Cartwheel Arts

Information Governance Policy and Procedures

To protect Cartwheel Arts' Trustees, staff, colleagues, participants, customers, and everyone we work with, and our business, by following good Information Governance principles following the General Data Protection Regulations EU law (GDPR).

Contents

Introduction and our Information Governance Framework

Personal privacy is taken very seriously at Cartwheel Arts. The purpose of this document is to protect our Trustees, staff, colleagues, participants, customers, and everyone we work with, and our business by following good Information Governance principles, which make sure that all information (personal and commercial) is collected, stored, used, shared, and disposed of safely and securely, in line with legal requirements and best practice.

Everybody working at, or volunteering for, Cartwheel Arts, is responsible for good information governance. The policy must be always adhered to including when working at the office, from home or any other private or public location.

For the purpose of this document, the term 'Cartwheel representatives' will refer to any staff member, volunteer, Trustee, freelancer or contractor, or other individual who is working or volunteering on behalf of Cartwheel Arts.

Our Information Governance Framework consists of this document and its appendices and annexes and the following linked reference documents:

- Social Media Guidelines
- ICT/E policies
- Image Consent form
- Photographer guidelines
- Confidentiality policy
- Contracts for staff and freelance contractors

The Information Governance policy complies with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations 2003

Information Governance is about making sure that all the information we come into contact with at Cartwheel – whether it's about people or about business matters – is handled properly throughout its "data journey".

Information Governance applies to all information, in any format, including hard copy and electronic copy, as well as photographs, videos, telephone or sound recordings, not just written or typed information.

Information is a valuable asset, especially the personal information that our participants and colleagues entrust Cartwheel Arts with, and we must handle it with respect and keep it secure. The consequences of an incident that results in personal or business information falling into the wrong hands can include serious harm and distress to individuals whose data is breached and harm to Cartwheel Arts. The business could be prosecuted and have large fines imposed, as well as serious reputational damage.

Cartwheel Arts will implement information governance effectively and ensure the following:

- Information will be protected against unauthorised access;
- Confidentiality of information will be assured;
- Integrity of information will be maintained;

- Regulatory and legislative requirements will be met;
- Information governance training will be available to all staff as necessary to their role;
- All breaches of confidentiality and information security, actual or suspected, will be reported and investigated.

All staff will receive in-house training as part of their induction. External training will be available on request.

Who is responsible for Information Governance?

Everybody working at, and for, Cartwheel is responsible for good Information Governance (IG). These procedures apply to all staff members, freelancers, colleagues, including permanent, temporary and fixed-term colleagues, contractors, consultants, people on work experience placements, volunteers and Board and committee members and advisors.

Cartwheel Arts are registered with the Information Commissioners Office. The data processed by Cartwheel Arts means that a Data Protection Officer is not required. However, as is good practice, the named lead for the organisation is the Operations and Development Manager, who is responsible for:

- Developing and implementing information governance procedures and processes
- Raising awareness and providing advice and guidelines about IG to all staff, volunteers and freelance contractors
- Ensuring that all data flows, internal and external are periodically checked against the IG framework
- Ensuring participants are appropriately informed about Cartwheel Arts' information handling activities

Personally Identifiable Information (PII)

Cartwheel Arts collects, stores and processes different type of personally identifiable information as part of the regular day to day operations and management of the charity.

- Trustees
- Employees
- Volunteers
- Apprentices and student placements
- Participants
- Customers
- Partners
- Funders
- Audiences
- Other stakeholders can include businesses, suppliers, other charities, public bodies, etc.

Our data retention table (see Appendix 2) outlines in detail:

1. What data we hold
2. For how long
3. The lawful basis for holding that data
4. Who takes ownership
5. The format it is stored (digital/printed)

The conditions for processing data:

We hold personal information for one of six reasons, which are:

- Consent - people have positively and clearly given their consent
- Legal Obligations - there is a legal reason that we have to do this e.g. HMRC, accident reports for health and safety records
- Contractual – i.e. Funder requirements, in order to fulfil a contract / service with the individual (i.e. access to an arts course)
- Legitimate Interest – we are using people's data in a way that they would reasonably expect. For example, if someone has attended a previous creative writing project and we contact them to let them know about similar projects in the future
- Vital Interest – very limited in scope and generally only applies in matters of life and death i.e. Safeguarding and individuals at risk of immediate harm
- Public Task – doesn't tend to apply to VCSE organisations as tends to be statutory and public bodies

For most of Cartwheel Arts activities the condition for processing would be Legal Obligations, Contractual (i.e. funding requirements) or Legitimate Interest.

We uphold the 7 GDPR Principles as follows:

1. We process data lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')
2. We collect data for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation')
3. We only collect data that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
4. We ensure data is accurate and, where necessary, kept up to date; every reasonable step is taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
5. We keep data 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')
6. We process data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')
7. We are responsible for and can demonstrate compliance with the above principles ('accountability')

4 - The Information Journey

This diagram illustrates the stages that information goes through on its "journey" at CWA, starting with when we collect it. Each stage carries its own risks and requires careful consideration.

5 - Collecting Information

The people the information is about must be told clearly why we are collecting their information, how we will use it, and how we will share it with, and sometimes they must give us their consent for the collecting and processing or their information.

