Code of Practice

This document is a governing document for our work. It has been created by the Board of Trustees in consultation with CCI associates* and is shared with all artist and project associates working with the organisation. It covers agreed guidelines on:

- **Board procedures**
- **Complaints**
- **Confidentiality**
- **Data protection: confidentiality and security**
- **Employment**
- **Equal opportunities and diversity (full policy reviewed February 2023, to review 2025)**
- **Financial management**
- **Fundraising**
- **Health and Safety (full policy reviewed May 2023, to review 2025)**
- **Insurance**
- **Premises and security**
- **Risk Management**
- **Safeguarding for children and vulnerable adults (full policy reviewed October 2022, to review 2024)**
- **Training**
- **Use of vehicles**
- **Volunteers**

* here refers to Director, Charity Manager and Finance Manager

www.cambridgecandi.org.uk

Cambridge Curiosity and Imagination
Cambridge Junction
Clifton Way
Cambridge CB1 7GX

Cambridge Curiosity and Imagination is a Charity (No: 1126253) and Company Limited by Guarantee (No: 6301716).

Adopted 2020 (revised December 2022)

Board Procedures:

All trustees have confirmed that they understand that they are a member and director of the limited company and are aware of their liability. In accordance with the rules of the Charity Commission, trustees agree to give their time on a voluntary basis unless otherwise agreed.

Trustees commit to meet four times a year with additional meetings when necessary.

The Board is managed by a Chairperson.

Business can be transacted at a general meeting only if a quorum is present. A quorum for CCI is 4 members who are entitled to vote.

The agenda should be drawn up by the core team in advance and agreed with the Chair.

Board papers are to be circulated a week in advance including Director's report and Management Accounts.

Trustees commit to join the board for 3 years with an option to stand again if agreed. Trustees are able to resign before the end of their set term. The trustee will need to put their resignation in writing.

A Board recruitment pack is available (March 2022) to support discussions with potential new members. New members of the Board should be discussed and approved in a meeting where a quorum is present if possible. Potential new members identified by core team/trustees should have full board agreement before an invitation is extended.

Observers can be invited to attend meetings.

Complaints

CCI views complaints as an opportunity to learn and improve for the future, as well as a chance to put things right for the person or organisation that has made the complaint.

A complaint is understood here to be any expression of dissatisfaction, whether justified or not, about any aspect of CCI.

All complaint information will be handled sensitively, telling only those who need to know and following any relevant data protection requirements.

Overall responsibility for the complaints procedure and its implementation lies with the management team, supported by the Trustees as appropriate. Further details regarding the handling of complaints are set out in the 'Equal opportunities policy'. Any complaints that are received (whether in person or writing) should be acknowledged and replied to within 4 weeks. Whether the complaint is justified or not, it is expected that the reply to the complainant should describe the action taken to investigate the complaint, the conclusions from the investigation, and any action taken as a result of the complaint. If complaints cannot be satisfactorily concluded at this point, then the Board of Trustees will be involved for further review.

Complaints are reviewed annually to identify any trends which may indicate a need to take further action.

No complaints were received in 2017/18, 2018/19, 2019/2020, 2020/21, 2021/22.

Confidentiality

Cambridge Curiosity and Imagination is committed to maintaining high standards of confidentiality in all aspects of its work. The organisation holds some confidential information. This is provided by, or derived from, voluntary/community organisations, members of the public, third parties and associates.

Confidentiality is essential because we recognise:

- The possible consequences for the organisation or individual if it is breached;
- The rights of organisations and individuals to have control over information about them;
- The duties placed on us whereby breaches of confidentiality could lead to formal complaints, grievance or disciplinary actions, or even legal action against us;
- Good practice and our standards for Customer Care.

