Julie Haywood
COMMUNITY VENTURES LTD

# Information Governance, Data and Privacy Policy

October 2026

| | |
|---|---|
| **Version: Final** | **Next Review Date: October 2027** |
| **Title:** | **Information Governance, Data and Privacy Policy** |
| **Author:** | **Policy Assistant** |
| **Applicability:** | **All organisation** |

This policy will be reviewed once a year as a minimum.

# 1. Introduction

Julie Haywood Community Ventures Ltd is a consultancy firm built on principles of trust, professionalism, and strategic insight. The firm recognises its responsibility to uphold the highest standards of information governance, data protection, and privacy across all facets of its work.

This policy outlines the framework by which Julie Haywood Community Ventures Ltd manages and safeguards data—whether relating to clients, partners, stakeholders, or internal operations. It reflects our commitment to legal compliance, ethical handling of information, and proactive risk management, aligning with applicable data protection regulations including the UK GDPR and the Data Protection Act 2018.

We strive to embed privacy by design and default into our consultancy services and internal processes, maintaining transparency, accountability, and resilience in how information is accessed, stored, processed, and shared.

# 2. Legal Compliance

We are committed to complying with applicable data protection laws, including the European Union's General Data Protection Regulation (GDPR), the UK Data Protection Act, and other relevant national and international laws. Our approach to data protection is designed to meet or exceed these standards.

GDPR stands for General Data Protection Regulation. It has now been replaced by the UK GDPR and together with the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR) forms the main legislation relating to personal data in the UK.

# 3. Purpose & Scope

This policy applies to all personal data collected, processed, and stored by Julie Haywood Community Ventures Ltd during our business operations. It is relevant to all employees, sub-

contractors and associates who may have access to personal data. Personal data may be collected from clients, partners, employees, or other stakeholders as part of our business activities.

Julie Haywood Community Ventures Ltd operates to a data policy to ensure that data is:

3.1 Processed lawfully, fairly and in a transparent manner in relation to individuals (i.e. ensuring that there is a lawful basis for everything we do with personal data, that our use of data is underpinned by a privacy notice that reflects the organisation accurately, and that we adhere to our policy).

Our data policy aims to ensure that we process data with consent, with proportionality, with compliance and with purpose.

3.2 Collected for specified, explicit and legitimate **purposes** and not further processed in a manner that is incompatible with those purposes (i.e. stating clearly in our privacy notice what our purposes are, knowing what lawful bases we are using to make data processing legitimate and not doing anything extra with the information that we have collected).

3.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (i.e. not collecting or keeping information about our clients/employees/sub-contractors/associates that we do not need and making sure that we collect all the information that we do need).

3.4 Accurate and, where necessary, kept up to date (i.e. that we listen well to our clients and colleagues so that data we capture is correctly recorded, interpreted and used; we copy data exactly where this is required, we use adequate and secure databases and filing systems, we practice good data inputting, we file regularly, we double check data queries and we make changes immediately if our clients/colleagues tell you that their details have changed).

3.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (i.e. knowing how long we are legally obliged to keep information, and where there is no legal obligation, deciding how long we need to keep information and at the very least, putting our storage limits into our privacy notice, sticking to these times and making sure that we safely dispose of information when we say we will).

3.6 Processed in a manner that ensures appropriate security of personal data (i.e. that we know of any home working risks, we have secure office space, our IT systems and computers are protected, memory sticks & laptops are used securely, we train our staff and we ensure the right disclosures if there are any breaches of information regulations).

3.7 Appropriate use of Artificial Intelligence sets out principles for the responsible use of Artificial Intelligence (AI) tools and technologies within Julie Haywood Community Ventures Ltd. It ensures AI is used ethically, securely, and in alignment with our values, client commitments, and legal obligations.

# 4. Definitions

In order to ensure clarity of interpretation in this policy we offer the following definitions:

- **Personal Data**: Any information relating to an identified or identifiable individual, such as names, contact details, or any other data that can directly or indirectly identify someone.
- **Sensitive Data**: Personal data that is subject to more stringent protection under data protection laws, such as health information, racial or ethnic origin, political opinions, or religious beliefs.
- **Data Subject**: An individual whose personal data is processed.
- **Data Controller**: The entity that determines the purposes and means of processing personal data.
- **Data Processor**: The entity that processes personal data on behalf of the Data Controller.
- **Data Processing**: Anything that is done with personal data, including collecting, recording, keeping, working with it and giving it away
- **UK GDPR**: The United Kingdom General Data Protection Regulation
- **DPA**: The Data Protection Act 2018
- **ICO**: The Information Commissioner's Office. It is an independent body set up in the UK to uphold information rights
- **AI:** Artificial intelligence

# 5. Privacy Notice & Approach to Confidentiality

At Julie Haywood Community Ventures Ltd, we respect your privacy and are committed to protecting your personal information. We provide this summary 'Privacy Notice' to explain in outline how we collect, use, and protect the personal data you provide when you interact with us or use our services.

