Individual Rights Policy

1. **Introduction**

Connected Places Catapult (CPC) is under a legal duty to comply with 'individuals rights' requests under the data protection legislation, in relation to personal information that it holds. It is a legal requirement that all requests for personal information held by CPC are handled in accordance with data protection legislation.

This policy and accompanying procedures set out the procedures to follow when requests are received anywhere within CPC.

2. **Scope and definitions**

It is the responsibility of all CPC staff to respond to and help process requests.

Any personal data in relation to an individual, no matter what format, where or how it is stored by CPC falls into the scope of information that can be requested by individuals (i.e. data subjects). All requests must be reviewed, without delay to see if the request can and should be complied with by the Legal and Commercial department.

Requests received by third parties in regard to access to a data subjects personal data (i.e. the Police or Home Office) should be sent immediately to dataprotection@cp.catapult.org.uk.

3. **Details of the policy and compliance with the data protection legislation**

Acknowledging individual's rights

An individual or their representative can exercise several data subject rights. These do not confer automatic agreement to the request but will be duly considered by CPC.

These rights include but are not limited to the following:

- Obtain from CPC confirmation as to whether or not personal data concerning them is being processed , and, where that is the case, request access to the personal data (a subject access request (SAR) – please refer to the Subject Access Request Procedure found in the Legal & Commercial area within the staff SharePoint site)
- Obtain from CPC without undue delay the rectification of inaccurate or incomplete personal data processed by CPC concerning them. CPC staff can complete rectification of inaccurate data held by CPC through the MyHR system. All members of the public should email dataprotection@cp.catapult.org.uk
- Obtain from CPC the erasure of personal data concerning them in certain circumstances, all public requests should be emailed to dataprotection@cp.catapult.org.uk. CPC staff can complete an erasure request of their personal data held by CPC through the MyHR system.
- Obtain from CPC restrictions of processing of personal data concerning them in certain circumstances (Right to restriction – please refer to appendix A)
- Receive the personal data concerning them, which they have provided to CPC, in a structured, commonly used and machine-readable format and have the right to

transmit those data to another controller in certain circumstances. All requests should be emailed to dataprotection@cp.catapult.org.uk.

- Object to processing of an individual's personal data in certain circumstances. All requests should be emailed to dataprotection@cp.catapult.org.uk.
- Not to be subject to a decision based solely on automated processing by CPC (Rights related to automated decision-making including profiling) should be emailed into dataprotection@cp.catapult.org.uk

It should be noted that there are exemptions to some of these rights and whilst CPC must acknowledge the request, there may be legal grounds for not complying with it.

Recognising an individual's right request

- A request can be made verbally or in writing
- A request does not need to mention the phrase containing the right being exercised to be a valid request. As long as the individual has clearly described their request, this is valid. CPC will check with the requester that their request has been understood and request any identification /authorisation (if required).
- CPC will record the details of all requests it receives.

The format that an individual rights request is received may differ from request to request (e.g. in writing or verbal).

CPC staff can submit a request for access to their personal data to the Risk & Compliance Manager, verbally or in writing (dataprotection@cp.catapult.org.uk). Please refer to the Subject Access Request procedure (refer to Legal & Commercial area on staff SharePoint site) for further details on the process.

Members of the public can submit their request to dataprotection@cp.catapult.org.uk.

Refusing a request

If CPC considers that a request is 'manifestly unfounded' or excessive we can decide either to charge a 'reasonable fee/ or refuse to deal with the request.

Charging a fee

- Individual rights requests are free of charge however CPC may in some circumstances be able to charge a fee such as for repetitive requests
- The reasonable fee will be based on the administration costs of complying with the request
- The request does not need to be complied with until the fee has been paid.

Calculating response time

Under data protection legislation CPC has one calendar month to respond to any request.

The time limit will be worked out from the day after the request is received (whether the day after is a working day or not) until the corresponding one-month date from that point.

Extending the response time

CPC can extend the time to respond by a further two months if the request is complex or if a number of requests have been received from the individual. CPC will let the individual know without undue delay and within one month of receiving their request and explain why the extension is necessary.

Verifying identify

If CPC has doubts about the identity of the person making the request it can ask for more information. However, it is important that CPC only requests information that is necessary to confirm who the individual is.

CPC will let the individual know without undue delay that it needs more information from them to confirm their identity. CPC does not need to comply with the request until it has received the additional information.

Responding to a request

CPC's response to a request may be by letter or email.