5.1. Data Protection Impact Assessments (DPIAs)
Privacy Impact Assessments identify risks whenever we plan to collect, use or share personal information as part of a project, or when we plan to change the way we handle personal information. A PIA helps to assess the severity of the risk, decide how they should be managed and put processes in place to control them. We have carried out a DPIA that interrogates how we process data during our projects (see Appendix 3)

5.2. How we collect personal information:

- Forms should be designed to only collect the minimum amount of information we need and include a Data Protection statement if collecting personal information (see below.)
- **Notes in writing, on management systems, in emails or via text/WhatsApp** should always be factual and only include the minimum needed. The person/people being written about have a right to access the notes/emails, so they should be written with respect, with this in mind.

5.3. How we tell people about collecting their information:

- **Cartwheel's Privacy Notice** is on our website. It explains how we process personal information; the way we collect it, how we use our records and what rights people have in relation to their own information.
- **Our Data Protection Statement:** any staff member, freelance practitioner, Trustee or volunteer collecting data is responsible for communicating how that information will be used and must be ensure they have communicated our Data Protection Statement adequately. Methods of communicating the Data Protection Statement include – verbally communicating when handing out forms, including a written description on Personal Information forms, handing out our GDPR postcards, or other, easy-read versions.

Verbal statement to those providing information: “The information you provide will be stored and used in accordance with the law. It will be used for Cartwheel Arts purposes only and it’s important that you feel fully informed before providing your information so if you have any questions or concerns about why we are asking for any information, please let us know at any time.”

5.4 Data Protection Clause is included in all staff and freelance contracts.

“By signing this contract, you are confirming you have read our GDPR Guidance for Freelancers and commit to upholding the GDPR principles as outlined in our Privacy Notice. If you have any questions or concerns you must contact a member of the Cartwheel Arts staff team immediately.”

Cartwheel Arts shall take all reasonable steps to ensure that all its contractors, partners and agents comply with this clause where they are handling or processing Personal data on behalf of Cartwheel Arts.

5.5 Reasons for collecting personal information

Most of the information we process is to allow us to provide a service to our target markets and audience, customers, participants, staff members, freelancers, funders, colleagues, partners, sponsors, business, members, volunteers or donors or to interact with other people. This includes information that our freelancers, contractors or anyone providing a service on our behalf may need to do their job.

Sometimes we collect and hold additional information that is not strictly necessary in order to provide a service but can help us to analyse and improve our services, such as Equality and Diversity information. When asking people these kinds of questions they must be made aware it is optional and feel free to not provide the information. It must be clearly explained why we would like to collect the information. The consent given must meet the criteria set out in the “Definitions’ section below. Data must be stored anonymously.

For the avoidance of doubt about why we are collecting information, or how we should process any existing or new information, CWA representatives should speak to the Operations & Development Manager.

The full Privacy Notice (appendix 5) is publicly available on the Cartwheel Arts website.

5.5 Disclosure and Barring Service (DBS) Checks

Cartwheel Arts processes DBS checks for its employees, freelance practitioners and volunteers where necessary. As most of our work takes place with Children, Young People and some vulnerable groups, within school settings and in the community, we ask that everyone working with these groups undertakes either a Standard or Enhanced DBS check.

As an employer, we are legally responsible for making sure the job role is eligible for a DBS check, and we must obtain fully informed consent to conduct the check. Our legal basis for collecting this information is legitimate interest and is in line with our Children & Adult Safeguarding Policies and Procedures. Potential staff, Trustees and

volunteers have the right to refuse a DBS check, however, this may impact the capacity in which we can work with the individual.

We use an online system called Care Check, an approved Registered Body with the Disclosure and Barring Service where key staff members can access data provided by the individual completing an application and the status of their application. All individual undertaking an DBS Check can read Care Check's Privacy Notice for further information on how their data is collected and stored through this system:

https://www.carecheck.co.uk/about/policies/privacy-policy/

In order for Cartwheel Arts to view an employee or volunteers' DBS Certificate using the Update Service we require their consent, DBS reference number, date of birth and full name used on the application.

We do not store copies of criminal records check certificates unless there is a dispute about the results of the check. Instead, a confidential record is kept of:

- the date the check was completed
- the level and type of check (standard/enhanced/barred list check and the
- relevant workforce)
- the reference number of the certificate
- the decision made about whether the person was employed (with reasons).

If there is a dispute about the results of a check, we may keep a copy of the certificate for no longer than six months.

Ref: https://learning.nspcc.org.uk/media/1442/child-protection-records-retention-and-storage-guidelines.pdf

---

6 - Storing information

We store information electronically and on paper. We use different programmes and formats to store information all of which are protected in different ways.