By engaging with our services, you agree to the practices described in this notice.

A full explanation of our Information, Data and Privacy Policy is provided from Section 1 onwards below.

We may collect the following types of personal information:

- **Contact Information**: Name, email address, phone number, and business address.

- **Professional Information**: Job title, company name, industry, and related business details.
- **Service-related data**: Information related to the services we provide, including project details, communication, and feedback.
- **Technical Data**: IP address, browser type, and usage data when you interact with our website or digital platforms.

We use the personal data we collect for the following purposes:

- To provide and improve our consulting services.
- To communicate with you regarding your inquiries, projects, and other business matters.
- To send you updates, newsletters, or other marketing materials (only if you have opted-in).
- To comply with legal and regulatory obligations.

We do not sell or rent your personal information to third parties. However, we may share your data with trusted third-party service providers who assist in delivering our services (e.g. hosting services, analytics providers). These third parties are required to keep your information confidential and are not allowed to use it for any other purpose.

We retain your personal data only as long as necessary for the purposes outlined in our policy or as required by law. When data is no longer needed, we will take steps to securely delete or anonymise it.

Depending on your jurisdiction, you may have certain rights regarding your personal data, including:

- The right to access, correct, or update your personal information.
- The right to request the deletion of your data, subject to certain conditions.
- The right to object to the processing of your data or request restrictions on its use.

If you would like to exercise any of these rights, or if you have any concerns about how we are handling your data please contact us at julie@juliehaywood.co.uk

We implement reasonable technical and organisational measures to protect your personal data from unauthorised access, use, or disclosure. However, no method of electronic transmission or storage is completely secure, and we cannot guarantee the absolute security of your data.

We operate to the principles and standards of confidentiality. If at any time your data has been subject to any kind of data protection breach we will follow the procedures outlined in our policy below.

We may use cookies and similar tracking technologies to enhance your experience on our website. These technologies help us analyse web traffic and improve the functionality of our site. You can choose to disable cookies through your browser settings, but this may affect some features of the website.

We may update this Privacy Notice from time to time. Any changes will be posted on this page with an updated "Last updated" date. We encourage you to review this Privacy Notice periodically to stay informed about how we are protecting your information.

# 6. Artificial Intelligence

## 6.1 Scope

Artificial intelligence (AI), in its broadest sense, is intelligence exhibited by machines, particularly computer systems. It is a field of research in computer science that develops and studies methods and software that enable machines to perceive their environment and uses learning and intelligence to take actions that maximize their chances of achieving defined goals. Such machines may be called AIs.

Some high-profile applications of AI include advanced web search engines (e.g., Google Search); recommendation systems (used by YouTube, Amazon, and Netflix); interacting via human speech (e.g., Google Assistant, Siri, and Alexa); generative and creative tools (e.g., ChatGPT, Apple Intelligence, and AI art). Collectively AI tools are called 'Generative AI'.

This policy applies to all staff, associates, and contractors using AI tools in the course of their work, including generative AI (e.g. chatbots, content creation), analytical AI (e.g. data modelling), and embedded AI features in software platforms.

## 6.2. Acceptable Use

AI may be used to support tasks such as:

- Drafting reports, templates, or communications
- Summarising documents or data
- Generating ideas, outlines, or visual aids
- Supporting research and benchmarking
- Enhancing productivity and client deliverables

All use must be:

- Transparent: Users must be clear when AI has contributed to outputs.
- Reviewed: AI-generated content must be checked for accuracy, relevance, and tone.
- Secure: No confidential or personally identifiable information (PII) may be entered into public or third-party AI tools.
- Compliant: Use must align with GDPR, client contracts, and sector-specific regulations.

## 6.3. Use of Microsoft Copilot

Microsoft CoPilot is Julie Haywood Community Ventures Ltd JULIE HAYWOOD COMMUNITY VENTURES LTD's AI platform of choice, as when used within Microsoft 365 (formerly Office 365), Copilot is protected by enterprise-grade security, compliance, and privacy controls that are built into the Microsoft 365 ecosystem.

