anyone working for us or on behalf in any capacity, such as our employees, officers or directors, anyone they authorise to do things on their behalf, our representatives and other third parties who act on our behalf, our suppliers and even our customers.

The provisions of this policy therefore apply to all those listed in paragraph 0 above.

Bribery can occur in both the public and private sectors.

### **The legal position on bribery and corruption**

Bribery and corruption are criminal offences in most countries and in the UK, we are bound by the Bribery Act 2010.

### **Who is responsible for this policy?**

We are all responsible for adhering to the policy and the Chief Executive Officer has overall responsibility for monitoring the policy in collaboration with the senior management team.

### **Gifts and hospitality**

You should not solicit any gift or hospitality in the course of your work for CCP.

You should not offer or receive from any person or organisation who has had, has or may have any influence over our business any gift or hospitality which is unduly lavish or extravagant or otherwise inappropriate, or which could be seen as an inducement or reward for any preferential treatment.

We regard the following to be inappropriate (the list is not exhaustive):

- a personal or corporate gift to a value in excess of £100
- hospitality to a value in excess of £100
- any gift that includes cash or a cash equivalent (such as vouchers)
- any gift or hospitality given or received in secret; and
- any gift or hospitality given or received in your name rather than in the name of CCP.

### **Records**

It is essential that we keep full and accurate records of all our financial dealings. Transparency is vital; false or misleading records could be very damaging to us. Under money laundering regulations our lawyers and accountants are obliged to report anything which appears to be irregular.



You must therefore declare and properly record (in writing) all hospitality and gifts given or received. You must also submit all expenses claims relating to hospitality, gifts or payments to third parties in accordance with our prevailing expenses claims process and properly record the reason for the expenditure.

### **Monitoring**

The senior management team will monitor the policy regularly to make sure it is being adhered to.

### **What to do if you think something is wrong**

Each of us has a responsibility to speak out if we discover anything corrupt or otherwise improper occurring in relation to the business. If you are offered a bribe, or are asked to make one, or if you discover or suspect that any bribery or corruption has occurred or may occur, you must notify the Chief Executive Officer OR report in accordance with the procedure set out in our Whistleblowing Policy as soon as possible. You can do this anonymously. You must make your report as soon as reasonably practicable.

### **Compliance with this policy**

The Company takes compliance with this policy very seriously. Failure to comply puts both individuals and the Company at risk.

Because of the importance of this policy, failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. Any non-employee who breaches this policy is liable to have their contract terminated with immediate effect.

## Recruitment and Selection Policy

User group:	Management and HR staff
Policy category:	HR
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

This policy ensures that the recruitment and selection process at Capital City Partnership (CCP) is transparent and unbiased and results in the appointment of the best candidate, based solely on merit. It outlines the procedure for recruiting, to ensure consistency across all recruiting managers.

The recruitment process must be:

- A fair process
- In line with our equality and diversity policy
- Consistent for each vacancy advertised.

### Scope

This policy applies to recruiting managers within CCP and HR staff.

### Policy elements

Hiring managers must use pre-determined criteria at all stages of the recruitment process, thereby reducing the risk of bias or discrimination.

Different types of bias include (this list is not exhaustive):

- **Affinity bias** - when you unconsciously prefer people who share qualities with you or someone you like.
- **Ageism** - stereotyping of and discrimination against individuals or groups on the basis of age.
- **Attribution bias** - how you perceive your actions and those of others.
- **Beauty bias** - based on physical attractiveness.
- **Confirmation bias** - how people primarily search for bits of evidence that back up opinions, rather than looking at the whole picture.
- **Conformity bias** - when your views are swayed too much by those of other people.
- **Gender bias** - preference for one gender over the other.
- **Halo effect** - when we focus on one particularly great feature about a person.
- **Horns effect** - the opposite of the halo effect: you focus on one particularly negative feature about a person, which clouds your view of their other qualities.
- **Racial bias** - harmful aversion to, stereotyping of, or discrimination against a race.
- **The contrast effect** - when you assess two or more similar things and compare them with one another, rather than looking at each based on their own merits.

To reduce unconscious bias in the recruitment process, the following steps must be taken:

- Be mindful of language in job adverts.
- Anonymous candidates during shortlisting (this is done by HR).
- Standardise the interview process by using competency based questions and a standardised marking method.

- Watch out for bias toward likeability (halo effect).
- Have more than one person present at interviews.
- Think about diversity/inclusivity goals.

