Data Protection Management Framework Policy

1. Introduction

A privacy compliance framework provides a structure for managing personal data in a confidential and secure manner compliant with current data protection legislation. It provides a consistent way for employees to deal with the many different information handling requirements including:

- Data Protection Management
- Confidentiality and personal data protection assurance
- Corporate Information assurance
- Information Security assurance
- Secondary use assurance
- Respecting data subjects' rights regarding the processing of their personal data.

This framework outlines how the data protection agenda will be addressed by Connected Places Catapult and its Group[1] (referred from here on within this document as CPC).

The framework is based upon the legal requirements of the Data Protection Act 2018, the UK General Data Protection Regulation, and the Human Rights Act 1998.

2. Purpose

To outline the strategic framework for managing and supporting the data protection agenda for CPC. The framework provides a solid basis upon which data protection and all its component parts will be implemented throughout CPC.

To describe the roles and responsibilities of those with formal oversight responsibilities for data protection within CPC.

To ensure that data protection is appropriately supported and resourced within CPC, and to describe the data protection responsibilities of all staff.

CPC will ensure:

- Regulatory and legislative requirements will be met
- Confidentiality of information will be assured
- Information will be protected against unauthorised access
- Quality and Integrity of information will be maintained
- Business Continuity Plans will be produced, maintained, and tested
- Data Protection training will be available for all staff
- All data protection breaches, actual or suspected, will be reported to, and investigated by the Risk & Compliance Manager in conjunction with the Data Protection Manager
- Retention and destruction of data in line with national legislation

[1] As at the date of this framework, the Connected Places Catapult group of companies comprises 6 companies being:
Connected Places Catapult (company number 11837978); Connected Places Catapult Services Limited (company number 11839397); Transport Systems Catapult (company number 08041919); Transport Systems Catapult Services Limited (company number 08517330); Future Cities Catapult (company number 08041915); Future Cities Catapult Services Limited (company number 08517376)

To inform staff to maximise the organisational information assets by ensuring that CPC can demonstrate personal data is:

- Held securely and confidentiality
- Processed fairly and lawfully
- Obtained for specific purpose(s)
- Recorded accurately and reliably
- Used effectively and ethically
- Shared and disclosed appropriately and lawfully
- Retained and destroyed lawfully

3. Scope

This framework applies to:

- **All staff** - This includes all individuals employed by CPC and those working for CPC in a temporary capacity, including but not limited to agency staff, seconded staff, students and trainees, and any self-employed consultants or individuals working for CPC under contracts for services, individuals appointed to CPC's governing bodies and their committees and any other individual directly involved with the business or decision-making of CPC.
- **Systems** – CPC systems will include, but are not limited to, discrete systems such as those holding information relating to personal data, finance, risk, complaints, incidents, human resources and payroll; less technical systems such as Excel spreadsheets held on the IT network, and paper based systems such as human resource files.
- **Information** – All information processed (electronic and paper based) in relation to any CPC activity whether by employees or other individuals or organisations under a contractual relationship with CPC. All such information belongs to CPC unless proven otherwise.

4. Policies

CPC will establish and maintain policies to ensure that compliance with all relevant legal and regulatory frameworks is achieved, monitored, and maintained.

The following table sets out the CPC policies supporting this framework:

Policies	Description
Confidentiality and Data Protection Policy	This policy sets out the roles and responsibilities for compliance with the Data Protection Act and lays down the principles that must be observed by all who work within CPC and have access to personal or confidential business information.
Information Security Policy	This policy is to protect, to a consistently high standard, all information assets. This policy defines security measures applied through technology and encompass the expected behaviours of those who manage information within the organisation
Records Management Policy	This policy is to promote the effective management and use of information, recognising its value and importance as a resource for the delivery of corporate and service objectives
Data Breach Policy	This policy sets out the roles, responsibilities, and process to be followed when reporting and investigating a data breach.

Individuals Rights Policy	This policy is to promote individuals rights under the GDPR. This policy details each of the individual rights detailed with the GDPR, and the internal process, templates which are to be used when receiving a request.
Data Protection Impact Assessment Policy	This policy to ensure privacy by design is implemented within all projects. This policy defines the process to be applied, including management of information risks within the project.
Subject Access Request Policy	This policy promotes the individual right under the GDPR. This policy details the individuals right and within the GDPR, and the internal process and templates which are to be followed when processing a request.