- **Data Security**

  **Tenant Isolation**: Data stays within your Microsoft 365 tenant. Copilot respects the same access controls, permissions, and boundaries as the rest of your Microsoft 365 environment.

  **Encryption**: Data is encrypted both at rest and in transit using Microsoft's secure infrastructure.

- **Compliance and Governance**

  **GDPR and UK Data Protection Act**: Microsoft 365 Copilot is designed to support compliance with UK and EU data protection laws.

  **Audit and eDiscovery**: Copilot interactions can be governed by Microsoft Purview tools, enabling audit trails, retention policies, and eDiscovery where configured.

  **Data Residency**: Data handling aligns with your organisation's Microsoft 365 data residency settings.

- **Privacy and Control**

  **No Training on Data**: Microsoft states that Copilot interactions are not used to train foundation models.

  **Admin Controls**: IT admins can manage Copilot access, configure data boundaries, and apply DLP (Data Loss Prevention) policies.

  **User Transparency**: Copilot clearly indicates when content is AI-generated and encourages human oversight.

## 6.4. Prohibited Use

AI must not be used for:

- Making autonomous decisions that affect clients, staff, or stakeholders
- Replacing professional judgement in legal, clinical, financial, or safeguarding contexts
- Generating misleading, discriminatory, or offensive content
- Circumventing data protection, copyright, or ethical standards

- Producing content without recognition of the use of AI or to replace other more meaningful approaches to delivering products for clients (e.g. direct research, stakeholder engagement, on site observation, client interaction etc.)

Under no circumstances must any personally-identifiable data be uploaded and included in any AI tools or development work.

### 6.5. Identifying and Mitigating Bias in Outputs

Generative AI that is trained on pre-existing training data will generate outputs based on that data as processed by its internal algorithms. As a result, biases present in the training data could also be present in outputs produced by that Generative AI.

Generative AI often does not provide references for materials in its training data in outputs. Users should remain aware of this at all times when using Generative AI tools and should never assume that an output is unbiased or free of discrimination.

Outputs produced by Generative AI tools must, where applicable, be reviewed and fact-checked before further use by the user and by their line manager using reliable and up-to-date alternative sources as would be used when carrying out similar tasks without the use of Generative AI. In the event that biases or other inaccuracies are present, outputs must be amended and corrected as appropriate.

### 6.6 Verifying Accuracy of Outputs

Generative AI that is trained on pre-existing training data will generate outputs based on that data as processed by its internal algorithms. As a result, inaccuracies present in the training data could also be present in outputs produced by that Generative AI. For example, the training data could be accurate only up to a certain point in time.

Generative AI often does not provide references for materials in its training data in outputs. Users should remain aware of this at all times when using Generative AI and should never assume that an output is correct.

Outputs produced by Generative AI must, where applicable, be reviewed and fact-checked by the user and where relevant their line manager.

## 7. Role-Based Responsibilities

### 7.1 Managerial

Julie Haywood Community Ventures Ltd is not required to have a Data Protection Officer, as determined by the nature and scale of the data we hold, and all Managing Partners share

responsibility for Information Governance, Data Protection and Privacy. However, we have selected Julie Haywood for the aspects covered in this policy.

Julie is responsible for overseeing the implementation and enforcement of this policy, allocating resources, and ensuring that all employees receive adequate training on information governance.

All staff, contractors and collaborators are responsible for complying with this policy, following information handling procedures, and reporting any breaches or concerns regarding information security.

### 7.2 Subcontractors & Associates

Our sub-contractors and associates must. All policies are published on our website.

Our network of freelance professionals plays a vital role in our project delivery. They are expected to:

- Familiarise themselves with Julie Haywood Community Ventures Ltd Information Governance, Data and Privacy Policy standards and relevant client expectations.
- Operate in line with the requirements in this policy and within any contract of agreement that we have agreed with them.
- Report any issues, concerns, or queries promptly to a managing partner for assessment.

## 8. Data Use in our Business

We collect personal data from clients, employees, sub-contractors and associates, as part of providing our consulting services (we also collect Information about companies, organisations and public authorities but this information is not personal data). However, information about individuals working for and with us (employees, sub-contractors, associates) where they are individually identifiable and the information relates to them as an individual may constitute personal data.

Data in our business may be collected through:

- Client consultations
- Project documentation and reporting
- Surveys or feedback forms
- Communications (emails, calls, meetings)
- Employment records
- Etc.