CCI seeks to ensure that:

- Confidential records are properly managed.
- Confidential information is only released in accordance with our Data Protection Policy, legislative considerations, best practice and strict guidelines of the organisation.
- Information is only disclosed with the informed consent of the person or organisation to whom the information relates, with the following exceptions:
    - when, by law, we must share information, for example with the Council Tax Office and Inland Revenue;
    - in an emergency, when public safety is at risk and when information is required by the police to prevent or detect crime.
- it promotes a policy that respects commercial sensitivity

CCI confirms that:

- The use of information that Cambridge Curiosity and Imagination collects and processes will be used to provide a service or carry out an authorised or requested transaction.
- Cambridge Curiosity and Imagination will not sell, trade, rent or lend confidential information to anyone.
- Cambridge Curiosity and Imagination does use specified information to provide a Directory of Voluntary/Community Organisations where only permitted contact details and essential information to delivering the service will be provided. No confidential individual information will be included.
- Cambridge Curiosity and Imagination may become privy to certain business information, which will be treated in the same confidential manner as person specific information.

Data protection – Confidentiality and Security

At Cambridge Curiosity and Imagination (CCI), we are committed to protecting any data and ensuring it is securely stored. There is a privacy statement on the CCI websites – this can be read here http://www.cambridgecandi.org.uk/privacy-policy (updated September 2019).

This policy had been updated in April 2018 to reflect the new data protection legislation called the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulation (PECR). GDPR supersedes the Data Protection Directive. We recognise and adhere to the seven principles of data protection as set out in the EU General Data Protection Regulations (GDPR).

Cambridge Curiosity and Imagination recognises the public's and voluntary/community sector's expectation that their personal information will be handled in accordance with the law.

Cambridge Curiosity and Imagination regards the lawful and correct treatment of personal information as important to successful operations and to maintaining the confidence of those people it deals with.

CCI does not share data with partners or other organisations without written permission.

Passwords for data storage are changed annually.

Cyber Crime - The government Cyber Security Breaches Survey 2019 revealed that over two thirds of high income charities had recorded a cyber breach or attack in 2018. Of those charities affected, the vast majority (over 80%) had experienced a phishing attack, which are fraudulent emails. Whilst CCI is not a high income charity associates have been made aware of the Small Charity Guide and we are vigilant to the threat of cyber crime and have insured appropriate defences are in place, including raising awareness with associates and volunteers.

https://ncsc-content.s3.eu-west-1.amazonaws.com/Cyber%20Security%20Small%20Charity%20Guide%202.pdf

If a serious incident were to arise we would report it using this guidance https://www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Charity Guide

This advice has been produced to help charities protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/charity** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- **Identify what needs to be backed up.** Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.
- **Ensure the device containing your backup is *not* permanently connected** to the device holding the original copy, neither physically nor over a local network.
- **Consider backing up to the cloud.** This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- **Switch on PIN/password protection/fingerprint recognition** for mobile devices.
- Configure devices so that when lost or stolen they can be **tracked, remotely wiped** or **remotely locked.**
- Keep your **devices** (and all **installed apps**) **up to date,** using the **'automatically update'** option if available.
- When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs.**
- **Replace devices that are no longer supported by manufacturers** with up-to-date alternatives.

Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- **Use antivirus** software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- **Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the **'automatically update'** option where available.
- **Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.
- **Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges.** This will reduce the impact of successful phishing attacks.
- **Scan for malware** and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like **poor spelling and grammar,** or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/ PIN protection** or **fingerprint recognition** for mobile devices.
- **Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.
- **Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).
- Do not enforce regular password changes; they only need to be changed when you suspect a compromise.
- **Change** the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- **Provide secure storage** so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.
- **Consider using a password manager.** If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

For more information go to www.ncsc.gov.uk @ncsc

Employment

CCI does not operate a pay roll.

All associates are currently employed on free-lance contracts and as such are responsible for their own tax and national insurance contributions.

CCI does not pay sick leave but does endeavour to rearrange work to minimise lost earnings.

There are agreed job descriptions for the 3 roles of Director, Office Manager and Finance Manager.

Terms and conditions for all freelance posts were reviewed in November 2016. These were last reviewed in March 2021.