6.1 Digital information

We use different systems, programmes, hardware and software to store and access digital information:

- We work with external technical support to provide appropriate physical, technical and procedural controls to all our hardware and software to ensure that data is protected, kept securely and accessible through different software and storage systems. Each team member is responsible for their emails, personal/project files and filing systems to make sure that the information archived or retained is regularly reviewed and deleted when needed.
- All staff members have access to a password-protected spreadsheet where all passwords for electronic information, computers and software and access to any electronic folders or documents are stored.
- All our digital data is kept in 4 different ways:

    - Online Google drive is our main storage unit. Each member of staff has access to Cartwheel Arts' Google drive using a username and password with 2-step verification.
    - We have an external hardware memory drive located in the office that hold historical backs ups of the whole system and up-to-date back ups of selected data (e.g. financial and board records).
- We use the following software to store different type of data:
    - **MailChimp** – We send a quarterly e-newsletter to subscribers who have asked to be added to the circulation list. On each newsletter there is the option to unsubscribe. Mailchimp uses secure systems to make sure that data is not lost or used in a wrongful manner.
    - **Database –** We are currently still storing data in Ninox, A GDPR compliant online database that has been designed and built for Cartwheel Arts.
    - **Website –** Madewithweb created our new website using their unique software. All the information kept in the CMS is password protected and only for the use of Cartwheel Arts.

6.2 Physical information

We store paper copies and originals of contracts, financial documents, project files, funding applications, meetings, etc. All personal information is stored in locked filing cabinets.

- **Document and Information Retention / Archiving –** Cartwheel Arts' Data Retention Table sets out the length of time we keep documents. Employees should refer to this before destroying or archiving documents.

6.3 Storing personal data outside the EEA:

The GDPR places special restrictions around transferring personal information outside of the European Economic Area (EEA). "Transfer" includes storing personal information on servers outside the EEA, which is the most likely way Cartwheel Arts information would be transferred outside of the EEA.

All Cartwheel Arts core ICT services are located within the EU.

When we are working/contracting with a 3rd party, who will then become a Data Processor for Cartwheel Arts (e.g. IT contractors, freelancers, etc.) the contract must include our standard Data Protection contract clause, which includes reference to the fact that data cannot be transferred outside of the EEA without prior written consent from Cartwheel Arts.

---

7 Using information

- Personal information can only be used for the purpose it was collected.
- If Cartwheel believes that information previously collected for one purpose would be useful for another purpose, then a legal basis for using the information for the new purpose must be established. If no legal basis can be found, permission must be sought from the person the information belongs to.
- Cartwheel Arts can only use information they have a legal right to, taking into account copyright and patents.
- While using information, it must be kept secure.

7.1 Information quality:

All colleagues are responsible for the quality and accuracy of the information they handle and produce. If colleagues are unsure about their work and the information they are handling, they should speak to their line manager. If Cartwheel is made aware that personal information is out of date or inaccurate it should be amended or deleted as appropriate.

Each staff member is responsible for the contacts they work directly with (participants, funders, colleagues, partners, etc.) and should regularly check that personal details are up to date.

Periodically, staff members are asked to check and update their own personal details.

8 Access to and use of information/systems

Staff access
Through their induction staff members will be provided with the relevant level of access to the network, systems and information.
When a member of staff leaves, user accounts and passwords will be deleted or changed. Ex-employee accounts will be redirected to their line manager, to have access to the leaver's mailbox, for a limited time.

Password Management
Secure passwords are essential and the use of capitals, lower case and numeric characters is recommended. Generic passwords should not be used and passwords should not be shared. There is a list of company passwords which is password protected.

Unacceptable use of Information/systems/equipment:
Cartwheel Arts equipment must only be used in line with this policy and the ICT/E policy, and not used for any illegal activity or activity which breaches any of our policies or which might damage the reputation of the charity. Any information staff members come into contact with during their work must only be used for their work. Any colleague breaching this policy will go through disciplinary procedures (see Disciplinary policy). It is a criminal offence for any colleague to misuse or disclose personal information that they have access to for their work, or to purposefully gain access to personal information. See link for Criminal offences under the Data Protection Act 1998 https://www.cps.gov.uk/legal-guidance/data-protection-act-1998-criminal-offences

Using equipment, software & services that store information:
Equipment & software
Cartwheel Arts owned equipment (e.g. tablets, PCs, Macs, laptops, phones) and software is provided for staff.
Fingerprint or facial recognition technology for access to phones and laptops is not mandatory and staff should only set this up with the understanding that the phone provider is then storing and processing their personal data. Staff will take full responsibility for researching the implications of this for themselves if choosing to add this option on top of creating a secure passcode or password.
Public Wi-Fi
Staff members should avoid using public Wi-Fi where possible and be aware of the risks if connecting to public Wi-Fi.

Update Management
Staff members should regularly connect their devices to the Internet or network to receive all patches and updates (e.g. laptops, PCs, Macs). This helps to protect our devices and network.

Use of Email/instant messaging & Internet including social media:
Staff members and freelance project managers with access to our systems must take care when using email, messaging, and social media. Personal use must not interfere with the day-to-day work of the charity, must not cost the charity anything, and must not breach any policies or regulations.

Sending emails – Emails are formal communications from the company, so should be treated with the same a care as a letter, for example. A standard notice is electronically added to outgoing emails, which includes our contact details and states that the email is confidential. This is the disclaimer notice currently in use:

"This email and its attachments may be confidential and are intended solely or the use of the individual to whom it is addressed. Any views or opinions expressed are solely those of the author and do not necessarily represent those of Cartwheel Arts Ltd. If you are not the intended recipient of this email and its attachments, you must take no action based upon them, nor must you copy or show them to anyone. Please contact the sender if you believe you have received this email in error."

