STEP AHEAD RECRUITMENT LTD - DATA PROTECTION POLICY

1 ABOUT THIS POLICY

(1) Why do we have a policy?

(a) As an Organisation we store and use information, including personal information ("data"), about clients and others such as employees, workers (staff), job applicants, contractors, suppliers and others with whom we deal or have contact with according to our business obligations. In this Policy, which applies to everyone in the organisation, we will explain how we

- protect the data
- meet our legal obligations including the Data Protection Act 2018 and GDPR (General Data Protection Regulations)
- maintain the rights of individuals whose data we hold ("data subjects")

(b) Our policy works on the basis of "Privacy by Design" which means that we develop data protection measures that meet the needs of our organisation and regularly review them.

(c) The date and version of this policy is shown in the header.

(2) The importance of this policy

(a) Everyone who works for, or on behalf of, the organisation has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy.

(b) Any employee who fails to comply with our data protection policy is dealt with under our disciplinary procedure.

(3) Criminal Liability

(a) The law provides for a number of criminal offences which can be committed in relation to personal data. These include making it an offence to alter personal data to prevent disclosure where a person has made a request exercising their data subject access right and they would have been entitled to receive information in response to that request.

(b)(i) Some of the offences (like the example above) apply not only to data controllers but to company directors and employees (including apprentices) and volunteers.
(ii) It is therefore vital that everyone in the organisation understands their responsibilities and obligations and contacts the Appointed Person to discuss any concerns or raise queries as soon as they arise and before processing any personal data.

(4) Information Commissioners Office (ICO) Registration

As the law requires we are registered with the ICO and the Appointed Person will give you the relevant details or you can search for our registration details at https://ico.org.uk/esdwebpages/search

(5) Accompanying documents
We refer to the following documents in this policy which are located at the end of this policy:

Annex	Document Name	Document Description
Annex 1	Our Data Inventory	Record of what data we hold and how and why we process it
Annex 2	Security Measures	Details of our organisational and technical measures to implement the data protection principles
Annex 3	Individual Request Form	A form which can be used by any individual data subject to exercise their personal data rights

2 WHO'S WHO INCLUDING OUR APPOINTED PERSON

(1) Data Controller
We are a data controller (we "decide the purposes and means" of any data processing").

(2) **Appointed Person**
(a) This type of organisation does not need to appoint a Data Protection Officer. However we have an Appointed Person, who monitors and implements this policy to ensure that we comply with our obligations. Information at the end of this policy (section 14) includes how our Appointed Person can be contacted.

(b) The Appointed Person will offer guidance and assistance in respect of any aspect of data protection and is responsible for compliance. Our Appointed Person will also ensure that anyone working with us understands their personal responsibility to comply with this policy.

(c) The Appointed Person will also:

- Inform and advise the organisation as a whole about how it complies with data protection laws
- Monitor our compliance with data protection laws. This may include conducting audits, data protection impact assessments, supervising staff training and generally managing our internal data processes and activities
- Be the initial point of contact regarding data protection for everybody in the organisation, individuals whose data we process and any supervisory authorities

(3) We may also use data processors in relation to personal data. Data processors are people or organisations who process data on our behalf and in accordance with our instructions. For example we may use a market research company as part of our organisation's marketing development.

(4) Staff Training and awareness

- All of our employees will undergo basic data protection awareness during their induction with us
- Employees who will be dealing with personal data will also receive data protection training relevant to their role. Training will be in a variety of methods, including online training and "on the job" training from managers
- Employee Training is recorded in each individual's Employee Training Record
- We will ask all suppliers, contractors and those with whom we work to confirm that the relevant people working with us have also received data protection training relevant to their respective roles

3 ABOUT DATA

(1) Data

Data (information) includes not only electronically stored information, but includes information written on paper and all records which form any part of our data "system". Our data inventory contains our record of

- What personal data we hold (a basic description of the data)
- The category of data (personal or special)
- Whose data it is

Data can be:

(a) "**Personal data"** means information which relates to a living person who can be identified from that data (a "**data subject**") on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data. Examples of personal data include:

- Contact details (particularly name, address, telephone number and email address)
- Identification information (including passport details, visa and immigration status, date and place of birth)
- Billing information (particularly bank account numbers and information and tax information)

(b) "Special Category personal data" refers to more sensitive types of personal data about an individual including their:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic or biometric data (where it is used for ID purposes);
- Health;

- Sex life and sexual orientation; and
- Any criminal convictions and offences

(c) Non-personal information – will not identify a person but just helps us to use the information to improve our services by identifying, for example, information collected using our website by recording pages accessed and files downloaded to record how visitors to the website use it.