### **Job Descriptions/Person Specifications**

Job descriptions and person specifications must be written with precedence to the competencies that would make the most positive contribution to the organisation’s business requirements (i.e. flexibility, initiative, leadership etc.) and not with a specific candidate in mind. Key selection criteria must be determined before a job is advertised and clearly noted in the job description.

### **Shortlisting**

Applicants are evaluated according to the predetermined selection criteria only. Recruiting managers will not have access to any personal information (name, address, ethnicity, disability information etc.) at this stage.

### **Interviewing**

When interviewing candidates, the same interviewers should be present at each interview and a set of pre-determined questions asked of each candidate, allowing them equal time to respond. If a candidate is at a disadvantage for any reason (i.e. has a disability), reasonable adjustments must be considered.

### **Reference checks**

Reference checks will only be carried out once a candidate has accepted the post (subject to satisfactory checks). Reference checks should be conducted before an official offer letter is sent out and should be carried out in a consistent manner, using the CCP reference request template.

### **Legality**

Privacy and equal opportunity legislation require that the recruitment process is conducted in a fair and transparent manner.

During no stage of the recruitment process (from advertisement to interview) can there be any discriminatory behaviour (intentional or unintentional), based on a person’s age, sex, marital status, religion, nationality, sexual orientation, or disability\*. A candidate may have recourse to legal action if they feel they have been discriminated against, so impartiality is not only the right thing to do, but also good risk management practice.

All applications must be kept confidential and unsuccessful applications destroyed within three months of recruitment being finalised.

### **Procedure**

Once a new position has been identified and agreed with the Chief Executive, the recruitment process can begin:

<b>Staff member</b>	<b>Action</b>	<b>Details</b>
Recruiting manager	Job application pack and application form created.	The <a href="#">Job application pack</a> must include organisation information, job description, person specification and employee benefits. The <a href="#">CCP application form</a> must be used.
CEO/DCEO	Job application pack to be approved. Once approved sent to HR staff to advertise.	

HR	Final proof of documents then post vacancy on job advertising sites.	Job advertising sites include: MyJobScotland, GoodMoves, S1Jobs and Joined Up for Jobs.
HR	Manage applications.	Create a folder for applications in the secure HR folder. Save full and redacted copies of applications. Respond to applicants confirming receipt of email.
HR	Send redacted applications for shortlisting.	Once applications have closed, send redacted applications to the recruiting manager.
Recruiting manager	Shortlist applications.	Use the <a href="#">essential criteria checklist</a> to assist with shortlisting applicants. Any applicants who have recorded they have a disability and meet the essential criteria will automatically be given an interview. Once applicants have been selected for interview, inform HR staff to invite them to interview.
HR	Email interviewees with interview information and time slots.	Send interview invites out and record responses for attendance. Notify recruiting manager of responses.
HR	Email unsuccessful candidates.	Email unsuccessful candidates to let them know their application will not be progressed.
Recruiting manager + any other interviewer(s)	Prepare for interview.	Prepare interview questions and <a href="#">marking rubric</a> .
HR	Provide recruiting managers with full applications.	Send full application forms for those attending interviews to the recruiting manager.
Recruiting manager + any other interviewer(s)	Interviews take place	Interviews and scoring take place using the pre-prepared interview questions and marking rubric.
Recruiting manager	Outcome of interviews communicated.	Inform interviewees of the outcome of their interview and provide any requested feedback.
HR	Reference checks	Request references from referees of preferred candidate(s).
HR	Send offer letter *subject to references*	Offer letter is prepared and sent to the candidate for signing.
HR	Send new start templates to be completed.	Once new start templates have been received, pass on to Finance.

Failure to comply could lead to disciplinary action.

*\*This list is not exhaustive. Discrimination of any kind is prohibited.*

## Notice Periods

User group:	All Employees
Policy category:	HR
Last reviewed or modified:	March 2022
Review date:	March 2024

### Policy brief and purpose

This policy outlines notice periods for both employees ending their employment, and CCP giving notice to employees.

### Scope

This policy applies to all employees of CCP.

### Policy elements

Capital City Partnership's notice period is as follows:

#### Employees giving notice

Length of service	Notice you must give
Under 1 month	2 weeks
1 month to 2 years	4 weeks
Over 2 years	Up to 8 weeks (if required)
CEO and Deputy CEO	3 months

#### CCP giving notice

Length of service	Notice you must give
1 month to 2 years	At least a week
2 years to 12 years	A week's notice for every year employed
12 or more years	12 weeks