Confidentiality and Data Protection Policy

Business Launchpad/Tooting Works

tootingworks.co.uk
020 8516 7700
89 Bickersteth Road,
London, SW17 9SH

Business Launchpad is powered and funded by Tooting Works to Support London's Young Entrepreneurs Since 1988

Confidentiality and Data Protection Policy

Business Launchpad (BLP) is committed to providing a safe environment for young people and volunteers. BLP recognises that trust is essential to providing effective opportunities and is the foundation for all relationships within our programmes. Maintaining confidences is an integral part of building trust between young people, volunteers and the organisation and will be respected at all times, apart from where it conflicts with reporting safeguarding concerns.

All members of staff and volunteers must be aware of the confidential nature of their work and sensitive information they may come across. All staff and volunteers are provided with a brief introduction to confidentiality during their induction and are expected to familiarise themselves with BLP policies in relation to these issues.

In addition, the Data Protection Act 1998 places an obligation on all organisations to implement the 8 guiding principles when obtaining, handling and storing personal information.

BLP therefore states:

Young People

BLP is committed to ensuring that young people are able to share information with staff and volunteers in a confidential manner.

Young people can expect that any information that they give to a member of staff or volunteer is treated as sensitive and confidential and will not be shared, unless:

- It is believed that the young person, or another young person, is in danger or is being harmed. In this case the young person will be told that the information has to be shared with the appropriate agencies and offered support in understanding this.
- The young person discloses that they are involved, or plan to become involved in acts of terrorism.

Staff and Volunteers

All staff and volunteers at BLP are expected to uphold the organisations commitment to confidentiality. This means that all staff and volunteers are expected to:

- Keep records, files and documents stored in a safe and secure manner

- Not discuss any information given by a young person in confidence, unless they have a safeguarding concern or the young person gives their permission
- Tell a young person when information cannot be kept confidential (ie. Where there is a safeguarding concern)
- Encourage a young person to talk to other people (e.g. parents or guardians) or professionals where they feel it would be in the young person's interest

Staff and volunteers can expect that as an organisation BLP will:

- Provide them with a suitable means for storing confidential documents
- Ensure that their own information (e.g. medical or emergency contact information or information in their personnel file) is stored securely, is kept confidential and only seen by colleagues where appropriate in relation to their role
- Safely destroy personnel information when a member of staff or volunteer ceases to work for the organisation
- Take disciplinary action where the Confidentiality Policy is not upheld (unless this is due to child protection concerns a court order has been issued)

Parents/Carers

Parents/Guardians of young people attending BLP's programmes can expect that the information they provide (e.g. medical information, contact information etc) will:

- Be kept in a secure, confidential manner and will only be used for the purpose provided (i.e. to safeguard the health and wellbeing of the young person)
- Enable the club to ensure that parents receive information from the organisation that is necessary e.g. letters and emails regarding information about upcoming events and activities.
- Not be sold
- Will not be shown to other organisations without prior consent.

Definitions

Confidentiality

- Refers to all forms of information including personal information about people using services or employees or volunteers, including information about the organisation or other organisations.

Data Protection

- Concerns only personal information which is recorded, whether this be in electronic or manual format.

The records we keep:

- Personal information, names, addresses, email, contact names, emergency contacts, medical conditions for staff, children of adults, young people and their families including bank and National Insurance numbers if/when applicable.
- Medical reports, safeguarding records, accident and injuries documents including medical intervention.
- Date and times of attendance.
- Applications, Contracts, DBS information, Supervision & Appraisals information, medical and employment records for staff, students and volunteers.

Roles and Responsibilities

The CEO and the board of trustees is responsible for gaining assurance that confidentiality is managed appropriately within BLP and that adequate resources are made available to implement this Policy.

The CEO is responsible for ensuring that all confidential information processed by the charity is handled in line with this Policy and associated procedures and for providing assurance of such to the trustees.

The individual in charge of GDPR compliance is responsible for ensuring that access to confidential information audited in line with BLP's audit policies and procedures.

The individual in charge of GDPR compliance is responsible for providing advice in relation to this Policy.

The CEO is responsible for ensuring that clauses are contained within all contracts in accordance with the confidentiality agreements procedure and that confidentiality training is included in corporate inductions.

