Cartwheel Arts

Confidentiality Policy

Policy for staff members, Board members, temporary and freelance workers using ICT in Cartwheel Arts or on behalf of Cartwheel Arts

1. Introduction

1.1. The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within Cartwheel Arts (from here on CWA) and have access to person-identifiable information or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

1.2. All employees working at CWA are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and the 2018 EU General Data Protection Regulations 2016 (enforceable from 25th May 2018)

1.3. It is important that Cartwheel Arts protects and safeguards person- identifiable and confidential business information that it gathers, creates processes and discloses, in order to comply with the law, and to provide assurance to participants, staff members, Trustees and the public.

1.4. This policy sets out the requirements placed on all staff when sharing information within CWA and between CWA and its stakeholders and partners.

1.5. Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, and must not be stored on removable media unless it is encrypted as per our Information Governance Policy.

1.6. Information can relate to participants and staff (including temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

1.7. A summary of Confidentiality Do's and Don'ts can be found at **Appendix A.**

1.8. The Legal and CWA Mandated Framework for confidentiality which forms the key guiding principles of this policy can be found in **Appendix B.**

1.9. How to report a breach of this policy and what should be reported can be found in **Appendix C.**

1.10. Definitions of confidential information can be found in **Appendix D.**

2. Scope

Staff, freelancers, volunteers, apprenticeships, temps and trustees are within the scope of this document:

3. Roles and Responsibilities

3.1. **The Director** has overall responsibility for strategic and operational management, including ensuring that CWA policies comply with all legal, statutory and good practice guidance requirements.

3.2. **The Operational Manager** - is responsible for ensuring the implementation of all the policies on a day to day basis as well as maintaining the currency of this policy, providing advice on request to any member of staff on the issues covered within it, and ensuring that training is provided for all staff groups to further their understanding of the principles and their application. The OM is also responsible for all HR matters ensuring that the contracts of all staff (permanent and temporary) are compliant with the requirements of the policy and that confidentiality is included in inductions for all staff.

3.3. **Project Managers** are responsible for ensuring that the policy and its supporting standards and guidelines are built into all processes and that there is on-going compliance from all their team members, including artists and Emotional Suport Workers. They must ensure that any breaches of the policy are reported, investigated and acted upon.

3.4. **All staff**

- Confidentiality is an obligation for all staff. Staff should note that they are bound by the Confidentiality policy, sign and keep a copy of CWA's confidentiality agreement. There is a Confidentiality and Data Protection clause in their contract and that they are expected to participate in induction, training and awareness raising sessions carried out to inform and update staff on confidentiality and Data Protection issues.
- Any breach of confidentiality, inappropriate use of staff records or business sensitive/confidential information, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract, and must be reported.

4. Company Procedures

4.1 Principles

4.1.1 All staff must ensure that the following principles are adhered to:

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure of information must be discussed with either your Line Manager or the Director.

4.1.2 CWA's is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

4.1.3 Person-identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.

4.1.5 All staff should clear their desks at the end of each day. In particular they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked.

4.1.6 Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin and or shredded. Discs, tapes, printouts must not be left lying around but be filed and locked away when not in use.

4.1.7 In addition to your Contract of Employment you need to sign a Confidentiality Agreement. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

4.2 Disclosing Personal/Confidential Information

4.2.1 To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it.

4.2.2 It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

4.2.3 Information can be disclosed:

- When effectively anonymised in accordance with CWA's Information Governance protocols.
- When the information is required by law or under a court order. In this situation staff must discuss with their Line Manager or Information Governance staff or Director before disclosing, who will inform and obtain approval from the Board.
- In Child Protection proceedings if it is considered that the information required is in the public or child's interest. In this situation staff must discuss with their Line Manager and/or Director before disclosing, who will inform and obtain the approval from the Board.
- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must discuss with their Line Manager and/or Director before disclosing, who will inform and obtain approval from the Board.

4.2.4 If staff have any concerns about disclosing information they must discuss this with their Line Manager or Director.

4.2.5 Care must be taken in transferring information to ensure that the method used is as secure as it can be. CWA's has a password protected File Sharing System only available to staff members and partially accessible to the Baord. For further information on Data Sharing CWA's Information Governance policy

4.2.6 Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mail and post. See the Information Governance Policy.

4.2.7 Transferring participants information to anyone outside of CWA's network may only be undertaken in special circumstances and only with permission from the Director who will be approved by the Board. For more information on how, when and to whom you can share information please see our Informaiton Governance Policy.

4.3 Working Away from the Office Environment

4.3.1 There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry CWA's information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents.

4.3.2 Taking home/ removing paper documents that contain person-identifiable or confidential information from CWA's premises is discouraged.

4.3.3 To ensure safety of confidential information staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations.

4.3.4 When working away from CWA's locations staff must ensure that their working practice complies with CWA's policies and procedures. Any electronic removable media must be encrypted.

4.3.5 Staff must minimise the amount of person-identifiable information that is taken away from CWA's premises.

4.3.6 If staff do need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e. windowless envelope, suitable bag, etc. prior to being taken out of CWA's buildings.
- Confidential information is kept out of sight whilst being transported.

