



INFORMATION POLICY

Protecting your data



02 DECEMBER 2024
HOUSE OF DAMNATION CIC
Old Bakery Studios, Blewett's Wharf, Malpas Road, Truro TR1 1QH



"Privacy is a human right. Encryption is a human right.
No qualifiers"

- Sarah Jamie Lewis, *Trans Privacy Researcher*



Contents

Purpose	1
Scope	1
Accessibility	2
Principles	3
Definitions	4
Accountability and Responsibilities.....	1
Information Handling Process	3
Processes	4
Unacceptable Behaviour	9
Monitoring and Improvement	10
Policy Review	11
Appendix 1 – Frequently Asked Questions (FAQs)	i
Appendix 2 – Data Retention Schedule	iii
Appendix 3 – Version Control.....	vi

Purpose

The purpose of this policy is to ensure that House of Damnation CIC manages all information ethically, securely, and transparently, in accordance with legal requirements and recognised good practice.

We are committed to protecting the confidentiality, integrity, and availability of all information we hold, whether digital, physical, personal, operational, or creative, and to using that information responsibly in support of our mission, values, and community.

This policy underpins compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the principles of ISO 27001 (Information Security Management). It also reflects expectations set by the Information Commissioner's Office (ICO), the Charity Excellence Framework, and the Good Business Charter.

Implementation of this policy mitigates legal, reputational, and ethical risks associated with information handling and ensures that HoD operates with accountability and public trust.

Compliance is monitored through internal reviews and Board assurance reports to ensure ongoing effectiveness.

Scope

This policy applies to all staff, volunteers, Board members, contractors, and partner organisations who handle or have access to information belonging to House of Damnation CIC. It covers all information assets, including personal data, organisational records, creative content, financial data, and operational materials — whether held electronically, on paper, or in any other format.

The policy applies to information generated, received, or stored by House of Damnation CIC in the course of its work, including data held on mobile devices, cloud platforms, email systems, and external storage media. It also extends to materials created for artistic, promotional, or public purposes such as event photography, video, and digital media.

This scope ensures that all information handling activities comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and recognised information security standards such as ISO 27001. It mitigates risks relating to data loss, unauthorised disclosure, misuse of creative intellectual property, and reputational harm. Compliance with this policy is monitored through staff and volunteer training completion, data protection audits, and Board assurance reporting. Supporting documents include the Data Retention Schedule, Privacy Notice, and Acceptable Use of IT and Communications Guidance.

Accessibility

House of Damnation CIC is committed to ensuring that all information it holds, creates, or shares is accessible, understandable, and usable by everyone who needs it. We recognise that accessibility is a legal, ethical, and practical requirement, not an optional feature.

We follow the principles of the Equality Act 2010, the NHS Accessible Information Standard, and Article 12 of the UK General Data Protection Regulation (UK GDPR), ensuring that individuals can access information about how their data is used in a clear, transparent, and inclusive way.

Alternative formats, translations, or other reasonable adjustments will be provided where practicable. Requests for accessible information can be made via any of our usual communication routes (see the *Contact Us* section of our website or appendix).

Responsibility for maintaining accessibility across all information systems, publications, and communications rests with the Communications Director (Data Protection Lead), who ensures compliance through annual reviews and reporting to the Managing Director and Board.

Barriers, requests, and accessibility incidents are logged within the Organisational Learning Log and reviewed through the Risk Register to support continuous improvement and equitable access to information.

Principles

Our approach to information management is guided by our core organisational values (Diligence, Authenticity, Magnanimity, and Neutrality) and by the seven principles of data protection set out in the UK GDPR: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity/confidentiality.

These values ensure that all information handled by House of Damnation CIC is treated with respect, care, and accountability.

- **Diligence:** We collect, store, and share information responsibly, ensuring accuracy, security, and lawful processing at every stage.
- **Authenticity:** We communicate honestly and transparently about how information is used, and ensure that records and data accurately represent reality.
- **Magnanimity:** We learn from mistakes, report breaches or errors openly, and use them as opportunities for growth and improvement.
- **Neutrality:** We handle information impartially, without bias, discrimination, or misuse of power.

These principles are supported by the ISO 27001 information security pillars of confidentiality, integrity, and availability. They underpin our compliance with the Data Protection Act 2018, UK GDPR, and our commitment to ethical and inclusive governance. Adherence to these principles is reviewed through regular data protection audits, staff training completion, and Board oversight of any reported breaches or incidents.