We may aggregate information which is anonymous and does not identify an individual. For example, we may aggregate information about where people live and their ages for marketing purposes.

This policy is primarily concerned with personal (including special category) information.

(2) How we collect data

(a) Direct Data

Most of the data we collect is obtained directly from data subjects through our dealings with others, such as clients, staff and those with whom we work, as well as suppliers.

(b) Indirect data

Sometimes we collect data indirectly, for example publicly available information. When we receive information about any individual from another source, then within a reasonable period of having obtained the data (a maximum of one month or our first communication or before the data is disclosed) we will let the data subject know

- That we have personal data about them and what data categories it falls into
- Where it came from

4 WHAT IS DATA PROTECTION?

By law you can only process (collect, record, organise, use, disclose share etc) personal data (data which could identify a natural person), if you

- Comply with the data protection principles and
- Have a lawful basis to do so, which means you must satisfy at least one of the lawful bases which it lays down

(1) Data Protection Principles

We agree with and adhere to the main principles laid out by law, so that personal data must:

- Be processed fairly, lawfully and transparently
- Be collected and processed only for specified, explicit and legitimate purposes
- Be adequate, relevant and limited to what is necessary for the purposes for which it is processed
- Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay

- Not be kept for longer than is necessary for the purposes for which it is processed
- Be processed securely

We are accountable for these principles and must be able to show that we comply.

(2) Lawful Basis

(a) For personal data, the lawful bases are:

- **Consent** – the individual data subject consents to the processing of their personal data
- **Contractual** – processing is necessary either to take steps towards entering into a contract or to enter into a contract with the individual data subject
- **Legal obligation** – processing is necessary because you need to comply with a legal obligation
- **Vital interests** – processing is necessary to protect the vital interests of either the individual data subject or another person
- **Public tasks** – processing is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the organisation
- **Legitimate interests** – processing is necessary for purposes of legitimate interests pursued by the organisation or a third party, **except** where such interests are overridden by the interests, rights or freedoms of the data subject

(b) For special categories of personal data, the lawful bases are:

- **Explicit consent** – the individual data subject has given their explicit consent for the processing of their personal data (unless relying on that consent is prohibited by law)
- **Employment, social security or social protection laws** – processing is necessary for carrying out those obligations
- **Vital interests** – processing is necessary to protect the vital interests of the data subject or another person where the data subject is either physically or legally incapable of giving consent
- **Not for Profit -** processing for certain not-for-profit organisations provided criteria are met
- **Public** – processing relates to personal data manifestly made public by the data subject
- **Legal matters**
- **Public tasks**
- **Public health**
- **Archiving, research or statistical purposes** – processing is necessary for archiving purposes in the public interest and provided criteria are met

Our data inventory at Annex 1 contains our record of

- Why we process particular data and
- The lawful basis for processing

(3) Withdrawing Consent

(a) Consent must be as easy to withdraw as it is to give (and without suffering any detriment unless consent is necessary for the service provided) which means that we have to provide information about how to do this. Examples of how consent can be withdrawn include:

- Send an email to michelle@stepaheadrecruitment.com
- Call us on 01344-300717

(b) We must take action as soon as is possible and within no longer than 7 days when someone withdraws their consent and we have a set procedure for dealing with this.

(c) Any staff member may receive a withdrawal of consent and they must

- If necessary (for example if consent is withdrawn during a telephone call), clarify the individual data subject's full name and otherwise identify them so we can be sure we are dealing with the correct person (the relevant details)
- Not deal with the withdrawal themselves unless that staff member has been specifically authorised and trained to do so and
- Pass details about the request to their line manager or the Appointed Person by emailing them during the same day that the withdrawal is received, either attaching a copy of any written withdrawal and/or providing the relevant details

5 WHAT DO WE USE PERSONAL INFORMATION FOR?

(1) Using data

(a) Our Organisation needs to process data for its business purposes and where the law says there are limited and justifiable circumstances. Processing should always be "fair, lawful and transparent".