The types of data we may collect include, but are not limited to:

- Contact information (name, address, phone number, email,)
- Employee information (qualifications, employment history, payee details, references etc.)
- Client-specific business information (service utilisation and activity reports, strategies, business plans, business-based risk, health and safety, clinical or operational reports, corporate reports etc.)
- Financial and commercial information (financial performance and activity, invoicing information, contracts and service specifications etc.)

We do not collect 'Sensitive Data' (e.g. ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation) on our data systems. We do however work with data controllers who may collect sensitive data in line with their data policy.

# 9. Data Controlling, Data Processing and Use of Data

Julie Haywood Community Ventures Ltd is a data controller for all data specific to our business and our staff (employees, associates and sub-contractors). As a data controller we have developed this policy and our business processes to ensure that we comply with our obligations to be lawful, transparent and proportionate in how we use data.

Julie Haywood Community Ventures Ltd is a data processor for any data specifically shared or delegated to us by our clients, for the purposes of undertaking client contractual business. In such circumstances our operation as a data processor must be reflected in a contractual agreement with the client, so that data controller 'permissions' around our business undertaking data processing on behalf of the client are clear.

In any case, personal data will only be processed for the following purposes:

- To provide consulting services to our clients
- To manage client, employee and colleague relationships (including quality assurance, and compliance with regulation, indemnity requirements etc.)
- To comply with legal or contractual obligations
- For internal record-keeping, such as invoicing, reporting, and project management
- For recruitment purposes (for prospective employees or contractors)
- To improve our services through feedback or research

Accountability obligations: We will comply with applicable UK GDPR accountability obligations, such as maintaining records and compliance.

9.1 Controller's instructions**:** We will only process personal data on instructions from a controller (unless otherwise required by law).

9.2 Processor contracts**:** We will enter into a binding contract with a data controller. This will contain the compulsory provisions that enable us to comply with our obligations as a processor under the contract.

9.3 Sub-processors**:** We will not engage another processor (i.e. a sub-processor) without the controller's prior specific or general written authorisation. If authorisation is given, we will put in place a contract with the sub-processor with terms that offer an equivalent level of protection for the personal data as those in the contract between us and the controller.

9.4 Notification of potential data protection infringements**:** you must notify the controller immediately if any of their instructions would lead to a breach of the UK GDPR or local data protection laws.

9.5 Co-operation with supervisory authorities: you are also obliged to cooperate with supervisory authorities (such as the ICO) to help them perform their duties.

As a specialist service provider, where Julie Haywood Community Ventures Ltd is processing data in accordance with its own professional obligations it will always be acting as the data controller. It will not agree to hand over or share data controller obligations with the client in this context.

We will not use personal data for purposes beyond those specified above without prior consent from the data subject.

Where we are interacting with a subcontractor or associate in our business we require them to sign an agreement which includes explanation of what we expect them to do with any information that we give them, or that they will collect on our behalf.

# 10. Data Security

We take appropriate technical and organisational measures to protect personal data from unauthorised access, disclosure, alteration, or destruction. These measures include:

- Data encryption (both at rest and in transit)
- Secure data storage solutions (Julie Haywood Community Ventures Ltd uses MS SharePoint for all storage requirements, which in turn is hosted, managed and maintained by a third party, Microsoft Certified, IT support provider).
- Access controls (ensuring only authorised personnel can access personal data). Julie Haywood Community Ventures Ltd grants access on a needs basis **exclusively at**

**project level** to associates and / or subcontractors who have a valid access requirement to client information. Subcontractors and associates have no access to Julie Haywood Community Ventures Ltd internal files, or other client-facing content which is not pertinent to their work, or covered under the scope of work outlined in either the Associate Agreement or Subcontractor Agreement.

- Information technology advice and support (including relevant to security) provision by externally commissioned experts
- Employee training on data protection best practices
- Appropriate technical and organisational measures to ensure the security of personal data, including protecting against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.

As outlined above, Julie Haywood Community Ventures Ltd aims to ensure that personal data is stored securely using modern software that is kept-up to date, taking account of Cyber Security considerations. Access to personal data is limited to personnel who need access and appropriate security is in place to avoid unauthorised sharing of information. Appropriate back-up and disaster recovery solutions are in place with secure cloud storage solutions.