Definitions

For the purposes of this policy, the following definitions apply:

- **Information:** Any recorded data, in any form (digital, paper, audio, visual, or verbal), that is created, received, or stored by House of Damnation CIC in the course of its work.
- **Information Asset:** A body of information, defined and managed as a single unit, that has recognisable value to the organisation — such as membership lists, event records, or creative content archives.
- **Personal Data:** Any information relating to an identified or identifiable living individual (a *data subject*). Examples include names, contact details, images, or opinions linked to a person.
- **Special Category (Sensitive) Data:** Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health information, or a person's sex life or sexual orientation.
- **Processing:** Any operation performed on data — including collecting, storing, using, sharing, or deleting it — whether by automated or manual means.
- **Data Breach:** Any security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Data Subject Rights:** The rights of individuals under the UK GDPR, including access, rectification, erasure, restriction, portability, objection, and the right not to be subject to automated decision-making.
- **Anonymisation:** The process of removing or altering personal identifiers so that individuals cannot be identified, directly or indirectly.
- **Pseudonymisation:** Replacing identifying data with artificial identifiers or pseudonyms while retaining a means of re-identifying data if necessary.

- **Data Controller:** The person or organisation that determines the purposes and means of processing personal data (for HoD, this is House of Damnation CIC).
- **Data Processor:** A person or organisation that processes data on behalf of the data controller.
- **Retention Period:** The length of time data will be stored before secure deletion or anonymisation, as defined in HoD's Data Retention Schedule.
- These definitions are consistent with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018, and will be reviewed annually or when legislation changes.

Accountability and Responsibilities

House of Damnation CIC recognises that accountability for information governance sits at every level of the organisation. While specific duties are delegated to named roles, overall responsibility for compliance with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 rests with the organisation as Data Controller.

Managing Director

- Holds overall accountability for information governance, lawful processing, and data protection compliance.
- Ensures that information risks, incidents, and serious data breaches are reported to the Board and, where appropriate, to the Information Commissioner's Office (ICO).
- Leads on creating a culture of transparency, security, and continuous improvement in information handling.
- Retains accountability for ensuring that all individuals' information rights under UK GDPR Articles 12–22 are respected and enabled through organisational systems and practices.

Communications Director (Data Protection Lead)

- Acts as the operational lead for data protection and information management.
- Maintains the Data Protection Register, coordinates Data Protection Impact Assessments (DPIAs), and ensures timely reporting and investigation of breaches or near misses.
- Coordinates and responds to all information-rights requests, ensuring that responses meet statutory timescales and ICO guidance.
- Provides annual assurance reports to the Managing Director and Board, highlighting risks, trends, and compliance performance.

- Ensures that public-facing information (e.g., privacy notices, consent forms, and policies) remains accessible, accurate, and up to date.

Board of Directors

- Provides independent oversight and assurance that House of Damnation CIC meets its legal and ethical obligations regarding information management.
- Reviews information-governance reports, risks, and incidents as part of the Board Assurance Framework.
- Approves major updates to this policy and associated procedures.

All Staff, Volunteers, and Contractors

- Must understand and follow this policy and complete relevant data-protection training.
- Are personally responsible for safeguarding information they handle and for reporting any data loss, breach, or concern immediately to the Communications Director (Data Protection Lead).
- Must only collect, use, or share information that is necessary for their role and within the boundaries of this policy.

Third Parties and Partner Organisations

- Where external partners or contractors process information on behalf of HoD, they must do so under a written agreement that meets UK GDPR requirements.
- HoD will ensure that any third-party processor provides appropriate technical and organisational measures to protect data and enable individuals to exercise their information rights.

Records of training completion, breach investigations, information-rights requests, and DPIAs will be maintained as evidence of compliance and reviewed quarterly through the Risk Register and Organisational Learning Log.

Information Handling Process

House of Damnation CIC is committed to the responsible collection, processing, storage, and sharing of personal and non-personal data in compliance with applicable laws, including the UK GDPR and the Data Protection Act 2018. This Information Policy ensures that all data activities within the organisation are conducted transparently, securely, and ethically, fostering trust among our customers, employees, and stakeholders.

