BELLISSIMO TRAINING CIC

DATA PROTECTION, GDPR, DATA SHARING AND DATA RETENTION POLICY

Policy Owner: Amy Lawrence
Role: Director, Designated Safeguarding Lead (DSL) and Data Protection Lead
Review Date: June 2027

1. Purpose

Bellissimo Training CIC is committed to protecting the privacy, confidentiality and security of all personal information relating to children, young people, parents/carers, staff, volunteers, schools and partner agencies.

This policy explains how personal information is collected, used, stored, shared, retained and disposed of in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and safeguarding requirements.

2. Information We Collect

Bellissimo Training CIC may collect and process:

- Student personal information
- Parent/carer contact details
- Attendance records
- Behaviour and wellbeing records
- Educational progress information
- Individual support plans
- Risk assessments
- Medical information and support needs
- Safeguarding records and disclosures
- Staff and volunteer records
- Emergency contact details
- Accident and incident reports
- Referral information from schools and local authorities

Information collected will be relevant, necessary and proportionate to the services being provided.

3. Data Security

Bellissimo Training CIC takes appropriate technical and organisational measures to ensure personal data remains secure.

These measures include:

- Secure Microsoft 365 Business systems
- Secure business domain email accounts
- Password-protected devices and accounts

- Multi-Factor Authentication (MFA)
- Verification and authentication applications
- Secure cloud-based storage
- Restricted access permissions
- Regular security updates
- Encrypted systems where available
- Locked storage for paper records
- Clear desk and confidentiality procedures

Access to personal information is restricted to authorised personnel on a need-to-know basis.

4. Online Security

Bellissimo Training CIC operates secure internet systems to protect staff and learners.

This includes:

- Secure Wi-Fi networks
- Separate guest Wi-Fi access
- Age-appropriate filtering and monitoring systems
- Secure login credentials
- Password management procedures
- Cyber security awareness for staff

All users are expected to use technology responsibly and in accordance with the provision's Online Safety Policy.

5. Confidentiality

All staff and volunteers must:

- Keep information secure
- Maintain confidentiality
- Share information appropriately
- Follow safeguarding procedures
- Report concerns immediately

Confidential information must never be discussed in public areas or shared with unauthorised individuals.

6. Data Sharing

Bellissimo Training CIC may share information with:

- Schools
- Local Authorities
- Children's Social Care
- Police
- Health professionals
- Safeguarding services
- Early Help services
- Other agencies involved in supporting a child or young person

Information will only be shared when:

- Consent has been obtained where appropriate;
- There is a lawful basis for sharing;
- Sharing is necessary to protect a child or young person from harm; or

- Bellissimo Training CIC is legally required to share information.

Where safeguarding concerns exist, the welfare of the child will take precedence over confidentiality. Information may be shared without consent where there is a lawful safeguarding basis to do so.

7. Data Retention

Bellissimo Training CIC retains information only for as long as necessary to fulfil legal, safeguarding, educational and operational requirements.

Retention Schedule

Record Type	Retention Period
Student Records	7 years after leaving the provision
Attendance Records	7 years
Safeguarding Records	In line with safeguarding requirements and transferred where appropriate
Accident/Incident Records	Until age 21 or longer where required
Staff Records	6 years after employment ends
Volunteer Records	6 years after leaving
DBS Information	Only as long as necessary for recruitment purposes
Financial Records	6 years plus the current financial year
Complaints Records	6 years
Risk Assessments	3 years after being replaced unless linked to an incident

Where records are no longer required they will be securely deleted, destroyed or permanently anonymised.

8. Individual Rights

Under UK GDPR individuals have the right to:

- Be informed about how information is used
- Access their personal information
- Request correction of inaccurate information
- Restrict processing where appropriate
- Object to certain processing activities
- Request a copy of information in a portable format
- Request deletion of personal information where applicable

9. Right to be Forgotten

Individuals have the right to request the deletion of their personal information where there is no lawful reason for Bellissimo Training CIC to continue processing it.

Requests will be considered in accordance with UK GDPR requirements.

However, Bellissimo Training CIC may be unable to delete information where records must be retained for:

- Safeguarding purposes
- Child protection records
- Legal obligations
- Insurance requirements
- Financial records
- Ongoing investigations
- Regulatory compliance

Where information cannot be deleted, the individual will be informed of the reason.

10. Subject Access Requests (SARs)

Individuals may request access to information held about them.

Requests should be made in writing to the Data Protection Lead.

Bellissimo Training CIC will respond within the timescales required under UK GDPR legislation.

11. Data Breaches

Any suspected or actual data breach must be reported immediately to Amy Lawrence, Data Protection Lead.

Breaches will be investigated promptly and, where required, reported to the Information Commissioner's Office (ICO).

Appropriate action will be taken to minimise risk and prevent recurrence.

12. Staff Responsibilities

All staff and volunteers are responsible for:

- Protecting personal information
- Following this policy
- Maintaining confidentiality
- Reporting breaches or concerns immediately
- Completing relevant training
- Following safeguarding procedures

Failure to comply with this policy may result in disciplinary action.

13. Monitoring and Review

This policy will be reviewed annually or sooner if legislation, guidance or operational requirements change.

Approved By: Amy Lawrence
Position: Director, DSL and Data Protection Lead

Review Date: June 2027

Signature: A.Lawrence_____

Date: 18/06/2026_____