5. Roles and Responsibilities

Overview

Senior level ownership and understanding of information risk management is vital and ensures a clear link to the overall risk management culture within the organisation. Senior leadership demonstrates the importance of the issue and its critical for ensuring information security remains high on the agenda of CPC's governing bodies and that resources requirements needed to support this agenda are understood.

The following sections provide a high-level description of the data protection responsibilities within CPC and more detailed descriptions for key roles can be found in **Appendix A.**

Governance and Accountability

Roles	Responsibilities
CPC Governing Bodies (the Boards of each group company)	Ultimate accountability for data protection rests with CPC Governing Bodies, which must ensure that they receive an appropriate level of assurance in relation to the data protection duties that are delegated to the Data Protection Steering Group and key officers. They must ensure that details of incidents involving the actual loss of personal data or breach of confidentiality are published are published in CPC's annual report and reported in line with national notification guidance and data protection legislation.
Audit and Risk Committee	The Audit and Risk Committee, as a single committee of all the Governing Bodies, approves data protection policies and receive updates on data protection performance, legal compliance as well as risks and incidents. The SIRO is an attendee of the Audit and Governance Committee and is responsible for updating the Governing Body on data protection matters.

Data Protection Steering Group	The Data Protection Steering Group is accountable to the Governing Bodies through the Audit and Risk Committee and will oversee the extent to which the principles and primary objectives of data protection are embedded within CPC. This will include through a comprehensive work plan monitoring progress toward achieving full compliance. The Data Protection Steering Group will be chaired by the Data Protection Manager. See Appendix B for Terms of Reference.
Senior Information Risk Owner (SIRO)	The SIRO operates at Governing Body level and is responsible for ensuring that organisational information risk is properly identified and managed, and that appropriate assurance mechanisms exist to support the effective management of information risk. The SIRO is supported by Data Protection Manager in relation to key areas of responsibility.
Data Protection Manager (DPM)	The DPM has lead management responsibility for ensuring that robust arrangements are in place regarding data protection. The DPM will assist in the monitoring of internal compliance, inform, and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioners Office. CPC will ensure that the DPM has sufficient support to carry out their role. This role is supported in the delivery of the Data Protection Annual Work Plan by the Risk & Compliance Manager
Risk & Compliance Manager	The Risk & Compliance Manager is responsible for development and delivery of the Data Protection Annual Work Plan. They are also responsible for supporting the SIRO and DPM in the delivery of their responsibilities.

Information Asset Owners (IAO)	Senior staff at Executive Director/Director and/or Deputy Director/Head of Department level will be required to act as IAO's as relevant to the information assets within their remit. They are directly accountable to the SIRO and will provide assurance that information risk is managed effectively for the information asset within their remit.
All staff	All staff, as defined by the scope of this framework, must be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, and information security management and information quality. This is cascaded through employment contracts, third party contracts, policy and processes and mandatory and role-based training.

6. Monitoring and Reviewing

This framework will be monitored and maintained and on an annual basis reviewed by the Data Protection Steering Group.

The CPC's Governing Bodies will be responsible for the scrutiny and approval of the Data Protection Management Framework. Once approved the framework will be submitted to the Governing Bodies for assurance.

Any individual who has queries regarding the content of this framework, or has difficulty understanding how this framework relates to their role, should contact the Risk & Compliance Manager.

7. Staff Training

As a minimum, all staff will need to complete the e-Learning on the BOB platform on a monthly basis, maintaining compliance always.

The Risk & Compliance Manager along with Human Resources will review training needs analysis on an annual basis to identify specific data security and protection training required for the key roles supporting the data protection agenda.

8. Policy Review

This policy will be reviewed as required and at least every two years by the Connected Places Catapult Risk & Compliance Manager and Board.

Appendix A

Key Role Descriptions

Role of the Senior Information Risk Owner (SIRO)

The SIRO is responsible for:

- The management of information risk within the organisation
- Holding Information Asset Owners to account for the management of information assets and related risks and issues
- Leading and fostering a culture that values, protects, and uses information for the success of CPC and benefit of their consumers
- Ensuring that information and cyber security are dealt with at the highest level of management
- Overseeing assurance in respect of service providers data protection and cyber security compliance
- Advising the Governing Body on information risk, system-wide issues, performance, and conformance with information risk management requirements and recommend mitigations.
- Owning CPCs' information incident management framework, ensuring that CPCs approach to information risk management is effective in terms of clear lines of responsibility and accountability, resources, commitment, and execution and that this approach is communicated to staff
- Providing written advice to the Accountable Officer on the content of their Annual Governance Statements regarding information risk
- Ensuring that effective mechanisms are established and published for responding to and reporting perceived or actual serious data protection incidents
- Working closely with the Data Protection Officer, Data Protection Manager, and Risk & Compliance Manager
- The SIRO is also required to undertake Information Risk Management training at least annually and must maintain sufficient knowledge and experience of the business and goals with emphasis on the use of and dependency upon internal and external information assets.