Key commitments include:

1. Transparency and Accountability

- We ensure that individuals are informed about how their data is collected, used, stored, and shared through clear and accessible privacy notices.
- We take full responsibility for maintaining compliance with legal and regulatory standards.
- For website visitors, we provide detailed privacy notices and cookie banners to ensure they understand how their data is used. Consent is requested for non-essential cookies and tracking technologies, and users can adjust their preferences at any time.

2. Data Minimisation

- We collect and retain only the data necessary for specific, legitimate purposes and ensure that it is handled appropriately.

3. Consent and Rights

- We respect individuals' rights regarding their data, including access, rectification, erasure, and objection.
- Consent for processing is obtained where required and can be withdrawn at any time.

4. Security and Integrity

- We implement robust technical and organisational measures to protect data from unauthorised access, loss, or breaches.
- Security protocols are regularly reviewed and updated to align with best practices.

5. Data Retention and Disposal

- Data is retained only for as long as necessary, in line with our Data Retention Schedule, and securely disposed of when no longer needed.

6. Third-Party Engagement

- We ensure that third-party providers handling data on our behalf comply with equivalent data protection standards through robust contractual agreements.

7. Incident Response

- We are prepared to respond promptly to data breaches or incidents, ensuring appropriate containment, investigation, and notification to affected individuals and regulatory authorities.

This policy reflects our ongoing commitment to safeguarding personal data and fostering a culture of respect, privacy, and trust within our organisation.

Processes

This section outlines the procedures and practices that House of Damnation CIC follows to implement the principles and commitments of this policy. These processes ensure compliance with legal obligations and the effective management of data throughout its lifecycle.

1. Data Collection and Consent Management

• Data Collection

Data is collected only for specified, legitimate purposes via clearly communicated mechanisms (e.g., forms, online platforms).

Privacy notices are provided at the point of data collection, detailing how data will be used, the lawful basis for processing, and the rights of data subjects.

- **Consent Management**

Consent is obtained in a clear, affirmative manner (e.g., opt-in checkboxes) for processing activities requiring consent.

Records of consent are maintained to demonstrate compliance.

Withdrawal of consent is facilitated through simple mechanisms, such as email requests or account settings.

- **Cookie Management**

Our website uses cookies to improve functionality, analyse usage, and support marketing campaigns.

Visitors are notified about cookie usage through a cookie banner when they first visit the site. Consent is required for non-essential cookies (e.g., marketing or analytics cookies).

Users can manage their cookie preferences through the website's "Cookie Settings" link, accessible in the footer.

- **Website Analytics and Third-Party Tools**

We use tools like Google Analytics to collect anonymised data about website usage, such as page views, session durations and navigation paths.

These tools may use cookies or other identifiers to track user activity. Data collected is processed in compliance with this policy and applicable laws.

- **Online Forms and Contact Requests**

Data submitted via website forms (e.g., contact forms or surveys) is used solely for the stated purposes and stored securely.

Consent is obtained before using the data for marketing or additional purposes.

2. Data Retention and Disposal

- **Retention Periods**

Data is retained only for as long as necessary to fulfil its intended purpose, in accordance with the organisation's Data Retention Schedule (see appendix 1).

Periodic audits are conducted to identify and securely delete data that is no longer needed.

- **Secure Disposal**

Physical records are shredded or incinerated.

Digital data is permanently deleted using appropriate software, ensuring it cannot be recovered.

3. Data Sharing and Third-Party Management

- **Third-Party Agreements**

Data shared with third-party processors is governed by contracts that ensure compliance with data protection laws.

Third parties are vetted to confirm they maintain adequate security measures.

- **Cross-Border Data Transfers**

Data transfers outside the UK are conducted only with appropriate safeguards, such as Standard Contractual Clauses or adequacy decisions.

4. Incident Response

- **Reporting Breaches**

All data breaches must be reported immediately to the designated Data Protection Officer (DPO) or equivalent.

Employees are trained to recognise and escalate potential breaches.

- **Investigation and Containment**

Breaches are investigated promptly to identify the cause, mitigate risks, and implement corrective actions.

Affected data subjects and the Information Commissioner's Office (ICO) are notified within 72 hours when required by law.

- **Incident Log**

All breaches are recorded in a log, detailing the nature, impact, and resolution of each incident.

5. Data Access and Individual Requests

- **Access Requests**

Data subjects can request access to their personal data by submitting a request to the DPO.

Requests are fulfilled within one month, free of charge, unless they are complex or excessive, in which case an extension or fee may apply.

- **Other Requests**

Requests for rectification, erasure, restriction, or data portability are handled in accordance with the rights outlined in this policy.