Data security measures are applied to:

- All information systems purchased, developed and managed by/or on behalf of our organisation
- Organisational and business sensitive information
- Personnel/Staff information
- Photographic images, digital, text or video recordings
- Structured and unstructured record systems - paper and electronic
- Company information held on paper, mobile storage devices, computers, laptops, tablets, mobile phones, cameras and other devices.
- The processing of all types of information, including (but not limited to) organisation, adoption or alteration of information, retrieval, consultation, storage/retention or use of information, disclosure, dissemination or otherwise making available information for operational or legal reasons, alignment, combination/linkage, blocking, erasing or destruction of information.

Confidentiality and data protection on client site (such as a satellite clinic or a 3rd party service contractor) is the responsibility of the Data Controller (and as contracted suppliers we will act in accordance with data controller security requirements).

# 11. Data Storage, Retention and Disposal

A data record is any recorded information created or received in the course of the partnership's business, which needs to be retained to provide evidence of a business activity, transaction, or decision. Records can exist in any format or media, including paper, electronic, photographs and images, and audio and visual recordings.

When personal data is deleted, this should be done safely such that the data is irrecoverable.

Not all documents and files used in a business process will necessarily need to be captured into record keeping systems. Only those required to provide an adequate, accurate record of the work carried out or decisions made. The capture of relevant records into appropriate record keeping systems should be an integrated part of all company business processes.

The content of a record will primarily be determined by the purpose for which it is being created. Record keeping is a tool of professional practice and one, which should facilitate the care process. It is not separate from the process, and it is not an optional extra to be fitted in.

Records will be deleted either upon reaching the end of the lifecycle as outlined below or upon a legitimate request from a Data Subject (UK GDPR Article 17). Deletion includes all copies and back-ups. Examples of records that could be deleted are; physical media, data files materials, which include (but are not limited to) backup media, printed listings, and paper.

In our business personal data will be retained for no longer than 7 years, unless otherwise required by law. After this period, personal data will be securely deleted or anonymised.

For client-controlled data, retention periods may vary depending on the nature of the consulting project and any specific contractual or legal obligations. We look to Client Data Controllers to advise on their requirements.

All company records are subject to the provision of the General Data Protection Regulation (UK GDPR, post Brexit) as enacted in May 2018 and incorporated into the Data Protection Act 2018. Principle 5 - as set out in Article 5 of the UK GDPR, states that personal data shall be:

*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');*

In the event that our company is served with any subpoena or request for documents, or any employee becomes aware of a governmental investigation, or audit concerning the company or the commencement of any litigation against or concerning such employee shall inform the lead Partner and any further disposal of documents shall be suspended until such time as the lead Partner, with the advice of counsel, determines otherwise.

We shall take such steps as is necessary to promptly inform all relevant employees, associates, sub-contractors of any suspension in the further disposal of documents.

# 12. Data Subject Rights

Under data protection laws, individuals have the following rights concerning their personal data:

- **Right to Access:** The right to request access to personal data we hold about them.
- **Right to Rectification:** The right to request correction of any inaccurate or incomplete personal data.
- **Right to Erasure (Right to be Forgotten):** The right to request deletion of personal data, subject to certain conditions.
- **Right to Restrict Processing: The** right to request that we limit the processing of their personal data.
- **Right to Object:** The right to object to the processing of personal data for specific purposes, including direct marketing.
- **Right to Data Portability:** The right to request a copy of their personal data in a commonly used, machine-readable format.

Every data subject is entitled to see what information an organisation holds about them. They are **NOT** entitled to see anyone else's information. Anyone who wants to see their information can ask by putting their request **in writing or verbally,** however it is recommended that these be in written form to ensure clarity and to create an audit trail**.** This is called a subject access request (SAR) and Julie Haywood Community Ventures Ltd Ltd has one calendar month to respond to any such request.

To exercise these rights, individuals can contact Alex Robertson using the contact information provided below.

Data subjects have other rights beyond the right to apply for access to their data. These rights include:

- The right to prevent their personal data being processed for direct marketing.
- The right to give written notice requiring us not to take any automated decisions using their personal data or to stop any use of their data in our profiling.

- Where personal data is inaccurate the individual concerned can ask us to correct it and if we do not they can apply to the court to make a decision.
- If an individual suffers damage because of what employees of us do with their personal data they are entitled to apply for compensation (which would be considered through lawful processes).
- The right to be forgotten – this applies only if there is no lawful reason for keeping a person's data.
- The right to data portability – if a data subject asks us to transfer all the information about them (that we have been given) to someone else, we must do this.
- The right to object to processing.

If any employee, sub-contractor or associate is worried about how we handle the information that they gave to us or received from us they can make a complaint through our complaints process, which we will investigate and action accordingly.