Line Managers will be responsible for ensuring that all BLP staff/volunteers have read this Policy, the Information Sharing Policy and Access to Information Policy and are working to the required standard. They will ensure that a high standard of record keeping is maintained by conducting regular audits and will provide training for staff.

All BLP staff/volunteers including contractors and subcontractors with access to confidential information have responsibilities to ensure that they comply with this Policy and with any guidance subsequently produced.

Notification

The information Commissioner maintains a public register of data controllers who process data (information) and who are required to notify their details to the Commissioner.

Sharing information about those at risk

BLP expects staff to discuss any concerns they may have about the welfare of child or young person immediately with the CEO and subsequently to check that appropriate action has been taken.

If both CEO is not available: staff or volunteers must tell an appropriate agency, such as the local authority children's services, the NSPCC or the police, promptly if you are concerned that a child or young person is at risk of, or is suffering, abuse or neglect unless it is not in their best interest to do so.

You don't need to be certain that the child or young person is at risk of significant harm to take this step. If a child or young person is at risk of, or is suffering, abuse or neglect, the possible consequences of not sharing relevant information will, in the overwhelming majority of cases, outweigh any harm that sharing your concerns with an appropriate agency might cause.

When telling an appropriate agency about your concerns, you should provide information about both of the following:

- The identities of the child or young person, their parents and any other person who may pose a risk to them
- The reasons for your concerns, including information about the child's or young person's health, and any relevant information about their parents or carers.

You should ask for consent before sharing confidential information unless there is a compelling reason for not doing so. For example, because:

- A delay in sharing relevant information with an appropriate person or authority would increase the risk of harm of the child or young person
- Asking for consent may increase the risk of harm to the child, young person, you or anyone else.
- You have already decided that disclosure is justified in the public interest.

You should ask the child or young person for consent if they have capacity to give it. If not, you should ask a person with parental responsibility. You should ask for consent from any adults you want to share information about. When asking for consent, you should explain why you want to share information and how it will benefit the child or young person. ***You should also explain the following:***

- what information you will share
- who you will share it with
- how the information will be used?
- where they can go for independent advice and support (see Safeguarding Policy Y:\Policies\Safeguarding Policy\Safeguarding Policy Children Young People and Vulnerable At Risk Adults.docx)

Sharing with third parties

External agents or contractors who process personal data and other confidential information on behalf of Business Launchpad must be aware of BLP's information governance requirements; what they can and cannot do, and who they should contact if things go wrong prior to them given access to BLP's information assets.

All external agents and contractors should complete and sign a confidentiality agreement within their contract. BLP manager's responsible for contracting with third party organisations where access to BLP's information assets is required, should undertake a due diligence check and risk assessment to establish the adequacy of the third party's confidentiality, security and information governance arrangements.

Consequences of breaching the Data Protection Act

Staff and volunteers can be criminally liable if they knowingly or recklessly disclose personal date in breach of the Act.

A serious breach of data protection is also a disciplinary offence and will be dealt with under BLP's disciplinary procedures. If a member of staff or volunteer accesses another employee's/volunteers or young person's personal records without authority this constitutes a gross misconduct offence and could lead to summary dismissal.

Managing Breach of Confidentiality

If accidental disclosure occurs, the responsible BLP manager should take swift action to minimise the damage. They should find out who knows about the incident, talk to them and remind them of their duty to maintain confidentiality.

The breach must be reported in line with BLP information Breach Policy.

All staff and volunteers should help prevent accidental disclosures occurring by regular pointing out that certain information is confidential and checking that people have understood.

Disclosure

Disclosure of personal data and other confidential information should only be made in accordance with BLP's Information Sharing Policy and Information Access Policy.

Disposal

When no longer required, all personal data and other confidential information, including computer printouts, must be disposed of according to Business Launchpad's secure disposal procedures in Disposal of Removable Storage Media 92017-H policy.

Policy Name	***Version***	***Doc ref***
Confidentiality and Data Protection	***2***	

Policy Owner	***Felicia Mattis-Rome***

Approval status

Date adopted by Trustees	02/11/2021		
Date published	27/11/2023	***Date for next review***	***27/11/2024***

Document Control

Reviewers

Name	***Position***
Felicia Mattis-Rome	CEO
Hareg Tamiru	People and Insights Manager
Djolene Leila Dowdye	Operations Assistant