Objections to processing are reviewed and respected unless overridden by compelling legitimate grounds.

6. Monitoring and Improvement

House of Damnation CIC is committed to ensuring that this Information Policy is consistently applied, effective, and reflective of best practices and legal requirements. Regular monitoring and improvement processes ensure the policy remains relevant and operationally robust.

Monitoring

1. **Routine Audits**

Regular audits of data collection, storage, processing, and disposal practices are conducted to ensure compliance with this policy and applicable legislation.

Audits include:

- Data retention practices.
- Incident response handling.
- Third-party data processing agreements.

2. **Employee Compliance**

Periodic reviews of employee adherence to data handling responsibilities.

Training records and assessments are monitored to ensure staff remain informed and competent.

3. **Feedback Mechanisms**

Feedback from employees, customers, and stakeholders on the implementation of the policy is actively sought and reviewed.

4. **Incident Tracking**

Analysis of data breaches, complaints, and subject access requests to identify recurring issues or gaps in compliance.

Improvement

1. **Policy Updates**

Updates are made in response to:

- Changes in legal or regulatory requirements (e.g., updates to UK GDPR).
- Advancements in technology or best practices.
- Organisational changes that affect data handling processes.

2. **Training and Awareness**

Additional training is provided when significant updates or improvements are made to the policy.

Awareness campaigns are conducted to ensure all stakeholders understand their roles in implementing the updated policy.

3. **Continuous Feedback Loop**

Feedback from monitoring activities is used to:

- Improve processes.
- Address gaps or inconsistencies.
- Enhance the overall data governance framework.

Reporting

Findings from monitoring activities are documented and shared with senior management. This ensures accountability and enables informed decision-making regarding data governance priorities.

Unacceptable Behaviour

We are committed to handling all data requests and enquiries respectfully and fairly. In return, we expect the same courtesy from individuals engaging with us. House of Damnation CIC will not tolerate abusive, threatening, discriminatory, or aggressive behaviour under any circumstances.

Where communication becomes unreasonable or harassing, we reserve the right to:

- Limit or restrict contact to written correspondence;
- Cease communication where further discussion would serve no productive purpose; and
- Refer the matter to the appropriate authorities if necessary.

These measures are taken only to protect the wellbeing of our staff, volunteers, and contractors, while ensuring the fair and lawful management of all data matters.

Monitoring and Improvement

House of Damnation CIC is committed to maintaining the highest standards of data protection. To ensure this policy remains effective, it is regularly monitored, reviewed, and improved through the following activities:

Data Monitoring

- All data protection activities, including incidents, subject access requests, and breaches, are logged and reviewed to identify trends, recurring issues, and areas for improvement.
- Findings are documented within the organisational learning log and reported to senior management.

Audit and Compliance Reviews

- Regular internal audits assess compliance with the UK GDPR, the Data Protection Act 2018, and this policy.
- These reviews evaluate data handling, retention, security measures, and third-party agreements.

Policy Improvement

- Lessons learned from audits, incidents, and legislative changes inform updates to this policy and related procedures.
- Additional staff training and awareness sessions are provided when significant changes occur.

Board Oversight and Transparency

- An annual summary of data protection performance, incidents, and improvement actions is presented to our Board to ensure accountability and continuous improvement.
- The updated policy is made available on our website to maintain transparency with our community and stakeholders.

Policy Review

This Information Policy will be reviewed annually to ensure it remains effective, relevant, and aligned with our values and objectives. A log of amendments and updates can be found at Appendix 3.

Appendix 1 – Frequently Asked Questions (FAQs)

- **What is personal data?**

Personal data is any information that can identify you directly or indirectly – for example, your name, contact details, or information about how you interact with us.

- **Why do you collect my data?**

We collect information so we can provide our services safely, communicate effectively, and meet legal and operational requirements. We only collect what we genuinely need and use it responsibly.

- **Do you share my data with anyone else?**

Sometimes, yes; but only with your express permission and only with trusted third parties who help us deliver our services or meet legal obligations. These organisations are bound by strict contracts to keep your data safe and never use it for their own purposes.

- **How long do you keep my information?**

We keep data only for as long as it's needed for the reason it was collected. Once that time has passed, it's securely deleted or anonymised, following the Data Retention Schedule in this policy (see appendix 2).