Receiving emails – Staff members need to be aware of phishing emails. This is a fraudulent email asking to confirm details or click on a link: staff members should never respond to these requests or click on links from unfamiliar or **suspicious emails, even if the supposed sender is known to us.** Any suspicious emails should be reported to the rest of the team and the sender, if a Cartwheel contact.

Staff members must be very careful to not accidentally disclose commercially confidential information or other people's personal information in social media posts. Participant details should not be shared; 'thank you' comments and reviews posted on social media can be shared in public sites but always without an individuals' identifiable details.

---

9 - Physical security

The working space – All staff members are responsible, at all times, for making sure desks and any other working spaces, such as meeting areas, are kept secure. No sensitive data containing documents should be left out for anyone passing to be able to pick up and look at. Sensitive information should be kept in locked filing cabinets.

Visitors – The offices are not an open to the public but we hold meetings, arts sessions and other kind of gathering by invitation only. The staff member that coordinates the meeting is responsible for any information shared at the meeting and for clearing up after the meeting.

Workshop leaders are responsible for looking after data relating to participants, keeping it safe and passing it to the Project Manager as soon as possible.

Locked screens – Staff members must make sure their screens are locked if equipment is let unattended for any period of time, even if they are still in the office.

Mobile working – Staff members must take special care when working outside of the office, at home or in another location, to keep information secure.

Staff must remember to:

- Keep devices secure, especially overnight (not in a vehicle);
- Think about where paperwork is kept just as much as devices;
- Be aware of where they're having conversations, and who can hear them;
- Be aware of who can see their screen or paperwork;
- If they're working remotely, every time they leave a location take a minute to check they have all their papers and devices with them, so they don't leave anything behind.
- If a device or any paperwork does get mislaid or stolen, report to their line manager and Cartwheel's ICT support as soon as possible so we can quickly protect our data and report the potential breach.

---

10 - Sharing information

Cartwheel Arts will never sell data to third parties.

Sharing any type of information – business or personal information – is high risk and must always be approached with care.

Even internally, sharing should always be on a need-to-know basis.

If it is information about people, to be legally shared, it must be justified under the Data Protection Act 2018.

Sharing must always be done securely, so that it isn't lost or accessed by the wrong people.

The people whose information Cartwheel Arts holds have the legal right to receive copies of that information, known as making a Subject Access Request (SAR)

Staff members, freelancers, volunteers and Trustees must sign a Confidentiality Agreement which commits them to adhering to our Confidentiality Policy and also this policy if the person has access to sensitive information.

Where required, freelance practitioners are given temporary access to necessary folders in the Cartwheel Arts shared drive. Once the project / reason for access is finished the permissions should be withdrawn. This is the responsibility of the Project Manager.

Staff members can give restricted access to Board members and specific partners to certain folders on the shared drive that are relevant to them.

---

11 – Contracts, Partnership Agreements, Memoranda of Understanding etc

Cartwheel Arts regularly work in partnership with other organisations. Therefore, situations may arise where we need to share information to deliver a project. Participants will be informed when this is the case. Cartwheel are contractually obliged by funders to report on project delivery. This is usually statistical data where individuals cannot be identified. Case studies will only be carried out with the express permission of the individual and quotes are generally anonymous.

Cartwheel Arts is usually the Data Controller but will sometimes be commissioned to be the Data Processor. Where this is the case there will be a 'sharing information' clause written into the contract.

Whenever Cartwheel are entering into a contract where the third-party will be a 'Data Processor' the contract should be reviewed for appropriate Data Protection/Information Governance controls. This includes where:

- The contract involves sharing personal information (about our participants, colleagues or anyone else) with a third-party, such as a partner, supplier or contractor; or
- A third-party will store personal information we give them on their computer systems, servers or at their premises (this includes archiving.)

In addition, there must be a Data Protection clause in the contract.

- Sometimes when we are working with partner organisations, such as Local Authorities, we sign up to an Information Sharing Agreement (ISA), also sometimes known as an Information Sharing Protocol.

---

12 - Subject Access Requests

A Subject Access Request (SAR) is the legal right of people to ask for copies of all the information we hold about them.

It is our policy to be as open and transparent as possible, and to give people copies of their own information, and things like letters that have previously been sent to them, if possible, without them having to make a full Subject Access Request.

The Operations & Development Manager and Director are responsible for SARs.

---

13 - Disposing

All personal and business information must be disposed of securely, so that it can't be found or accessed later, and possibly misused.

Personal information must be disposed of when it is no longer needed for the reason it was collected.

If in doubt, seek advice from ICT support about how to permanently dispose of any digital information.

See the Document Retention Table for advice on when to dispose of information and documents.

Archived documents should be called back and securely destroyed at the end of their retention period.

13.1. Hard copy information

Cartwheel Arts currently destroys all sensitive information through a shredder.

13.2. ICT equipment

Cartwheel Arts consults our ICT support on secure disposal of all ICT equipment. This will include the disposal of equipment that may contain personal data and

confidential information on hard drives in PC's and laptops and servers, back up tapes, mobile phones and tablets.