4.3.7 If staff do need to take person-identifiable or confidential information home they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information.

4.3.8 Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not use or store person- identifiable or confidential information on a privately owned computer or device.

4.4 Carelessness

4.4.1 All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally.

Staff may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard.
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts and other documents.
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, unattended

4.4.2 Steps must be taken to ensure physical safety and security of person- identifiable or business confidential information held in paper format and on computers.

4.43 Passwords must be kept secure and must not be disclosed to unauthorised persons. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. If you allow another person to use your password to access the network, this constitutes a disciplinary offence and is gross misconduct which may result in your summary dismissal.

4.5 Abuse of Privilege

4.5.2 When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of CWA.

4.5.3 If staff have concerns about this issue they should discuss it with their Line Manager or Director.

5. Distribution and Implementation

5.1 Distribution Plan

5.1.1 This document will be made available to all Staff via email.
5.1.2 This document will be presented to the Board for approval.

5.2 Training Plan

5.2.1 This document will part of the staff induction.
5.2.2 Appropriate training will be provided to Staff as necessary.
5.2.3 Guidance will be provided to staff when needed.

6. Monitoring

6.1 Compliance with the policies and procedures laid down in this document and/or related to Data Protection will be monitored via the HR Task Group led by the Operations Manager and Director, together on a periodic basis.

6.2 The Operations Manager is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises.

7. Equality Impact Assessment

7.1 This document forms part of CWA's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

7.2 As part of its development this document and its impact on equality has been analysed and no detriment identified.

8. Associated Documents

8.1 The following documents will provide additional information:
Disciplinary Procedure
Grievance Policy
Harassment Policy
Equality, Diversity and Inclusion policy/Action Plan
Child Protection Policy/Code of Practice
Protection of Vulnerable Adults Policy/Code of practice
Social Media guidelines
Information Governance Policy
ICT/E- Safety Policy
Image consent form

Appendix A: Confidentiality Dos and Don'ts

- Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of CWA
- Do clear your desk at the end of each day, keeping all portable records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
- Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.
- Do ensure that you cannot be overheard when discussing confidential matters.
- Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
- Do share only the minimum information necessary.
- Do transfer person-identifiable or confidential information securely when necessary i.e. use CWA's shared folder and CWA's email accounts.
- Do seek advice if you need to share patient/person-identifiable information without the consent of the participant/identifiable person's consent, and record the decision and any action taken.
- Do report any actual or suspected breaches of confidentiality.
- Do participate in induction, training and awareness raising sessions on confidentiality issues.

Don'ts

- Don't share passwords or leave them lying around for others to see.
- Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
- Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible.
- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.

Appendix B: Summary of Legal and Mandatory Frameworks

CWA is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and freelancers and trustees of CWA, who may be held personally accountable for any breaches of information security for which they may be held responsible. CWA shall comply with the following legislation and guidance as appropriate:

The 2018 EU General Data Protection Regulations 2016 (enforceable from 25th May 2018)

Click here for an online link to the 2018 EU GDPR

Appendix C: Reporting of Policy Breaches What should be reported?

Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again.

All breaches should be reported to the Operational Manager or the Director in absence of the prior. If staff are unsure as to whether a particular activity amounts to a breach of the policy, they should discuss their concerns with their Line Manager. The following list gives examples of breaches of this policy which should be reported:

- Sharing of passwords.
- Unauthorised access to CWA's systems either by staff or a third party.
- Unauthorised access to person-identifiable information where the member of staff does not have a need to know.
- Disclosure of person-identifiable information to a third party where there is no justification and you have concerns that it is not in accordance with the Data Protection Act and CWA's Code of Confidentiality.
- Sending person-identifiable or confidential information in a way that breaches confidentiality.
- Leaving person-identifiable or confidential information lying around in public area.
- Theft or loss of person-identifiable or confidential information.
- Disposal of person-identifiable or confidential information in a way that breaches confidentiality i.e. disposing off person- identifiable information in ordinary waste paper bin.

Seeking Guidance

It is not possible to provide detailed guidance for every eventuality. Therefore, where further clarity is needed, the advice of a Senior Manager should be sought.

Reporting of Breaches

A regular report on breaches of confidentiality of person-identifiable or confidential information shall be presented to the Operational Manager or the Director in absence of the prior. The information will enable the monitoring of compliance and improvements to be made to the policy and procedures.

Appendix D: Definitions

The following types of information are classed as confidential. This list is not exhaustive:

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, National Insurance number etc. Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

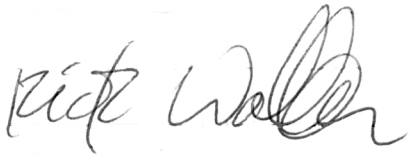
Sensitive/confidential personal information as defined by 2018 EU GDPR refers to personal information about:

- Race or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence, or
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings
- Non-person-identifiable information can also be classed as confidential such as confidential business information e.g. financial reports; commercially sensitive information e.g. contracts, trade secrets, procurement information, which should also Version control tracker

Cartwheel Arts

October 2018

Signed,



Alyson Malach (Chair Trustees) Rick Walker (Cartwheel Arts Director)