4. **Monitoring compliance and effectiveness**

The application of this policy and the accompanying procedures (see appendices) will be monitored by CPC through quarterly updates to the Data Protection Steering Group.

5. **Review**

This document may be reviewed at any time at the request of either staff or management, or in response to new legislation or guidance, but will automatically be reviewed two years.

Appendix A

Data Subject Processing Restriction Request Form

Under Article 18 of the EU General Data Protection Regulation (GDPR) you have the right to restrict certain personal data processing by Connected Places Catapult (CPC), subject to limited exceptions. If you wish to restrict CPC's processing of your personal data, you must submit your request in writing to:

Data Protection Manager by email dataprotection@cp.catapult.org.uk

We will then seek proof of identification as follows:

1) **Proof of identity** – this can be a passport, drivers' licence, national identity card or birth certificate; AND

2) **Proof of address** – this can be a utility bill, bank statement, credit card statement (no more than three months old) or current drivers' licence

For information on how we process your personal data and your rights under GDPR, please see our privacy notice: https://cp.catapult.org.uk/privacy-policy/

SECTION 1 - Requestor (data subject) name and contact information

Please provide the data subject's information in the space provided below. If you are a representative making the request on the data subject's behalf, you should provide your name and contact information in SECTION 3.

We will only use the information you provide on this form to identify you and the personal data associated with your processing restriction request, and to respond to your request.

Full name	
Any other names that you have been known by (including nicknames)	
Address	
Date of Birth	
Telephone no.	
Email	

If you are a former employee of Connected Places Catapult, please provide your employee number and your approximate dates of employment.

SECTION 2 – Proof of Data Subject's Identity

We require proof of your identity before we can respond to your processing restriction request. To help us establish your identity, you must provide identification that clearly shows you **name**, **date of birth**, and **current address**. This can be in the form of:

1) Passport, drivers' licence, national identity card or birth certificate

2) Utility bill, bank statement, credit card statement (no more than three months old) or current drivers' licence

Where your name has changed, please provide us with the relevant documents evidencing the change (e.g. marriage certificate).

SECTION 3 – Requests made on the Data Subject's behalf

Please complete this section of the form with your name and contact details if you are a representative acting on behalf of the data subject.

Full name	
Address	
Date of Birth	
Telephone no.	
Email address	

We accept photocopy or scanned image of one of the following proof of your identity:

- passport or photo identification such as a driver's licence.

We also require proof of the data subject's identity before we can respond to the request. To help us establish the data subject's identity, you must provide identification that clearly shows the data subject's **name**, **date of birth**, and **current address**.

We accept a copy of the following as proof of your legal authority to act on the data subject's behalf:

- Written consent signed by the data subject (original only – no photocopies or scans)
- Certified copy of Power of Attorney

We may request additional information from you to help confirm your or the data subject's identity. CPC reserves the right to refuse to act on your request if we are unable to identify the data subject or verify your legal authority to act on the data subject's behalf.

SECTION 4 – Request to restrict personal data processing

Under GDPR Article 18, you have the right to request that we restrict the processing of your personal data, subject to certain limited exceptions, when:

- You contest the accuracy of the personal data we process about you. We must restrict processing the contested data until we can verify the accuracy of your personal data
- We are unlawfully processing your personal information
- We no longer need to process your personal information, but you need the personal data for the establishment, exercise, or defence of legal claims
- You are objecting under GDPR Article 21(1) for processing that we:
    - Consider necessary to perform a task in the public interest under GDPR Article 6(1)(e); or
    - Consider necessary for CPC or a third party's legitimate interest under GDPR Article 6(1)(f)

If you object to processing that we perform under GDPR Articles 6(1)(e) and 6(1)(f), we will restrict the challenged processing activity pending verification of whether CPC or the third parties' legitimate interests override your interests.

To help us proceed with your request quickly and efficiently, please provide as much detail about the personal data you are requesting us to restrict the processing of and the above ground or grounds you are relying on for your processing restriction request.

We will contact you for additional information if the scope of your request is unclear or does not provide sufficient information for us to conduct a search (for example, if you request a processing restriction for "all information about me"). We will begin processing your restriction request as soon as we have verified your identity and have all the information we need to locate your personal data.

Applicable law may allow or require us to refuse to act on your request, or we may have destroyed, erased, or made your personal information anonymous in accordance with our record retention obligations and practices. If we cannot comply with your processing restriction request, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

SECTION 5 – Signature and Acknowledgement

I, ……., confirm that the information provided on this form is correct and that I am the person whose name appears on this form. I understand that: (1) CPC must confirm proof of identity and may need to contact me again for further information; and (2) my request will not be valid until CPC receives all of the required information to process this request.