(b) Processing means any operation which is performed on personal data, including data which is part of a filing system and any automated processing. Processing includes

- Collection, recording, organising, structuring or storing
- Adapting or altering
- Retrieval, consultation or use
- Disclosure by transmission, dissemination or otherwise making available;
- Alignment or combining
- Restricting, erasing or destroying

(c) Our business purposes include

- Providing clients with our services and products
- Complying with our business/professional regulations and the law (such as payroll)
- Releasing information legitimately if we are required by law to do so – such as by Court Order
- Generally managing our organisation and its business

Our data inventory at Annex 1 contains our record of

- What personal data we hold (a basic description of the data)
- The category of data (personal or special)
- Whose data it is
- When personal data is processed

(d) We do NOT use data for decisions which are solely taken on an automatic basis.

(2) Privacy Notices

It is important that every data subject receives essential and important information about how we collect and use personal data. We have provided

- A privacy policy on any website which we own and/or operate. Any staff member will print and provide a paper copy of this to anyone who asks for one

(3) Confidentiality

This section relates to the additional professional confidentiality obligations imposed on us.

(a) Most information which our clients supply to us is confidential, which means that we will not share/disclose it with anybody else until they have instructed us to do so or we have to release it by regulatory compliance, law or Court Order. So, for example, if we are instructed to share personal information with a third party, we will ask for the data subject's written consent to do that. However, some authorities (such as HMRC) may examine our information if they have a right to do so.

(b) We will obtain consent for each person/organisation that we have been instructed to share data with.

(c) Outsourcing - as part of our business we may use external providers for services such as for administration support and pass information to them. However, we have confidentiality agreements in place with them which means that information will only be held by them to provide services to us.

6 MANAGING DATA RISKS AND SECURITY

Data security means that we do what we reasonably can to protect the personal data that we hold and ensure our security is in accordance with current legal requirements.

(1) Managing risk - Data Protection Impact Assessments (DPIA)

It is important that we assess risks involved when we process data and so there will be occasions when we conduct a Data Protection Impact Assessments (DPIA).

DPIAs allow us to both identify risks and resolve issues at the earliest stage. There are certain circumstances when we must carry out a DPIA, including when

- We are using new technologies
- The processing is likely to result in a “high risk to the rights and freedoms of individuals”

The Appointed Person has overall responsibility for the DPIA

(2) Security Measures
(a) Our appropriate security measures are based on the likely risks to data which we have identified, for example loss of data or unauthorised disclosure. We have implemented appropriate organisational (people and processes) and technical measures to effectively implement the data protection principles.

(b) Our data inventory contains our record of

- Where data is located - who holds the data and who can access it
- What security controls are in place

(c) Our Security Measures at Annex 2 outline the appropriate organisational (people and processes) and technical measures we have implemented.

(d) Everyone must adhere to our data security procedures and will receive appropriate training. Any employee who fails to comply with our data protection policy is dealt with under our disciplinary procedure and such an event may mean termination.

7 INDIVIDUAL RIGHTS

(1) The law gives rights to each individual in respect of their personal data. The rights included are:

- To be informed (see Privacy Notices in section 5(2) of this policy)
- To access data (Subject Access) which includes to
  - obtain confirmation as to whether personal data is processed
  - be provided with further information about the processing
  - access their (the data subject's) data/obtain a copy of it
- Rectification (correct inaccurate or incomplete data)
- Erasure/be forgotten (we can't use the data but may quarantine it so it's not used unlawfully and we keep it in a separate list)
- Restrict processing (limit what we can do with the data)
- Data portability (so an individual can obtain and move, copy or transfer personal data easily)
- To object to processing data (limited circumstances)
- Those rights available when processing is carried out by automated means and profiling but this does not apply to us because we do not do this type of processing

(2) Although it does not have to be used we have an Individual Request Form (at Annex 3) which individual data subjects can use to exercise these rights and we have a set procedure for dealing with these requests.

(3) Dealing with requests to exercise data rights

(a) Any staff member may receive a request from an individual data subject to exercise a data right, irrespective of whether it is on an Individual Request Form or not (for example, someone may ask on the phone or by email). The staff member will

- Not deal with the request unless they have been specifically authorised and trained to do so
- Pass details about the request to their line manager or the Appointed Person by emailing them during the same day that the request is received

(b) We deal with each request as soon as we are able and within one month of receipt. If there is going to be a delay in dealing with any request or there is a reason why we can't comply with your request we will let the individual data subject know and explain why within one month of receiving their request. We must deal with even complex cases within 3 months.

(c) Individual data subjects have the right to lodge any data protection complaints with the ICO, who is the UK's supervisory authority. They should visit www.ico.org.uk for more information including how to access their helpline.

