Scottish Union of Supported Employment

Protecting Data Policy and Privacy Statement

Document Type	**Policy**
Owner	**David Cameron**
Position	**Chief Executive Officer**
Date of Issue	**14 July 2022**
Date of Review	**14 July 2024**
Version	**3**

Protecting Data Policy

This policy applies to employees, members, consultants and trustees.

1. Overview

1.1 SUSE takes the security and privacy of data seriously. We need to gather and use information or 'data' as part of our business and to manage our relationships. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. We have a duty to notify employees and stakeholders of the information contained in the policy.

1.2 This policy applies to current and former employees, workers, volunteers, consultants and people who participate on our projects. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside a contract of employment or contract for services and any other notice we issue to you from time to time in relation to your data.

1.3 This policy explains how SUSE will hold and process your information. It explains your right as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, SUSE.

1.4 This policy does not form part of a contract of employment or contract for services and can be amended by SUSE at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, SUSE intends to comply with the 2018 Act and the GDPR.

2. Data Protection Principles

2.1 Personal data must be processed in accordance with six 'Data Protection Principles'

It must:

- be processed fairly, lawfully and transparently
- be collected and processed only for specified, explicit and legitimate purpose
- 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 longer than is necessary for the purposes for which it is processed
- be processed security
- we are accountable for these principles and must be able to show that we are compliant.

3. How we define personal data

3.1 **'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 that 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.

3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

3.3 This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency) or it could be created by us. It could be provided or created during a recruitment process or during the course of a contract of employment or services or after its termination. It could be created by a manager or other colleagues.

3.4 We may collect and use the following types of personal data about you:

- recruitment information such as an application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments
- your contact details and date of birth
- your gender
- your marital status and family details
- information about a contract of employment or services including start and end dates of employment, role and location, working hours, details or promotion, salary (including details or previous remuneration), pension, benefits and holiday entitlement
- your bank details and information in relation to your tax status including your national insurance number
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings)
- information relation to your performance and behaviour at work
- training records
- electronic information in relation to your use of IT systems or telephone systems
- your images (whether captures on CCTV, by photograph or video)
- personal information relating to a disability or long term condition
- any other category of personal data which we may notify you of from time to time

4. How we define special categories of personal data

4.1 **'Special categories of personal data'** are types of personal data consisting of information as to:

- your racial or ethnic origin
- your political opinions
- your religious or philosophical beliefs
- your trade union membership
- your genetic or biometric data
- your health
- your sex life and sexual orientation
- any criminal convictions and offences

We may hold and use any of these special categories of your personal data in accordance with the law.

5. How we define processing

5.1 **'Processing'** means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage
- adaption or alteration
- retrieval, consultation or use
- disclosure by transmission, dissemination or otherwise making available
- alignment or combination
- restriction, destruction or erasure

This includes processing personal data which forms part of a filing system and any automated processing.

6. How will we process your personal data?

6.1 SUSE will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

6.2 We will use your personal data for:

- performing the contract of employment or services between us
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else).

  However, we can only do this if your interests and rights do not override ours (or theirs).

  You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in Section 12 below.

  We can process your personal data for these purposes without your knowledge or consent.

We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intent to rely on for processing it.

If you choose not to provide us with certain personal data you should be aware that we may not wish be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax and HMRC or to make reasonable adjustments in relation to a disability.

6.3 SUSE maintains a Record of Processing Activities (ROPA). This is reviewed on an annual basis and updated when information changes.

7. Examples of when we might process your personal data

7.1 We have to process your personal data in various situations during your recruitment, employment or engagement or participation and even following termination of your employment or engagement or participation.

7.2 For example (and see section 7.5 below for the meaning of the asterisks):

- to decide whether to employ or engage you or work with you on one of our projects.
- to decide how much to pay you, and the other terms of your contract with us
- to check you have the legal right to work for us
- to carry out the contract between us including where relevant, its termination
- training you and reviewing your performance*
- to decide whether to promote you
- to decide whether and how to manage your performance, absence or conduct*
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else
- to determine whether we need to make reasonable adjustments to your workplace or role*
- to monitor diversity and equal opportunities*
- to monitor and protect the security (including network security) of SUSE, of you, our other staff, customers and others
- to monitor and protect the health and safety of you, our staff, customers and third parties*
- to pay you and provide pension and other benefits in accordance with the contract between us*
- paying tax and national insurance
- to provide a reference upon request from an employer
- to pay trade union subscriptions*
- monitoring compliance by you, us and others with our policies and our contractual obligations*
- to comply with employment law, immigration law, equalities law, health and safety law, tax law and other laws which affect us*
- to answer questions from insurers in respect of any insurance policies which relate to you*

- running our business and planning for the future;
- the prevention and detection of fraud or other criminal offences;

- to defend SUSE in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*
- for any other reason which we may notify you of from time to time

7.3 We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose.

7.4 We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent
- where you have made the data public
- where processing is necessary for the establishment, exercise or defence of legal claims
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity

7.5 We might process special categories of your personal data for purposes in paragraph 7.2 above which have an asterisk beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness to work, to pay your benefits, to comply with our legal obligations under employment law including to make reasonably adjustments and to look after your health and safety

7.6 We do not take automated decisions about you using your personal data or use profiling in relation to you.

8. Storage of personal data

From August 2022 SUSE has stored data on a CRM system. This system is secure and can only be accessed by authorised personnel. Examples of information held includes:

- Details on employers who are working on a SUSE project
- Training providers / consultants who work with SUSE
- SUSE Staff, including sessional or staff on fixed term contracts
- Volunteers on SUSE projects, such as people who have lived experience group
- SUSE members

8.1 Data is held while someone is actively engaged with SUSE (e.g. in employment, participating on a SUSE project) and for a period afterwards. This is reviewed after 5 years and deleted if the data is no longer of a legitimate interest.