- **Can I see what information you hold about me?**

Yes. You have the right to request a copy of your data by making a *Subject Access Request*. We'll respond within one month and provide your information in an accessible format.

- **What if my information is wrong or out of date?**

You can ask us to correct or update any inaccurate or incomplete data. We'll make the change promptly and confirm once it's done.

- **Can I ask for my data to be deleted?**

Yes. You have the right to request deletion of your data under the “right to be forgotten”. We’ll comply unless we’re required to keep the information for legal or operational reasons, which we’ll explain clearly if that is the case.

- **What happens if there’s a data breach?**

If a data breach occurs, we’ll act immediately to contain it, assess the risk, and notify the Information Commissioner’s Office (ICO) and any affected individuals when required. We’ll also review what happened to prevent it recurring.

- **Who is responsible for data protection at House of Damnation CIC?**

We have a designated person responsible for data protection measures across the organisation. All staff, volunteers, and contractors are trained to handle information responsibly and report any concerns straight away.

- **What can I do if I’m unhappy with how you’ve handled my data?**

Concerns can be raised in line with our Feedback Policy. If you remain dissatisfied, you can contact the Information Commissioner’s Office for independent advice.

- **Is my information safe when I contact you or use your website?**

Yes. We use secure systems, encrypted connections, and restricted access to protect all personal data. We also review our security practices regularly to stay up to date with best practice.

- **Can I change my communication or consent preferences?**

Absolutely. You can withdraw consent or update your communication preferences at any time by contacting us directly. We’ll update your records and confirm once the change has been made.

Appendix 2 – Data Retention Schedule

This schedule outlines the retention periods for various types of data processed by House of Damnation CIC and provides guidance for secure disposal when the retention period ends. It is designed to comply with the UK GDPR, Data Protection Act 2018, and other applicable regulations.

Data Category	Retention Period	Rationale	Disposal Method
Employee Records	6 years after employment ends	Legal compliance (e.g., discrimination claims).	Secure shredding or digital erasure.
Recruitment Data (Unsuccessful)	6 months	Compliance with Equality Act 2010 recommendations.	Secure shredding or digital erasure.
Customer Contact Details	Until service termination + 1 year	For follow-up inquiries or potential disputes.	Digital erasure.
Financial Records	6 years	HMRC requirements under tax law.	Secure shredding or digital erasure.
Invoices and Payments	6 years	Compliance with UK tax regulations.	Secure shredding or digital erasure.
Special Category Data	Minimum period necessary	Reduce risks due to sensitivity (e.g., health data).	Secure shredding or digital erasure.
Incident Logs (e.g., breaches)	3 years	Regulatory reporting and internal reviews.	Secure shredding or digital erasure.

Marketing Consents	Until consent is withdrawn	UK GDPR compliance for consent-based activities.	Digital erasure.
Website Analytics Data	12 months	Useful for monitoring trends, not long-term storage.	Digital erasure.
Contracts and Agreements	6 years after termination	Limitation Act 1980 (contractual dispute period).	Secure shredding or digital erasure.
Training Records	3 years after training completion	Proof of compliance or qualification validity.	Secure shredding or digital erasure.
Customer Feedback and Surveys	12 months	Operational insights, no long-term need.	Digital erasure.
Risk Assessments	3 years from assessment date	Health and Safety Executive (HSE) guidelines.	Secure shredding or digital erasure.
Essential Cookies	Session Duration	Support core website functions	Automatically removed when closing browser
Analytics Cookies	Up to 12 months	Track anonymised browsing data	Expiration set by analytics platform. Users can also delete from browser.

Marketing Cookies	As per consent settings	Deliver targeted advertisements	Expiration set by analytics platform. Users can also delete from browser.
-------------------	-------------------------	---------------------------------	--

Notes

1. **Retention Adjustments:** If a legal case, audit, or investigation is ongoing, relevant records may need to be retained beyond the stated period.
2. **Anonymised Data:** When possible, data that no longer requires personal identifiers should be anonymised rather than deleted, as it reduces risks while preserving insights.
3. **Third-Party Records:** Ensure any third parties handling your data adhere to similar retention standards.

Appendix 3 – Version Control

Version	Date	Author	Approver	Summary of Changes	Next Review
1.0	Dec 2024	Managing Director	HoD Board	Document Created	Dec 2025

© House of Damnation CIC 2025

House of Damnation CIC is a registered company limited by guarantee in England and Wales. Company No. 15322977