14 - Handling Data Breaches

Losing personal information could cause harm or embarrassment to the people the information is about. It could also cause reputational damage to Cartwheel Arts and result in prosecution and a fine (the current maximum is £20 million or 4% of annual turnover).

Any loss, or suspected loss, of personal or sensitive business information, must be reported immediately – either directly to the appropriate line manager, the board and the ICT support. They will instigate all possible measures to regain the data, mitigate the risks, investigate what happened and assess the breach against the data protection regulator (ICO) reporting guidance. A major breach will be reported to the Director, the Trustees and the ICO.
Staff members should take any appropriate actions to attempt to recover the information first; for example, attempt to recall and email sent in error.

The named lead is the organisations Operations & Development Manager – Becky Smyllie. E: becky@cartwheelarts.org.uk. T: 01706 361300

1. Containment and recovery	The named lead, ICT provider and person responsible for breach will work together for damage limitation.
2. Assessment of ongoing risk	The named lead, ICT provider and person responsible for breach will work together to assess the ongoing risk.
3. Notification of breach	The individuals concerned must be informed about the data breach. The named lead or Director must also inform Cartwheel Arts Board of Trustees and the Information Commissioner Office.
4. Evaluation and response	The named lead will lead on evaluating what caused the data breach, how effective the breach management plan was in managing the breach, evaluating what could be done differently in the future to ensure no further breaches and circulating any lessons learned / updating policy and procedures.

14.1. Lost / Stolen devices

All staff members and anyone working for Cartwheel and using Cartwheel's devices, should report any loss or theft of ICT equipment to their line manager and ICT support as soon as possible. The Line Manager and the ICT support will take appropriate and swift action to track and disable/wipe the device if this is possible.

14.2. Managing cyber attacks

All cyber security incidents will be assessed, managed and reviewed by the Director and the ICT support, which will work to recover any lost information and mitigate the risks. The Director will be responsible for reporting any attempted or successful fraud or any Data Protection breaches to the right person or authority.

Cyber attacks can be reported to police via Action Fraud - 0300 123 2040 or www.actionfraud.police.uk

14.3. Disaster Recovery & Business Continuity

The ICT support together with the Director and the board will make sure processes are in place to protect our data and provide continuity of access to our data if an incident occurs that causes disruption to the business.

Events may include, amongst others:

- Infrastructure / systems failure
- Fire, flood, impact damage
- Malicious (Hacking) attack
- Theft of information / media

---

15 - Monitoring and review

15.1. Risk Management monitoring

Cartwheel's Risk Register includes a section on Data Protection. Controls and assurances are designed to prevent risks from materializing as far as possible. Key risks are monitored and reported to the Board.

15.2. Systems monitoring

Monitoring is in place on all information systems to detect any unauthorized activity (e.g. external or internal attacks) or security breaches (e.g. as a result of penetrating the network a third party has managed to access and remove certain information assets)

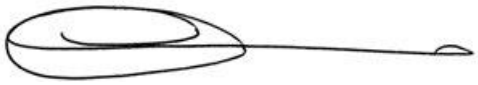
If any suspected security incidents or breaches are identified the ICT support will be informed to act accordingly to the risk.

15.3. Content Monitoring

Cartwheel Arts reserves the right to analyse all content pertaining to both equipment (i.e. hardware) and software, including Internet and Email usages at any time for:

- Fault diagnostics
- Unauthorised & unacceptable use of IT systems; software and equipment.

Cartwheel Arts
Signed,



Date: 17.11.23
Alyson Malach
(Chair Trustees)

Date: 13.11.23
Hebe Reilly
(Cartwheel Arts Director)

Appendices

Appendix 1 – Glossary

Glossary of terms used in Information governance and Data Protection

DPA	• Data Protection Act 2018
UK GDPR	• UK General Data Protection Regulation, tailored by the Data Protection Act 2018.
PIA	• **Privacy Impact Assessments** are a tool used to identify and reduce the privacy risks of projects. • A PIA can reduce the risks of harm to individuals through the misuse of their personal information.
Personal Information/ Data	• Any information that relates to the Data Subject; name, address, age, birth, Postcode, etc. • **Any** information that can **identify** a living person, either on its own or **with other** information. It does not need to include a person's name • Includes **comments or opinions** about a person. • Including; information held on computer systems, in paper files, in emails, photographs, films or social media
PII	• Personally Identifiable Information is information by which a data subject can be identified directly or indirectly. • If a charity has information about a data subject in its systems that may be used to identify it, the charity just ensure that how it stores and processes the information is compliant with the GDPR
Sensitive personal information	• Anything about a person's ethnic origin political opinions, religious beliefs, memberships of trade unions, physical or mental health, social life, or criminal offences (alleged or committed). • Must be treated with extra care, in line with **specific rules** in the DPA about sensitive data.
Data subject	• The person that the information is **about.** Any person that could be identified directly or indirectly. The EU stipulates that a DS can only be a person that is alive.
Data controller	• A person or organization with the authority to decide how and why personal information is used. • Cartwheel Arts is the only 'Data Controller' legal entity. • Cartwheel Arts is registered with the Information Commissioner's Office (ICO) as required.
Data Processor	• A 3rd party person or organisation, which **processes** personal data **on behalf** of a Data Controller, eg service providers, contractors,