Signature: ……

Name: ……..

Date: ……

SECTION 6 – Representative Signature

I, ……., confirm that I am authorised to act on behalf of the data subject. I understand that CPC must confirm my identity and my legal authority to act on behalf of the data subject and may need to request additional verifying information.

Signature: ……

Name: ……..

Date: ……..

Appendix B

The individual's rights in more detail

The right to be informed (GDPR Articles 12, 13 AND 14)
CPC must provide individuals with information including (but not limited to):

- Our purposes for processing personal data,
- Our retention periods for that personal data, and
- who it will be shared with.

This is called 'privacy information' or 'Fair Processing Information' and we must provide privacy information in the form of a Privacy Notice to individuals at the time we collect personal data from them. If we obtain personal data from other sources, we must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

How and what information should be provided
The information we provide to people must be:

- concise,
- transparent,
- intelligible,
- easily accessible, and
- it must use clear and plain language

We put our Privacy Notice on our website.

We must regularly review, and where necessary, update our privacy information. We must bring any new uses of an individual's personal data to their attention before we start the processing.

The right of access by the data subject (Subject Access Request (SAR) – GDPR Article 15)

What is the right of access?
The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information.

What is an individual entitled to?
Individuals have the right to obtain the following from CPC:

- confirmation that we are processing their personal data;
- a copy of their personal data; and
- other supplementary information such as:
    - the purposes of processing;
    - the categories of personal data concerned;
    - the recipients or categories of recipient we disclose personal data to;
    - retention period for storing personal data or, where this is not possible, our criteria for determining how long we will store it;
    - the existence of their right to request rectification, erasure or restriction or to object to such processing;
    - the right to lodge a complaint with the ICO or another supervisory authority;

- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards we provide if we transfer personal data to a third country or international organisation

Much of this supplementary information is provided in our privacy notice.

What about requests made on behalf of others?
The GDPR does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney if the individual lacks mental capacity.

What about the records of deceased individuals?
The GDPR and DPA 2018 no longer applies to identifiable data that relates to an individual once they have passed. However, for CPC the ethical obligation of confidence extends beyond death.

An individual will only be able to access the deceased individual's records if they are either or unless they requested confidentiality while alive, an individual's:

- personal representative (the executor or administrator of the deceased individual's estate)
- Someone who has a claim resulting from the death (this could be a relative or another person)

CPC's Subject Access Process should be followed.

The right to rectification (GDPR Article 16 and 19)

The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data. This right has close links to the accuracy principle of the GDPR (Article 5(1) (d)). However, although we may have already taken steps to ensure that the personal data was accurate when we obtained it; this right imposes a specific obligation to reconsider the accuracy upon request.

What do we need to do?
If we receive a request for rectification we should take reasonable steps to check that the data is accurate and to rectify the data if necessary. We should take into account the arguments and evidence provided by the individual.

The right to erasure (GDPR Article 17 and 19)

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for;
- we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;

- we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- we are processing the personal data for direct marketing purposes and the individual objects to that processing;
- we have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- we have to do it to comply with a legal obligation; or
- we have processed the personal data to offer information society services to a child

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the GDPR. For further details about the right to erasure and children's personal data please read the ICO guidance on children's privacy.

Right to restrict processing (GDPR Article 18 and 19)

Individuals have the right to request the restriction or suppression of their personal data. When processing is restricted, we are permitted to store the personal data, but not use it. This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information we hold or how we have processed their data. In most cases we will not be required to restrict an individual's personal data indefinitely, but we will need to have the restriction in place for a certain period of time.

The right to data portability (GDPR Article 20)

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view access and use their personal consumption and transaction data in a way that is portable and safe. It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

The right to object (GDPR Article 21)

An individual has the right to object to

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics

Right not to be subject to automated decision making and profiling (GDPR Article 22)

The GDPR applies to all automated individual decision-making and profiling. Article 22 of the GDPR has additional rules to protect individuals if we are carrying out solely automated decision-making that has legal or similarly significant effects on them. The processing is defined as follows:

- Automated individual decision-making (making a decision solely by automated means without any human involvement).

Examples include an online decision to award a loan; or a recruitment aptitude test which uses pre-programmed algorithms and criteria. Automated individual decision-making does not have to involve profiling, although it often will do.

- Profiling (automated processing of personal data to evaluate certain things about an individual) and includes any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.