8 RECORDS AND RETENTION OF DATA

(1) Record keeping is an important part of our data protection because it demonstrates how much we value data security and is a vital part of our compliance with the law. We keep a record of our data processing activities, including recording:

- The type of data processed and
- The purposes for which it was used

In addition, data processors will be asked to keep a record about who instructed them to process special category data.

(2) Our criteria

We keep information about people

- For as long as it is necessary for the purposes for which the personal data are processed
- To enable us to comply with our legal obligations, for example for tax purposes

(3) Data Retention

Data Subject	How long personal information/data is kept
Candidates	We will retain personal information for 2 years from the date of our last contact.
Clients	We will retain personal information for 7 years from the date that you ceased to be a client.
Potential Suppliers	We will retain personal information for 6 months from the date of the last time you contacted us.

Suppliers	We will retain personal information for 7 years from the date that you ceased to be a supplier.
Employees	We will retain personal information for 7 years from the date that you ceased to be an employee.
Potential employees	We will retain personal information for 6 months from the date of the last time you contacted us.

9 PERSONAL DATA BREACHES AND OUR OBLIGATIONS

(1)(a) A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

(b) Although we take great care with our data the law requires us to have a process in place should a problem occur. Therefore
(i) it is the responsibility of every member of staff who deals with personal data to be able to recognise a personal data breach.
(ii) if you become aware of an actual or potential breach of our data obligations you must

- Take notes and keep any evidence of it AND
- Report it to our Appointed Person, within 24 hours of the time of the actual, suspected or potential breach being identified

(c) Our Appointed Person will then determine what action must be taken, including whether the ICO must be notified.

(2) The Appointed Person will then take the necessary action to
(a) Fully investigate the issue.
(b) Take remedial action.
(c) Keep a record of the breach which will include

- The facts relating to the personal data breach
- The effects of the breach
- The remedial action taken

(d) Report relevant breaches to the ICO without undue delay after being identified and, where feasible, not later than 72 hours after becoming aware of a breach so as to minimise the risk of damage. Unless it is not possible to do so at the time (in which case the information will be provided without undue delay) that information will include

- The Appointed Person's name and contact details
- A description of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
- A description of the likely consequences of the personal data breach;
- A description of the measures which we've taken or propose to take to address the personal data breach, including, where appropriate, mitigating its possible adverse effects

(e) In cooperation with the ICO and/or any other relevant authorities (such as the police) and taking into account any guidance, directly notify any affected individual data subjects involved, without undue delay and as soon as is reasonably feasible (the ICO may still decide to do this directly), of the data breach to allow them to take the necessary precautions unless one of the following exemptions are met
(i) the breach is unlikely to result in a high risk for an individual's rights and freedoms
(ii) there was appropriate organisation and technical protection (such as encrypted data) in place when the breach occurred
(iii) notification would equate to a disproportionate effort, when an alternative such as a public information campaign may mean the individual can effectively be informed
(e) Where the Appointed Person notifies the affected individual data subjects about the data breach they will also make recommendations to mitigate potential adverse effects.

10 SHARING DATA WITH THIRD PARTIES DATA SHARING POLICY

(1) Types of data sharing

Sharing data can be because we want

- Someone to process the data and we remain as the data controller (they are a data processor)
- To share the data with another organisation so that we can both decide why and how the data we hold will be processed. In this relationship we will both be data controllers because we can both decide how the data will be processed

Before we share any data we always ensure that

- We have a lawful basis to enable us to share the personal data
- we can justify sharing the data

We also use a third party data-sharing checklist to record essential information when we are sharing data with a third party. The checklist is available from the Appointed Person.

(2) Who we share data with

Our organisation needs to share personal data with various third parties including:

- Third-parties who provide services to us
- Service providers who perform functions on our behalf
- Third-party data storage providers who process data on our behalf
- Public authorities who make a lawful request, including to meet national security or law enforcement requirements

Lists of the third parties with whom we share data are available from the Appointed Person and by accessing the Privacy Policy on our website

(3) Data Protection measures we take when sharing data

We have written agreements with those third parties to ensure that they

- Provide the same level of protection that the law requires and

- Transfer the minimum data necessary and anonymise data wherever reasonably possible
- Limit their use of the data to the specified services they provide on our behalf
- Process data on our behalf in accordance with our joint legal obligations

11 INTERNATIONAL DATA TRANSFER POLICY

(1) Sometimes it is necessary for organisations to transfer personal data outside the EEA and because some countries do not have the same level of data protection the law restricts the transfer of personal data so that this can only take place if

- Certain conditions are met. For example
  - there is a list of approved countries which provide an adequate level of data protection
  - there is an obligation on us to ensure that appropriate safeguards are in place, such as the EU-US Privacy Shield where organisations self-certify that they meet the Shield standards
- There is a derogation or exemption (such as the individual's informed, compliant and valid consent or contractual performance which allows us to do this
- It's a one-off transfer which meets the relevant criteria

(2) We do not send personal data outside the EEA.