Role of the Data Protection Manager (DPM)

The Data Protection Officer is responsible for:

- Assisting with monitoring internal compliance with the GDPR and other data protection laws, our data protection policies, awareness-training, training, and audits.
- Informing and advising on data protection obligations
- Providing advice regarding Data Protection Impact Assessments (DPIA)
- Acting as a contact point for data subjects and the Information Commissioners Office
- Having regard to the risk associated with processing operations, and consider the nature, scope, context and purpose of processing by the organisation when carrying out its duties
- Helping to demonstrate compliance as part of an enhanced focus on accountability
- Working closely with the SIRO and Risk & Compliance Manager

Role of the Risk & Compliance Manager

Key responsibilities include:

- Ensuring that CPCs meet the required data protection targets and expectations, both internally and externally, specifically bringing together through the Data Protection Annual Work Plan, obligations and best practice in data protection, information lifecycle management and information security.
- Ensuring robust security of electronic resources and encryption is implemented in line with national legislation and local policies.
- Ensuring appropriate record storage, archiving and security arrangements for data
- Ensuring that CPC comply with the requirement for mapping personal information flows
- Identifying and reporting governance risks
- Providing advice and guidance on all aspects of data protection and on all matters related to the Data Protection Act 2018 and other related legislation
- Developing and maintaining comprehensive and appropriate documentation that demonstrates commitment to, and ownership of, data protection responsibilities, such as the Data Protection Management Framework and associated policies and procedures.
- Ensuring that appropriate training is available to all staff and delivered in line with mandatory requirements.
- Maintaining a level of expertise required in order to provide guidance to staff
- Ensuring (through the implementation of the Data Protection Management Framework and associated data protection policies) that all staff understand their personal responsibilities for data protection
- Supporting the Data Protection Steering Group to discharge its data protection responsibilities
- Providing advice and guidance to staff regarding tendering and procurement processes to ensure that all services and contracted services have robust data protection arrangements in place
- Periodically reviewing CPCs' inventory of information assets.

Role of the Information Asset Owners (IAOs)

Information Asset Owners are responsible for:

- Leading and fostering a culture that values, protects, and uses information for the success of CPC and for the benefit of its consumers
- Understanding the nature and justification of information flows to and from information assets
- Knowing who has logical access to assets and why and whether it is a system or information
- Ensuring access to the asset if monitored and compliant with relevant legislation and guidance
- Identifying, understanding, and addressing risk to their information assets, and providing assurance to the SIRO
- Liaising with the Risk & Compliance Manager to update and maintain the Information Asset Register
- Completing relevant training as required for the role

Appendix B

Terms of Reference for the Data Protection Steering Group

1. **Purpose**

   The Data Protection Steering Group (referred from here on within this document as 'the Group') is a sub-committee of the Audit and Risk Committee which in turn reports to the CPC Governing Bodies (Board of each group company). The Data Protection Steering Group overseas the data protection processes, systems and practice across CPC and ultimately provides the Audit and Risk Committee with assurance that the organisation is compliant with, and managing any risk to the data protection compliance, through these processes.

2. **Composition**

   a. **Membership**

   Chair: Senior Information Risk Owner
   Deputy Chair: Data Protection Manager or Risk & Compliance Manager
   Secretary: Governance & Administration Officer
   Data Protection Manager
   Risk & Compliance Manager
   Representative from IT
   Representative for Information Security
   Representative from Digital Transformation
   Representative from Data Science Team
   Representative from Human Resources

   Adhoc members will be invited to meetings, where an agenda item requires attendance.

   b. **The Chair**

   The Senior Information Risk Owner (SIRO) will chair the Group. In the absence of the SIRO, the Data Protection Manager or Risk & Compliance Manager should assume the position of the Chair.

   c. **Attendance**

   All members of this Group are required to attend meetings set or send representation in their absence for continuity purposes. If the representative from any data protection areas is unable to attend, then apologies are expected prior to the meetings. Each of the representatives within the Group will provide brief progress reports on their specific areas of work and bring pieces of work to the group for discussion and approval. Organisation data protection related policies and procedures are also approved at Audit and Risk Committee level.

   d. **Quorum**

   The Group is quorate when at least three members of the group are present.

