Data protection, confidentiality and code of conduct

1. Introduction

Bloomers Wellbeing / Lles Blodau CIC ("the Organisation") is committed to:

- Protecting personal data
- Maintaining confidentiality
- Ensuring safe, ethical, professional conduct in all roles
- Safeguarding the privacy of children, young people, families, staff, and volunteers

This policy sets out legal responsibilities, expected standards of behaviour, and confidentiality rules.

It applies to:

- All staff
- Volunteers
- Students
- Contractors
- Directors
- Anyone representing the Organisation

2. Legal Framework

The Organisation complies with:

- UK GDPR
- Data Protection Act 2018
- Human Rights Act 1998
- Working Together to Safeguard People (Wales)
- Wales Safeguarding Procedures

We store and process information lawfully, transparently, and securely.

3. Data Protection Principles

All personal data must be:

1. Processed lawfully, fairly, and transparently
2. Collected for specified, explicit, legitimate purposes
3. Adequate, relevant, and limited to what is necessary
4. Accurate and kept up to date
5. Stored securely
6. Retained only for as long as necessary
7. Kept confidential at all times

Only authorised staff may access personal data.

4. Confidentiality

Confidentiality is central to the trust placed in Bloomers Wellbeing by young people and families.

4.1 Absolutely Mandatory Requirement

Staff and volunteers must never discuss conversations, disclosures, or session content with anyone other than the Youth Wellbeing Lead (DSL).
This includes:

- Friends
- Family
- Partners
- Other volunteers
- Other staff
- External agencies
- Schools (unless part of a safeguarding plan authorised by the Youth Wellbeing Lead)

This rule is paramount and must be strictly followed.

4.2 Exceptions (Safeguarding Only)

Confidentiality may be broken only when:

- A child is at risk of significant harm
- Someone else is at risk
- There is a legal obligation to share information (e.g., court order, safeguarding referral)

In all cases:

- Concerns must be reported immediately to the Youth Wellbeing Lead
- The Youth Wellbeing Lead decides on external information-sharing
- Staff must not make referrals or share information independently unless instructed

4.3 Storage of Confidential Information

All records and notes must be:

- Stored securely (digital or locked physical storage)
- Accessible only to authorised safeguarding personnel
- Recorded factually, accurately, and promptly
- Never saved on personal devices
- Never discussed in public or semi-public areas

5. Professional Boundaries & Conduct Standards

Staff and volunteers must model safe, ethical, and professional behaviour at all times.

5.1 General Conduct

- Treat all young people with respect, dignity, and compassion
- Maintain professional boundaries
- Use appropriate language and behaviour
- Follow safeguarding procedures at all times
- Act in the best interests of the child

5.2 Prohibited Conduct

Staff/volunteers must never:

- Share session details with anyone except the Youth Wellbeing Lead
- Form personal or inappropriate relationships with beneficiaries
- Contact young people outside agreed communication channels
- Share personal phone numbers or social media
- Meet beneficiaries outside approved sessions

- Discuss organisational issues publicly or online
- Use drugs or alcohol before or during work
- Discriminate or act in a way that undermines inclusive practice

5.3 Digital Conduct

- Use only Organisation-approved systems
- No screenshots, photos, or audio recordings of sessions
- No communication with young people on personal devices
- Follow online safety and data security guidance

6. Information Sharing

Information will only be shared:

- With the Youth Wellbeing Lead
- Following safeguarding procedures
- With explicit consent where appropriate
- With external agencies only when authorised by the Youth Wellbeing Lead
- On a strict need-to-know basis
- In compliance with GDPR and WSP

Staff must never decide independently what information to share externally.

7. Records and Documentation

All staff and volunteers must:

- Record safeguarding concerns immediately
- Store notes on the Organisation's secure system
- Never store information at home or on personal devices
- Keep records factual, objective, and time-stamped

The Youth Wellbeing Lead will oversee storage, retention, and disposal of records.

8. Subject Access Requests (SARs)

All requests for access to personal data must be referred to the Managing Director. Staff and volunteers must not respond directly.

9. Breaches of Confidentiality or Data Protection

A breach includes:

- Sharing session details with anyone other than the Youth Wellbeing Lead
- Unauthorised access to records
- Misuse of personal data
- Discussing beneficiaries outside professional settings

Breaches will be taken extremely seriously and may result in:

- Removal from role
- Disciplinary action
- Legal or regulatory reporting
- DBS referral (where required)

This policy was approved by the Directors on 2/7/25. This will be reviewed by July 2027.