DATA PROTECTION POLICY

This is a core policy that forms part of the induction for all staff, volunteers and Trustees. It is a requirement that all members have access to this policy and sign to say they have read and understood its contents.

Owner:	Circomedia
Author:	Face2Face HR withe General Manager updates
Date agreed by SMT/Board:	14th June 2023
Version:	1.3
Date of last review:	24th June 2025
Date of next review:	24th June 2026
Changes to document:	V1.1 June 2024 - slight reformatting/tidying, data protection compliance changed to person rather than role V1.2 New Circomedia Logo added April 2025 - included participants, audiences and students in data protection policy, special categories of data to include DBS checks, General Manager is the data protection officer V1.3 Formatting

This policy will be reviewed and ratified at least annually and/or following any updates to national and local guidance.

1. Introduction

Circomedia is committed to being transparent about how it collects and uses the personal data of its workforce, students, participants and audiences, and to meeting its data protection obligations. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR-related personal data. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

Circomedia has appointed the General Manager as the person with responsibility for data protection compliance, to whom questions about this policy, or requests for further information, should be directed.

2. Definitions

"Personal data" is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, biometric data and DBS checks.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

3. Data protection principles

Circomedia processes HR-related personal data in accordance with the following data protection principles:

- Processing personal data lawfully, fairly and in a transparent manner.
- Collecting personal data only for specified, explicit and legitimate purposes.
- Processing personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Keeping accurate personal data and taking all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Keeping personal data only for the period necessary for processing.
- Adopting appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Circomedia tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where Circomedia processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

Personal data is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which Circomedia holds HR-related personal data are contained in its privacy notices to individuals.

Circomedia keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

4. Individual rights

As a data subject, you have a number of rights in relation to your personal data.

4.1 Subject access requests

You have the right to make a subject access request. If you make a subject access request, Circomedia will tell you:

- whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from you;
- to whom your data is or may be disclosed;
- for how long your personal data is stored;
- your rights to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think Circomedia has failed to comply with your data protection rights; and
- whether or not Circomedia carries out automated decision-making and the logic involved in any such decision-making.

Circomedia will also provide you with a copy of the personal data undergoing processing.
To make a subject access request, you should send the request to the person with responsibility for data protection compliance. In some cases, we may need to ask for proof of identification before the request can be processed. We will inform you if we need to verify your identity and the documents we require.

We will normally respond to a request within a period of one month from the date it is received.

If a subject access request is manifestly unfounded or excessive, for example is a repeat of a previous request, we are not obliged to comply with it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request.

4.2 Subject access requests

You have a number of other rights in relation to your personal data. You can require Circomedia to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if your interests override our legitimate grounds for processing data (where we rely on legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about

whether or not the individual's interests override our legitimate grounds for processing data.

To ask Circomedia to take any of these steps, you should send the request to the person responsible for data protection compliance.

5. Data security

Circomedia takes the security of HR-related personal data seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Breathe HR is used to hold staff HR data and hold ISO 27001 accreditation.

Where we engage third parties to process personal data on our behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

6. Data breaches

If Circomedia discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of their effect.

7. International data transfers

Circomedia will not transfer HR-related personal data to countries outside the EEA.

8. Individual responsibilities

You are responsible for helping us keep your personal data up to date and should notify Circomedia of any changes promptly.

You may have access to the personal data of other individuals, and of our customers and students, in the course of your job role.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside Circomedia) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from Circomedia's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work

purposes.

-

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under our disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

9. Training

Circomedia will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.