   Frequency of attendance of members (or their nominated deputies) should be no less than 60% of scheduled meetings. When attendance of an individual member falls below this over an annual period, the issue will be raised with the individual by the Chair, and any steps taken to improve attendance will be taken.

3. **Meetings**

   a. **Frequency**

   The Group will meet monthly to fulfil its remit and reports to the Audit and Risk Committee quarterly, with an annual report to the CPC Governing Bodies Board in each financial year. The overarching reports will be taken to the Audit and Risk Committee by the Chair and to Board either by the Data Protection Manager or Risk & Compliance Manager.

   b. **Agenda and Papers**

   The agenda comprises of a series of reports or briefings from representatives within the Group containing updates on progress with work programmes, cyber security, training, policies and procedures, incidents, information assets and risk. The meeting agenda and supporting papers will be distributed at least five working days in advance of the meetings to allow time for members due consideration of issues. All papers will clearly state the agenda reference, the author and the purpose of the paper, together with the action to be taken.

   c. **Minutes**

   Formal minutes will be kept of the proceedings and submitted for approval at the next Group meeting, prior to submission to the Audit and Risk Committee. Recognising the issue of relative timing and scheduling of meetings, minutes of the Group may be presented in draft form to the next available Audit and Risk Committee meeting. The draft minutes will be cleared by the Chair of the Group and a nominated Lead prior to submission to the Audit and Risk Committee.

   d. **Other**

   In order to fulfil its remit, the Group may obtain any professional advice it requires and invite, if necessary, external experts and relevant staff representatives to attend meetings.

4. **Remit**

   Key Responsibilities of the Data Protection Steering Group

   a. To ensure that an appropriate comprehensive data protection framework and systems are in place throughout the organisation in line with national standards
   b. To develop a data protection policy and associated data protection implementation strategy and/or maintain the currency of the policy
   c. To develop the organisation's data protection work programme
   d. To ensure that the organisation's approach to information handling is communicated to all staff and made available to the public
   e. To co-ordinate the activities of staff given data protection, confidentiality, security, information quality, and records management responsibilities
   f. To offer support, advice, and guidance to the data protection programme within the organisation
   g. To monitor the organisation's information handling activities to ensure compliance with law and guidance

h. To ensure that training is made available by the organisation and taken up by staff as necessary to support their role
i. Provide a focal point for the resolution and/or discussion of data protection issues
j. To provide assurance that where there are changes in processes or working practices, that appropriate information risk assessments are undertaken
k. To provide assurance that organisation undertakes or commissions sufficient reporting, assessments and audits of data protection policies and operations so as to ensure that their implementation and practice both complies with the written policy and that the outcomes are measured to ensure intended benefits when delivered

5. Reporting arrangements to the Board and Accountability

The Group is accountable to the Audit and Risk Committee which in turn reports to the CPC Board.

The Group also receives and discusses data protection incidents, information risk and asset register to ensure that relevant organisation issues and themes are adequately addressed.

The Chief Executive Officer has overall accountability for ensuring that the organisation operates in accordance with the law with the support of their subordinates.

6. Authority

The Group is authorised by the Audit and Risk Committee to investigate any activity within its terms of reference. It is authorised to seek any information it requires from any employee and all employees are directed to co-operate with any request made by the Group. The Group are also authorised to implement any activity which is in line with the terms of reference, as part of the data protection work programme, which shall be signed off by the Audit and Risk Committee.

7. Monitoring and Review

The Group's performance will be monitored by the Audit and Risk Committee. Regular reports to the Audit and Risk Committee will be made by the Data Protection Manager and/or Risk & Compliance Manager, at a frequency determined by the Audit and Risk Committee.

The Group will provide assurance to the Audit and Risk Committee that compliance with these Terms of Reference is being monitored, by keeping accurate minutes of all the Group meetings, registers of attendance and providing update reports as required.

The Group will review these Terms of Reference annually. Any proposed changes to the Terms of Reference will need to be approved by the Audit and Risk Committee.