12 POLICY IMPLEMENTATION, MONITORING & CHANGES

(1) Clients will be made aware of this policy and its main content when we reach an agreement to provide our services and products to them.
(2) Suppliers will be made aware of the policy at the time we enter into an agreement that they will supply to us.
(3) Staff will be made aware of the policy and its content during induction or other training.
(4) We will review this Policy at least every six months (or as and when we know that any important changes in the law or guidelines is coming) and, where possible, twelve weeks' notice of any changes to the Policy will be given to staff and, as applicable, clients and suppliers.
(5) Suggestions about this Policy are welcome. Please make suggestions to the Appointed Person.

13 COMPLAINTS

(1) Any queries or complaints regarding our data protection should be addressed to our Appointed Person, using the details at the end of this policy.

(2) Any individual can complain to a supervisory authority – currently the ICO. The ICO can be contacted via its website at https://ico.org.uk/concerns/ (there is usually a live chat facility) or by using its telephone helpline on 0303 123 1113.

(3) Any individual data subject who wants to; obtain details about what personal information we hold about them; rectify data; restrict or object to processing; as from 25th May 2018 exercise the right to erasure, must contact our Appointed Person using the details at the end of this policy – please also see section 7 of this policy.

14 CONTACT DETAILS FOR THE APPOINTED PERSON

Appointed Person: Michelle Brown

By Email: michelle@stepaheadrecruitment.com

By Post: Venture House, Arlington Square, Downshire Way, Bracknell, Berkshire RG12 8WA

By telephone: 01344 300717

ANNEX 1 – OUR DATA INVENTORY
STEP AHEAD RECRUITMENT LTD – DATA INVENTORY

CONTACT DETAILS
Responsible Person: Michelle Brown – MD, Step Ahead Recruitment Ltd, Venture House, Arlington Square, Bracknell, Berkshire RG12 8WA
Telephone: 01344 300717
Email: michelle@stepaheadrecruitment.com

Last Review Date: 24th May 2018 Reviewed By: Michelle Brown NEXT review due: 24thMay 2019

What personal data do we process? Description of data	**Category of data** (personal or special)	**Whose data is it?** (categories of data subjects)	**Why do we process this data?** Purpose - why is the data held and what is it used for	**Basis for processing data**	**When is personal data processed?** (including disclosure)	**Where is it located - who holds the data and who can access it?**	**Where does the processing take place?** (international transfer and relevant safeguards)	**What security controls are in place?**	**How long is data kept for?**	**Is this covered by our privacy notice?**	**ACTION REQUIRED**
Employee number, Name, address, Date of birth, NI number , salary information, tax code	Personal	Current and former employees,	Payroll ,	Legal Obligation,	HMRC to pay relevant payroll taxes and NI	MD, accountant, HMRC	Accountant server,	Hard Drive back-up,	7 years to comply with HMRC	Yes- in Employee privacy	
Name, address, email, salary and benefits, information, notice period		Candidates	provision of recruitment services	legitimate interest or consent	Provision of recruitment services	MD	Manually, cloud SAAS CRM system, externally hosted (UK)	Online backup	2 years or 7 years to comply with HMRC	Privacy Policy	

ANNEX 2 – OUR DATA SECURITY MEASURES

This contains details of our organisational and technical measures to effectively implement the data protection principles.

- Physical Security – including securing documents in locked cabinets when not in use and shredding confidential waste
- Data backup – *include details of encryption standard, password access protocols, remote storage (without address - merely confirmation of remote storage) and frequency*
- User access control management. We restrict access on a "need to know basis
- Password control
- Regular software updates in accordance with the recommended guidelines, if appropriate, by using patch management software
- Timely decommissioning and secure wiping (that renders data unrecoverable) of old software and hardware
- Firewalls
- Real-time protection anti-virus, anti-malware and anti-spyware software
- Encryption of all portable devices
- Encryption of personal data in transit (e.g. SSL)
- Providing internal policies, procedures and training including about IT Use (such as emails, internet and social media) and a BYOD Policy
- Regular reviews of the way we process data in line with our data protection policies