	hosts for IT systems and **any other partners /person** that is given the right due to the nature of the partnership or the job. ● Cartwheel Arts' staff members are not considered 'Data Processors'
Processing	● Processing covers **anything** that can be done to information. ● This includes collecting, recording, storing, using, amending, sharing, disposing of or destroying personal information.
Consent	● Permission from the data subject to collect and process their information ● It must be **clear** and **unambiguous** ● We must not ask for consent if we can and would process the information anyway unless we are prepared to accept the consent later being withdrawn. ● Cannot be hidden in the terms and conditions or contract clauses ● Consent obtained from someone who does not feel they are able to refuse consent is not valid.

Appendix 2: Data Retention table

Data Retention Table								
Type of document	Document	Personal data	Rentention period	Due	Located	Owner	Reason for holding	Notes
Financial	Audit report of Accountants	No	Permanently		Digital/printed	Finance Officer	Legal obligation	
Financial	Bank statements	No	10 years		Digital/printed	Finance Officer	Legal obligation	
Company	Leases	No	Permanently		Digital/printed	Director/Development manager	Legal obligation	
Company	Contracts/commissions	No	10 years		Digital/printed	Director/Development manager	Legal obligation	
Company	Correspondence (legal)	Yes	Permanently		Digital/printed	Director/Finance Officer	Legal obligation	
Company	Deeds Mortgages, etc	No	Permanently		printed	Director/Finance Officer	Legal obligation	
Financial	Funding agreements	No	10 years		Digital/printed	Director/Finance Officer	Legal obligation	
Financial	Service Level agreements	No	10 years		Digital/printed	Director/Finance Officer	Legal obligation	
Financial	Employee Payroll records	Yes	10 years		Digital/printed	Director	Legal obligation	
Company	Employment applications (shortlisted	Yes	3 years		Digital/printed	Director	Legitimate interest	
Financial	Insurance records	No	Permanently		Digital/printed	Director/Finance Officer	Legal obligation	
Financial	Invoices	No	10 years		Digital/printed	Director/Finance Officer	Legal obligation	
Company	Patents	No	Permanently		Digital/printed	Director	Legal obligation	
Financial	Payroll records and tax returns	Yes	10 years		Digital/printed	Finance Officer	Legal obligation	
Financial	Purchase orders	Yes	10 years		Digital/printed	Finance Officer	Legal obligation	
Financial	Accident Records	Yes	Permanently		Digital/printed	Director	Legal obligation	
Company	HR records for ex-employees	Yes	7 years		Digital/printed	Director	Legitimate interest	
Company	Freelance contracts	Yes	10 years		Digital/printed	Director / Project Coordinator	Legal obligation	
Company	Volunteer records	Yes	5 years		Digital/printed	Director / Project Coordinator	Legitimate interest	
Company	Board / membership records	Yes	Indefinitely		Digital/printed	Director / Development Manager	Legal obligation	
Project	Image / video / audio / publication co	Yes	Indefinitely		Digital/printed	Director / Project Coordinator	Legitimate interest / Contractual	
Project	Participant information	Yes	10 years		Digital/printed	Director / Project Coordinator	Legitimate interest / Contractual	specifically health / mental health
Project	Project records	Yes	Funding, finance, PID/report indefinitely. Attendance info and anything else 5 years		Digital/printed	Director / Project Coordinator	Legitimate interest / Contractual	
Project	Safeguarding issues	Yes	10 years		Digital/printed	Director / Project Coordinator	Legal obligation	
Company	DBS Check Application	Yes	6 years (6 months for applications not submitted)		Digital	Care Check	Legitimate Interest	
Company	DBS Check Certificate	Yes	6 months only if a there is a dispute about the result		Digital/Printed	Director / Project Coordinator	Legitimate Interest	
Company	Newsletter recipients	Yes	Indefinitely (until they tell us otherwise). 'Opt out'/ unsubscirbe option available on all Mailchimp emails		Digital	Development Manager	Legitimate interest / consent	
Reasons for holding:								
Consent	People have positively and clearly given their consent							
Legal obligations	is there a legal reason why we have to do this e.g. HMRC and accident reports for health and safety records							
Contractual	in order to fulfil a contract / service with the individual. Funders requirements							
Legitimate interest	You are using data in a way that people would reasonably expect or where there is compelling justificaiton							
Vital interest	Very limited in scope generally only applies to matters of life and death i.e. safeguarding and individuals at risk of immediate harm							
Public task	Generally statutory and public bodies							

Appendix 3: Data Protection Impact Assessment

Cartwheel Arts Privacy Impact Assessment (PIA)

Submitting controller details

Name of controller	Cartwheel Arts
Subject/title of DPO	Operations & Development Manager
Name of controller contact /DPO (delete as appropriate)	Becky Smyllie

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
Cartwheel Arts projects aim to provide the highest quality experience requiring personal data to be collected for communication and monitoring purposes. This DPIA assesses the impact of collecting such data during our projects.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
Collect – via referral, digital and paper forms, CVs in the case of contracted freelancers and online services (e.g. Care Check for DBS checks) Use – Cartwheel only collects data that is necessary for the type of engagement an individual expects to have with us. To receive post or transport we use address and postcode. DOB is collected only for Art for Wellbeing referrals as groups are generally age specific. Phone numbers and email addresses are used for effective communication or criminal offence check where appropriate. Store – all physical paper forms are kept in locked cabinets at our office. Digital information is either stored on a password protected online drive and/or Ninox (a secure database). Phone numbers are stored on company mobiles through which online drives are also accessible. DBS check information is stored digitally via Care Check. Deletion – using our Data Retention table (appendix 2) we delete data as appropriate during annual data audit/purges.