# 13. Data Sharing

We are enabled to share data with organisations through four identified routes:

13.1 With organisations and individuals that work or provide a service to Julie Haywood Community Ventures Ltd by contractual agreement (and after assurances about compliance with UK data regulations). These individuals/organisations will be classed as our data processors. This includes providers of data platforms in which we may share or store data (e.g. Dropbox, Teams, SharePoint etc.)

13.2 With organisations to which Julie Haywood Community Ventures Ltd is legally obliged to give personal data (e.g. HMRC etc.)

12.3 With organisations with which Julie Haywood Community Ventures Ltd may be processing personal data either for a common purpose or each for their own purposes (e.g. Twitter, LinkedIn and Google), subject to satisfying ourselves that we are applying the right data sharing principles.

13.4 With organisations like the police or solicitors who ask for personal data to be disclosed to them. They are not automatically entitled to the data and we will satisfy ourselves that we are applying any relevant data sharing exemptions accurately before handing data over.

13.5 In case of emergency – a life threatening situation – it is acceptable to disclose information that is needed (and only the information that is needed, no more) without adherence to usual data protections practices (e.g. seeking consent) and we would always

record any such disclosure. For any other data sharing there must be an information sharing agreement in place based on an individual's consent, a legal obligation or an exemption.

## 14. International Data Transfers

The UK GDPR's prohibition on transferring personal data applies equally to processors as it does to controllers. This means we ensure that any transfer of data outside the UK complies with the UK GDPR's transfer provisions (i.e. adequacy/partial adequacy/extension to EU/UK GDPR rules/sign up to the international Data Privacy Framework Programme).

Our business use of Apple and PC products is compliant with UK GDPR rules by virtue of the adherence to GDPR international adequacy. Our use of Dropbox and Survey Monkey is also compliant by virtue of those companies operating to the UK/EU Extension.

Our core SharePoint sites are hosted on UK-based servers, and so are not subject to this clause.

If we transfer personal data outside the jurisdiction in which it was collected (e.g., across borders either by direct transfer or by use of a technical platform whose data processing or storage systems are outside of the UK), we will ensure that such transfers are carried out in compliance with relevant data protection laws and that adequate safeguards are in place to protect the personal data.

## 15. Data Breaches and Incident Reporting / Management

Managing Partners, employees, sub-contractors and associates of Julie Haywood Community Ventures Ltd must not look at personal data just because someone outside the organisation, associate or sub-contractor role asks them to do it or for personal interest. This action is called 'procurement' and any individual that does so can be prosecuted. We will not look at people's personal data when we do not need to.

We will also not destroy personal data in advance of sharing it with anyone who has made a request to see it. This activity would also be unlawful.

We will ensure that we do not talk to anyone outside our business about our clients or give anyone outside of our business operation personal data that we hold for which we do not have permission to share.

Should any breach of data regulations be suspected (loss, unlawful destruction, unauthorised disclosure, unlawful processing etc.) we require all employees, sub-contractors and associates to follow these steps:

- Notification must be made to our lead Managing Partner (Alex Robertson) immediately
- Alex will immediately instigate an investigation (under the requirement of our complaints policy) ascertaining nature, scale, impact etc.
- If a data breach is confirmed following investigation Alex will notify the data controller (if the breach relates to information collected, processed or shared by them or if it is data about them)
- Alex will consider if the breach has to be reported to the ICO
- Alex will also consider whether any action/support/intervention is required for any employee, sub-contractor or associate involved in the breach

## 16. Training and Awareness

We aim to ensure compliance in relation to our obligations under the UK-GDPR rules so that anyone acting under the authority of Julie Haywood Community Ventures Ltd, with access to personal data does not process that data unless they are permitted to do so by our business. We require all employees, sub-contractors and associates to be trained on how to handle personal data.

We provide annual training for employees regarding information governance policies, procedures, and best practices delivered by external experts in data law and compliance practices. We require all employees to participate in data training.

## 17. Compliance and Monitoring

We have implemented annual assessments of compliance with this policy to identify areas for improvement in information governance practices. Findings from our annual compliance assessments are reported to our Board for onward action.

## 18. Conclusion

Julie Haywood Community Ventures Ltd is committed to maintaining high standards of information governance to protect sensitive data and ensure compliance with data protection laws. This policy reflects our dedication to effective information management and security within our organisation.

## 19. Contact Information

For questions or concerns regarding this policy, or to exercise data subject rights, please contact us at: julie@juliehaywood.co.uk

**October 2026**
**Julie Haywood Community Ventures Ltd**