ANNEX 3 – OUR INDIVIDUAL REQUESTS FORM

INDIVIDUAL REQUEST FORM

If an individual wishes to exercise their legal right to access their personal data, they should use this form,

What personal data rights do I have?
The law, including the EU General Data Protection Regulation (GDPR), gives you certain rights in relation to your personal data, including the rights to:

- Access your personal data
- Rectify your personal data if it is inaccurate or incomplete
- Ask us to erase your personal data and prevent processing in specific circumstances
- Restrict processing of your personal data in certain circumstances
- Obtain and reuse your personal data for your own purposes across different services
- Object to processing your personal data in certain circumstances

How can I find out more about my rights or about your data protection?
If you want to find out more about these rights or how we protect personal data, contact:
Contact Name: Michelle Brown
Email Address: michelle@stepaheadrecruitment.com

How do I exercise my rights?
You can email us or complete this form and
Email it to: michelle@stepaheadrecruitment.com
Post it to: Step Ahead Recruitment Ltd, Venture House, 2 Arlington Square, Downshire Way, Bracknell, Berkshire RG12 8WA

Do I need to use this form?
You do not have to use this form if you don't want to but it does explain what information we need. Using the form will usually mean that your request is finalised more quickly. If you prefer to write to us you will find it helpful to look at the form to identify the information that we need.

When can I expect a reply?
We will reply to you as soon as we can and within 1 month of receiving your request. If for some reason we need more information, cannot comply with your request or there is going to be a delay then we will also let you know within 1 month of receiving your request.

Will you always supply information that I ask for?
We will always try to provide you with what you have asked for. However, sometimes there may be a reason why we cannot comply with your request. For example:

- we may need to confirm your identity or ask for more details
- if the information you want directly or indirectly reveal details about another person we will have to obtain consent from that person before we can let you see that information
- we may not be able to let you see information if letting you see it would adversely affect the

rights and freedoms of others

Do I have to pay anything?
In most cases we will be happy to provide you with what you want without making any charge. However, if you are asking for additional copies of information we have already provided to you, we may decide to charge a fee or refuse the request if it is considered to be "manifestly unfounded or excessive". We will advise you about any fee we intend to charge before we comply with your request.

However we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

INDIVIDUAL RIGHTS REQUEST FORM

SECTION 1: Details of the person requesting information
Please provide the following information.

Full Name	
Postal Address	
Email address:	
Contact telephone number:	

SECTION 2: Are you asking about data relating to you or to someone else?
Please tick the appropriate box and read the instructions which follow it.

□ **Yes -** I am asking about my own data and I attach proof of my identity (see section 3)

□ **No -** I am helping someone else to access their personal data.
Please complete the information below and attach

- the other person's written authority and
- proof of that person's identity and (see section 3)
- proof of your identity (see section 3)

Please complete giving details of the person whose personal data you are asking about:

Full Name	
Postal Address	
Email address:	
Contact telephone number:	

SECTION 3: Proof of Identity

So that we can be sure we are releasing personal information to the correct person please provide us with proof of identity and address from the table below. If we need more information we will contact you.

Proof of Identity – Choose and attach one	**Proof of Address – Choose and attach one**
Passport	Current driving licence
Photo driving licence	Current TV licence
National identity card	Utility bill (no more than 3 months old)
Birth certificate	Bank statement (no more than 3 months old)
Marriage certificate	Credit card statement (no more than 3 months old)
	Local authority tax bill (no more than 1 year old)
	HMRC tax document (no more than 1 year old)

SECTION 4: What do you want us to do?

Please see the "What personal data rights do I have?" at the beginning of this form and tell us/describe what you want us to do and let us have any other relevant details you think will help us to identify the information you want.

For example, if you want to access your personal data just tell us that this is what you want to do and let us have any other relevant details that you think will help us to identify the information you want.

SECTION 5: Declaration

I confirm that I have read and understood the terms of this Individual Rights Requests Form and confirm that the information I have given is true.

Please note that a person who provides misleading information or impersonates another or attempts to impersonate another may be guilty of an offence

Please complete:

☐ I am the person named in Section 1. The information supplied in this Request is correct.

OR

☐ I am helping the person named in Section 2 and enclose their authority to make this Request

OR

☐ I have parental responsibility/power of attorney for the person named in Section 2

Signed: ……

Name (block capitals)……

Date: …….

This is an option for which individual data subjects who want to exercise any of their legal rights in respect of their personal data can use.