Source of data – data is either collected directly from the individual or, with consent to share, from a referral partner.

Sharing of data – Cartwheel does not share data unless in the case of an emergency, with emergency or social services, where there is threat to a person's safety. Even with an individual's explicit consent to sharing data we would always try to support an individual communicating with other services independently.

Processing identified as "likely high-risk":

1. Fingerprint access to and storage on company phones.
    a. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology, defined in "accordance with the achieved state of technological knowledge" (recital 91), can trigger the need to carry out a DPIA.
2. Data concerning vulnerable data subjects (recital 75)
    a. increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Nature of the data:

Largely contact information including: Full name, Address, Postcode, Phone number(s), Date of Birth, contact preferences.

In the case of referrals this may also include comments from the individual (e.g. self-referral) or the referrer about the persons current situation.

We do not collect special category data (now including gender) unless on an anonymized monitoring form which is stored anonymously.

Criminal Offense data is collected, with consent, when contracting a new freelance practitioner and/or volunteer.

Employment history and referrals are collected when contracting a new freelance practitioner.

Quantity of data – related to the scale of the project however on larger projects there is little need to collect such comprehensive data.

Regularity – we collect and process data throughout the year based on current activity and receipt of referrals.

How long we keep it – as outlined in our Data Retention table (appendix 2)

Individuals affected – the number of individuals whose data we store will fluctuate continuously due to the nature of our work however Cartwheel only collects and stores data from a small percentage of individuals as necessary.

Geographical area – UK only. Except in circumstances where, when conducting a DBS check and the individual has lived outside of the UK we would be processing their address details from those locations.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Nature of the relationship with individuals:

- Referrals form external organisations; this information has been shared with us and the external organization has gained consent from the individual. Cartwheel then uses this data to make contact with the individual and process the data accordingly (i.e. if they do not want to engage at all we would delete their data and ask that they are re-referred should they change their mind)
- Self-referrals; either an individual has found us independently and uses our form to provide their details as an expression of interest for accessing our services or, when meeting the individual in person, we may ask them to provide their details for communication and monitoring purposes.
- Once registered with Cartwheel an individual accessing our services is then considered a participant who is able to engage with our activities and access support as appropriate.
- Freelance practitioners are providing their service in a paid capacity
- Volunteers are interested in gaining professional experience and have access to support and guidance and are always supervised.

Control – individuals have full control as to what data they provide however this may change the nature and extent to which we can work with them. We do not collect unnecessary data and therefore see the data collection as mutually beneficial.

Expectations for use of data – we are transparent about the purpose for collecting data and therefore keep everyone informed as to how we use it.

Our data collection will sometimes include children and vulnerable groups, namely refugee and asylum-seeking individuals and Cared for Children. The purpose for which is to provide the highest quality service. Data collected from these groups would only include: Name, address, DOB (where applicable – i.e. age specific projects), phone number and language spoken (for interpretation requirements). However, we do not store this data with any connection to their status.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
- To provide high quality services and support (contact details, referral comments, DOB for age specific projects and employment history/CV) - To monitor the areas in which our participants reside and assess that we are reaching the right communities based on our mission to serve areas of high deprivation (postcode) - To ensure our services are safe (DBS, references, employment history)

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
Our Information Governance Policy and Procedures is reviewed by the Board of Trustees, which includes this DPIA. We do not undertake formal consultation with other stakeholders (partners, practitioners and participants) however we listen and reflect based on conversations where data is the focus, for example, when inducting a new participant/volunteer or contracting a new practitioner.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
Lawful basis as outlined in the Data Retention Table (appendix 2) is Legitimate Interest or Legal Obligation for all data concerned within this DPIA. This processing achieves our purpose using the least amount of data possible. We ensure data quality through regular updates of our database. We explain verbally how data is used and have developed an easy read complaints document to support an individuals right to complain.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Power imbalance in the relationship between the position of the data subject and the controller leading to processing without informed consent.	Possible	Minimal	Low
Use of technology such as fingerprint or face recognition to access data can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms.	Possible	Minimal	Low

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
N/A – no medium or high risks identified		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix 4: Information Governance and Data Protection Guidelines for Freelance Practitioners

Information Governance and Data Protection Guidelines for Freelance Practitioners

Cartwheel Arts take personal privacy very seriously and it is also a legal requirement to handle data responsibly under UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018.

As a valued member of our freelance team, you may be responsible for handling sensitive or personally identifiable data including: name and contact details, gender, In Case of Emergency contact details, financial details, health and wellbeing data, projects accessed, images, video, artwork, publications.