9. Sharing your personal data

9.1 Sometimes we might share your personal data with contractors and agents to carry out our obligations under our contract with you or for our legitimate interests (for example the SUSE payroll is processed by SCVO).

9.2 We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to progress your data for the lawful purpose for which it has been shared and in accordance with our instructions

9.3 Such legitimate third parties include:

- payroll services
- pension company
- life assurance company
- providers carrying out projects on behalf of or in partnership with SUSE

9.4 We do not send your personal data outside of the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

10. How should you process personal data for SUSE?

10.1 Everyone who works for, or on behalf of, SUSE has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and SUSE's Data Security and Data Retention policies.

10.2 SUSE is responsible for reviewing this policy and updating the Trustees on SUSE's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to the CEO.

10.3 You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of SUSE and only if you are authorised to do so. You should only use that data for the specified lawful purpose for which it was obtained.

10.4 You should not share personal data informally

10.5 You should keep personal data secure and not share it with unauthorised people.

10.6 You should regularly view and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

10.7 You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

10.8 You should use strong passwords.

10.9 You should lock your computer screen when you are not at your desk.

1010 Personal data should be encrypted before being transferred electronically to authorised external contacts

10.11 Consider anonymising data or using separate keys/codes so that data subject cannot be identified.

10.12 Do not save personal data to your own personal computers or other devices

10.13 Personal data should never be transferred outside the European Economic Area expect in compliance with the law and authorisation of the organisation.

10.14 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

10.15 You should not take personal data away from SUSE's premises without authorisation from your line manager.

10.16 Personal data should be shredded and disposed of securely when you have finished with it.

10.17 You should ask for help from your line manager if you are unsure about data protection or if you notice any areas of data protection or security we can improve on.

9.18 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

10.19 It is a criminal offence to conceal or destroy personal data which is part of a subject access request. This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

11. How to deal with data breaches

11.1 We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the

Information Commissioner's Office within 72 hours. If you are aware of a data breach you should contact the CEO of SUSE immediately and keep any evidence you have in relation to the breach.

A data breach log is held on the SUSE network and can be accessed by Staff who have been trained how to complete it, in the event that this is necessary.

12 Subject access requests

12.1 Data subjects can make **'subject access request'** ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to your line manager who will coordinate a response.

12.2 If you would like to make a SAR in relation to your own personal data you should make this in writing to the Chief Executive Officer. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

12.3 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request

13. Your data subject rights

13.1 You have the right to information about what personal data we process, how and on what basis as set out in this policy.

13.2 You have the right to access your own personal data by way of a subject access request.

13.3 You can correct any inaccuracies in your personal data.

13.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you could contact your line manager.

13.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact your line manager.

13.6 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

13.7 You have the right to object if we use your personal data for direct marketing purposes

13.8 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within a month.

13.9 With some exceptions, you have the right not to be subjected to automated decision-making.

13.10 You have the right to be notified of a data security breach concerning your personal data.

13.11 In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right to consent or to withdraw your consent later. To withdraw your consent, you should contact your line manager.

13.12 You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

APPENDIX 1

Privacy Statement – GDPR Statement

SUSE takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the Data Protection Act 2018 and the EU General Data Protection Regulations in respect of data privacy and security.

Personal Information

Personal information includes information that can be used to identify you; this may include your name, email address, postal address (business), telephone number and credit/debit card details.

How Do We Collect Information?

We collect information from you in the following ways:

- Making an enquiry about our services, events, jobs and campaigns.
- Registering to become a member of SUSE.
- Registering for the SUSE newsletter
- Involved in projects managed by SUSE

How Will We Use This Information?

We will only use your personal information to give you the information or services you asked for. For example:

- To keep you informed about the work of SUSE.
- To send you information about third parties which may be of interest to you.
- To contact you about events, campaigns, jobs and consultations.
- To link you with 3rd party service providers if requested.

3rd Party Software

SUSE uses 3rd party software to run some of our application online, these include the online payment provider and email marketing software called Campaign Monitor.

Marketing and Sharing

SUSE will not share, sell or lease your information with a 3rd party, unless we have your written consent to allow us to share it.

How Do We Protect Personal Information?

SUSE will make sure your personal information is kept secure. You can ask for your information to be removed at any time and also the right to ask what information we hold about you at any time.

Cookies

Cookies are generated when a user enters the SUSE website. They are text files which identify users' computers to the SUSE server. They are stored on the hard drive of your device. An example could be when you are a member of SUSE and login to your SUSE account. Cookies may be engaged at this point to remember your account information, such as a password. This cookie will not give us access to your password.

Another example could be a third-party cookie such as Google Analytics. SUSE uses Google Analytics to help us improve our website. These analytics tools use cookies that are not controlled by SUSE but which are active when you use our website.

Our website works better with cookies enabled. Our cookies don't give us or anyone else access to your personal data.

If you have any issues or concerns with the information provided here please do not hesitate to contact us:

E: info@susescotland.scot T: 0141 777 5840

Appendix 2 Data Breach Log

The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

Personal data security breach log

Service providers must notify the ICO of any personal data breach within 24 hours

Organisation: Scottish Union of Supported Employment	Date:

No.	Your ref.	Details of breach						Consequences of breach	Measures taken/to be taken			
		Date of breach	No. people affected	Nature of breach (choose most relevant)	Description of breach	How you became aware of breach	Description of data		All individuals informed?	Remedial action	Other Regulators informed	When did you first notify the ICO of the breach?