IN FOCUS EDUCATION & DEVELOPMENT CiC

Data Protection Policy

Data Protection Officer – Kristianne Drake (kristianne@infocuset.co.uk)

Community Interest Company Limited by Guarantee: 13044034

FINAL – 01/12/2021	
Subject: Data Protection Policy	**Issue Number: 1**
	Pages 1 of
Distribution: All employees, volunteers, self employed	
Issued by: Xavier Fiddes: Company Director 'Head of Operations'	Issue date: December 2021
This policy sets out In Focus's approach to the protection of Data. If you have any comments, suggestions or amendments please put these in writing to the person issuing this policy.	

Policy Statement
This policy is the overarching policy for date security and protection for In Focus and sets out our commitment to data protection and individual rights and obligations in relation to personal data.

Data Protection Officer
The Company's Data Protection Officer is *Kristianne Drake*. They can be contacted at *kristianne@infocuset.co.uk.*

Purpose
The purpose of the Data Protection Policy is to be transparent about how data is collected and used. It is to support the 10 Data Security Standards, the General Data Protection Regulations (2016), the Data Protection Act 2018, the common law duty of confidentiality and all other relevant legislation.

Scope
This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers, and self-employed contractors. These are referred to in this policy as relevant individuals.

It includes in its scope all data which we process either in hard copy or digital copy and includes special categories of data.

Definitions

- **Personal data** is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, or online identifier. It can also include pseudonymised data.

- **Special categories of personal data** is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

- **Criminal offence data** is data which relates to an individual's criminal convictions and offences and information relating to criminal allegations and proceedings.

- **Data processing** is any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data protection principles
All personal data obtained and held by In Focus will be:

- processed fairly, lawfully and in a transparent manner
- collected for specific, explicit, and legitimate purposes
- adequate, relevant, and limited to what is necessary for the purposes of processing
- kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage by using appropriate technical or organisation
- measures
- comply with the relevant GDPR procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows, the right:

- to be informed
- of access
- for any inaccuracies to be corrected (rectification)
- to have information deleted (erasure)
- to restrict the processing of the data
- to portability
- to object to the inclusion of any information
- to regulate any automated decision-making and profiling of personal data.

Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship is held in the individual's personnel file (in hard copy or electronic or both). Where In Focus processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with data protection legislation.

Where In Focus engages third parties to process personal data on its behalf, such parties do so based on written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and company measures to ensure security of data.

Procedures
In Focus has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

1 it appoints or employs employees with specific responsibilities for:
- the processing and controlling of data

- the comprehensive reviewing and auditing of its data protection systems and procedures
- overviewing the effectiveness and integrity of all the data that must be protected.
- there are clear lines of responsibility and accountability for these different roles.

2 it provides information to its employees and service users on their data protection rights
    - how it uses their personal data
    - how it protects it

    The information includes the actions relevant individuals can take if they think that their data has been compromised in any way

3 it provides its employees with information and training to make them aware of the importance of protecting personal data
    - to teach them how to do this
    - to understand how to treat information confidentially

4 it can account for all personal data it holds
    - where it comes from
    - who it is shared with
    - who it might be shared with

5 it carries out risk assessments as part of its reviewing activities
    - to identify any vulnerabilities in its personal data handling and processing
    - to take measures to reduce the risks of mishandling and potential breaches of data security

    The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by In Focus

6 it recognises the importance of seeking individuals' consent for
- obtaining
- recording using
- sharing
- storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions.
- In Focus understands that consent must be freely given, specific, informed, and unambiguous. In Focus will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time

7 it has the appropriate mechanisms for
- detecting, reporting, and investigating suspected or actual personal data breaches, including security breaches.

8 it is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences

9 it is aware of the implications international transfer of personal data internationally.

Requesting access to data
Relevant individuals have a right to be informed whether In Focus processes personal data relating to them and to access the data that is held about them. Requests for access to this data will be dealt with under the following summary guidelines:

- email *Kristianne Drake* with the subject and details of the data access request. The request should be made to *kristianne@infocuset.co.uk*
- In Focus will not charge for the supply of data unless the request is manifestly unfounded, excessive, or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request
- In Focus will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform In Focus immediately if they believe that the data is inaccurate, either because of a subject access request or otherwise and if necessary immediate steps to rectify the information will be taken.

Data disclosures
In Focus may be required to disclose certain data/information to any person. The circumstances leading to such disclosures may include:

- any employee benefits operated by third parties
- disabled individuals - whether any reasonable adjustments are required to assist them at work
- individuals' health data - to comply with health and safety or occupational health obligations
- HR and payroll management and administration - to consider how an individual's health affects his or job
- the smooth operation of any insurance policies or pension plans.

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data security
In Focus adopts procedures designed to maintain the security of data when it is stored and transported.

In addition, employees must:

- access only data that they have authority to access and only for authorised purposes
- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by those who have a need and a right to access them
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- check regularly on the accuracy of data being entered into computers
- always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them
- use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by In Focus Directors. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where necessary
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left lying around where they can be mislaid or stolen.

Failure to follow the Company's rules on data security may be dealt with via In Focus' disciplinary procedure; significant or deliberate breaches of this policy could lead to dismissal from employment.

International data transfers
The Company does not transfer personal data to any recipients outside of the EEA.

Breach notification
Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the Company becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly if the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, In Focus will do so without undue delay.

Training
New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and to In Focus of any potential lapses and breaches of policies and procedures.