It is your responsibility to ensure that this information is kept safe and secure whilst it is in your care. When you no longer require the data, please ask your contact at Cartwheel Arts whether it should be returned to the organisation or destroyed. This applies to both electronic and paper information. We want to ensure that you are comfortable and confident in handling data so please ask if you require any further information or feel that you have training needs.

Everybody is entitled to make a Subject Access Request to request copies of any personal information that Cartwheel Arts hold about them, this includes emails and letters. If / when you are corresponding about an individual with Cartwheel Arts, please ensure that you write factual information and use a respectful tone.

We generally ask session leaders to fill in registration forms and/or registers and Image / Video / Content consent forms. We would ask that you use the full first name and the first initial of the surname. You are responsible for ensuring that this information is stored and shared with Cartwheel responsibly.

Each participant must be given a postcard that tells them how Cartwheel Arts will use and look after their data. You will be informed if it is part of your role to give this information out. If a participant wants further information, then please give them the office contact details (below).

If there is a data breach (data is lost or stolen) then you must inform the Operations and Development Manager at Cartwheel Arts, immediately by phone 01706 361 300 (if no one answers you must leave a message but do not disclose personal information on this message) or email admin@cartwheelarts.org.uk with subject: “Data Breach”.

Our Breach Management Plan will be put into action and your cooperation in this process will be required.

This guidance must be followed alongside any further guidance or instructions in your contract.

You must also read our Privacy Notice in full and be aware of where to access our Information Governance Policy & Procedures – please speak of a member of staff if in doubt.

Privacy Notice can be found via: https://www.cartwheelarts.org.uk/privacy-notice/

To access our Information Governance Policy & Procedures please visit our website: http://www.cartwheelarts.org.uk/about-us/policies/

Appendix 5: Privacy Notice

Cartwheel Arts Privacy Notice Aug 2023

We take your personal privacy very seriously at Cartwheel Arts. We have created this privacy notice to explain how we collect, store, manage, process and protect any personal information. It includes the types of information that we might hold, how and where we'll use it and how we'll look after it.

If you want to contact us about our privacy notice, or anything to do with your data at Cartwheel Arts then please email admin@cartwheelarts.org.uk, 01706 361300 or by post: Cartwheel Arts, 110 Manchester Street, Heywood, Lancashire, OL10 1DW.

How we collect personal information:

- You request to join our mailing list
- You participate in one of our projects
- You are or become a staff member / Trustee / volunteer
- You work for us as a freelance practitioner
- You make a donation
- You visit our website

We'll always make it clear what data we are collecting from you.

The following data and information may also be collected when you visit our website:

- IP address
- Referring website
- Web browser and device
- Cookies
- Time and date of visit
- Pages visited
- Location

Images / Video:

- We don't have CCTV at Cartwheel Arts, although some of the venues that we hire for projects may do - we don't have access to this.
- We often take photos and/or video and sound recordings at our events and project sessions. We will ask for your consent to do this, if you refuse then we'll ask you to wear a badge so that the photographer can see that you don't want to be photographed. At larger events where it is not feasible to ask for individual consent, we will clearly indicate that photographs / video is being taken and how to withdraw consent.

Why:
We collect personal information to fulfil legal and contractual requirements, or if we feel that there is a legitimate interest, or if you have given us consent to do so.

- If you are taking part in a project then we need to hold your contact details so that we can keep you informed.

- Often, our funders will require us to collect information about the projects that we are delivering. You will always be told what this is. Most of the data is statistical or anonymous so can't be linked to an individual. We will get your express permission to use anything that is personally identifiable such as a case study.
- Lots of our projects produce outputs such as video, print, art work or content for websites and press releases. We will always ask for your consent to use this.

We will only collect sensitive personal information, such as health, disability, economic situation if we are contractually obliged to, or is it is to help to keep you safe. For example, if you are coming on a trip with us then we would need to know if you are asthmatic or have a nut allergy etc.

What you can expect from us:

- We'll never provide any of your information to a third party without your permission
- You have the right to challenge us about any information that we hold relating to you
- You have the right for your details to be removed from our systems (database and newsletter)
- We may compile statistical data from time to time (for our Impact Report, to report to funders etc) but this will never include references to particular individuals
- We will never, ever sell or give our mailing lists to a third party
- We store any information as securely as possible. Anything stored digitally is password protected and paper records are stored in secure cabinets.

We uphold the 7 GDPR Principles as follows:

1. We process data lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')
2. We collect data for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation')
3. We only collect data that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
4. We ensure data is accurate and, where necessary, kept up to date; every reasonable step is taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
5. We keep data 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')
6. We process data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

7. We are responsible for and can demonstrate compliance with the above principles ('accountability')

Your data protection rights

Under data protection law, you have rights including:

Your right of access - You have the right to ask us for copies of your personal information.

Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

Your right to object to processing - You have the the right to object to the processing of your personal information in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you. Please note that we may not always be able to do what you ask – for example if you ask us to erase data which we have an over-riding legal duty to keep.

Please contact us at admin@cartwheelarts.org.uk – 01706 361 300 – 110 Manchester Street, Heywood, OL10 1DW if you wish to make a request.