Letters of contract are written for all roles by the Director. The Director's is written by the Chair of the Board.

The Director carries out an annual review of responsibilities with the Office Manager and Finance Manager.

Equal opportunities

CCI has an *Equal Opportunities Policy* last updated March 2021. This is downloadable from the CCI website and reviewed bi-annually.

The Board recognises that it is responsible for the regular review and successful implementation of this policy. It will next be reviewed in March 2023.

Financial Management:

CCI has a well-tested financial management systems supported by a qualified accountant. Operating as a charity and company limited by guarantee for over ten years, the charity has robust systems for managing income and expenditure including:

- Keeping accounting records to explain transactions and show charity's financial position, monitored by multiple associate members.
- Posting financial records to computer accounts package (VT), kept up to date with bank and reconciled every week
- Reviewing sales ledger regularly
- Four cheque signatories (Ruth Sapsed, Neil Parker, Jo Diver and Richard Mclean), with management accounts and cash flow prepared by third person (Jo Diver)
- Reporting management accounts including cash flow at all trustee's meetings
- Preparing an annual report and statutory accounts to meet legal requirements, all formally approved by the Trustees

Cash flow is managed by:

- Maintaining cashflow forecast, updating weekly to ensure accurate outlook for programme
- Agreeing clear payment terms
- Invoicing promptly
- Encouraging online payments

Safeguarding any assets of the charity:

- All potential income sources are realistic with appropriate contingencies established
- All known costs have been identified and costed together with a contingency for each programme
- Consideration given to impact of depreciation and maintenance costs for equipment
- Remaining vigilant of cyber-crime, in particular phishing emails

Systems are reviewed by key core associates annually with the last review on 24th November 2022.

Fundraising

Procedures related to fundraising are reviewed by the Board regularly. The charity adheres to good fundraising practices as set out by the Information Commissioner's Office (ICO).

Health and Safety

CCI's Health and Safety policy can be downloaded from the website.

The Board recognizes that it is responsible for the regular review and successful implementation of this policy.

Insurance

Cambridge Curiosity and Imagination maintains up-to-date insurance. This is reviewed annually. Currently the policy covers public liability of up to £2,000,000 employer's liability of up to £10,000,000 and trustee liability of up to £250,000.

This cover is arranged through Graham Sykes Insurance, a specialist insurance broker for Media, Arts & Entertainment.

Premises and security

CCI currently owns no premises or vehicles or significant pieces of equipment (i.e. valued at over £250).

Risk Management

The Trustees have conducted their own review of the major risks, financial, physical and operational to which the Charity is exposed and systems have if necessary been modified to mitigate those risks. Procedures have been put in place to minimise both external and internal risks and these procedures are periodically reviewed to ensure that they still meet the needs of the Charity.

The Board understand that major risks for CCI are to be reviewed regularly and reported in a Risk Register. Sections of this are reviewed at every Board meeting.

Safeguarding for children and vulnerable adults

CCI has a *Safeguarding for children and vulnerable policy.* This can be downloaded from the CCI website. It is reviewed bi-annually.

The Board recognizes that it is responsible for the regular review and successful implementation of this policy.

Training

All associates are employed on free-lance contracts so CCI is not contractually obliged to offer external training and development. It is however committed to a continual process of evaluation and reflection to enable the organisation to grow and develop. Where possible project teams are enabled to meet to share practice and CCI endeavours to create capacity for appropriate external training and development within funding applications.

Use of vehicles

CCI does not own any vehicles. All freelancers are expected to take responsibility for the insurance and maintenance of their own vehicles.

Volunteers

CCI does not currently have a formal system for recruiting volunteers.

Where people do support projects on an informal basis, we liaise to brief them clearly in advance about their responsibilities and any relevant health and safety issues, we ensure they have a valid DBS check and ask them to carry this with them. A code of practice will be drawn up in 2023 to support this informal role.

It is the project manager's role to ensure that they are well supported and guided in their role.