Data Protection Policy

Policy information	
Organisation	**Blueberry Academy** **Acting as:** **"Data controller" a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed** **"data processor", in relation to personal data, any person (other than an employee of the data controller) who processes the data on behalf of the data controller.**
Scope of policy	This policy covers all data that either originates from Blueberry, data that is passed on the Blueberry or data which Blueberry passed on from Blueberry. See data Data Flow Map for overview
Policy operational date	25/05/2018 - Policy to be reviewed every 3 years
Policy prepared by	Privacy Lead – Angela Whitehall Directors – Andy Bucklee / Andrew Cambridge
Date approved by Management Team	25th May 2018
Policy review date	Every three years.

Introduction	
Purpose of policy	• Complying with the law • Following good practice • Protecting staff, trainees (& families) and partners • protecting the organisation
Types of data	• Personal data • Sensitive data
Policy statement	Blueberry Academy has a commitment to: • comply with both the law and good practice • respect individuals' rights • be open and honest with individuals whose data is held • provide training and support for staff who handle personal data, so that they can act confidently and consistently • Notify the Information Commissioner voluntarily, even if this is not required
Key risks	Main risks within your organisation: • Data being shared where it's not relevant or inappropriate disclosure of information through inadequate security. • individuals being harmed through data being inaccurate or insufficient or not up to date.

Responsibilities	
The Directors have overall responsibility for ensuring that the organisation complies with its legal obligations.	
Privacy Lead	Responsibilities include: • Briefing the Directors on Data Protection responsibilities • Reviewing Data Protection and related policies • Ensuring that Data Protection induction and training takes place • Advising staff on Data Protection issues • Notification to the ICO • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors
Employees & Volunteers	All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. ('Employees' are both paid employees and volunteers.)
Enforcement	All staff are required to share any breaches with the Privacy Lead and to inform of any practice where they have concerns.

Security	
Setting security levels	All data is treated with the strictest importance and breaches of security will be dealt with disciplinary procedures.
Security measures	• Password protection for all EHCPs and Core Assessments • Usernames and passwords required to access ICT • Data log of all data coming into and out of the organisation • All staff aware of increased need for vigilance with data through training • Staff own laptops and phones password protected • Personal data held only in one location • Data kept offsite kept in locked storage
Specific risks	• passing data without applying security checks • Working off site with data • Remote access to online data • Shared data being passed on inappropriately • Others seeing or overhearing data not for them

Data recording and storage	
Accuracy	Regular checks and reviews for accuracy completed within review meetings. Re-checking data passed on over phone.
Updating	• All inactive data is destroyed after 3 years • Speculative CVs not kept for more than 6 months without express permission from the candidates
Storage	• Staff and Trainee information stored in locked office • Electronic data stored in secure system
Retention periods	• For personalised learners, York Learning will retain specific personal data for 13 years after the learning is completed. This will be information required under our legal obligation and will be the personal data we have processed on the ILR. • Learner portfolios can be collected by the learner upon completion of the course or return of portfolios from awarding bodies. Portfolios will be stored for 6 months before being securely deleted both in hard or electronic copy. • Personal and health information, EHCPs, medical reports, other sensitive records will be deleted within 6 months of trainees leaving the Blueberry Academy. • Electronic records of academic achievements will be deleted within one academic year • Staff data will be deleted within one year of leaving employment unless there is a legal requirement to retain.
Archiving	• Inactive data is moved to archive after 6 months • Inactive data is destroyed after 3 years

Data Subject Rights	
Retaining data	There is some information which we are required to keep for legal reasons. This is information which we need for you to be able to attend the Blueberry Academy. The details are given in our relevant privacy policies which can be provided to you on application to Angela Whitehall, Privacy Lead for Blueberry Academy, 01904 638885 awhitehall@blueberryacademy.co.uk
Accuracy of data	Where data is inaccurate, the information will be updated to make it accurate on production of proof of the updated data.
Deletion of data	Where we are processing your data on a legal basis, we cannot delete this data until the end of the retention period required. Where your permission to retain information has been sought, this data can be deleted on request.

Data Subjects Right of Access	
Responsibility	Privacy Lead ensures right of access requests are handled within the legal time limit of one month from verification of identity.
Procedure for making request	Right of access requests must be in writing. There is a responsibility on all employees to pass on anything which might relate to an access request to the appropriate person without delay. Contact Angela Whitehall- Privacy Lead for Blueberry Academy, 01904 638885 whitehall@blueberryacademy.co.uk
Provision for verifying identity	Where the person managing the access procedure does not know the individual personally there is a requirement to check their identity before handing over any information
Charging	The first request will be free, subsequent requests may incur a charge if they are onerous or vexatious.

Transparency	
Commitment	Data Subjects are aware that their data is being processed and • for what purpose it is being processed • what types of disclosure are likely, and • how to exercise their rights in relation to the data
Procedure	There are standard ways for each type of Data Subject to be informed: • Privacy policies • Employee Handbook • Welcome letter or pack for trainees / parents • Blueberry Academy website
Responsibility	The Privacy Lead is responsible for transparency in relation to different types of Data Subject.

Lawful Basis	
Legal Basis	Data is held on the basis of one of the following: • Legitimate interests • Consent • Contract • Legal obligation • Vital interests
Underlying principles	• All data held by Blueberry Academy is for the purpose of providing the best support possible for trainees and staff • No data is used for commercial purposes
Opting out	In some circumstances, data subjects may opt out of their data being held and used, for example, the Blueberry newsletter mailing list or having photographs used. Permission will be sought where there data subjects may opt out.
Withdrawing consent	Where data subjects have given permission for their data to be used, they can withdraw this permission. In other circumstances there is a legal basis for holding this information.

Employee training & Acceptance of responsibilities	
Induction	All employees who have access to any kind of personal data will have their responsibilities outlined during their induction procedures
Continuing training	There are ongoing opportunities to raise Data Protection issues during employee training, team meetings and supervisions.
Procedure for staff signifying acceptance of policy	Employees will show acceptance of their responsibilities to Data Protection through signing off the staff induction.

Policy review	
Responsibility	The Privacy Lead has responsibility for carrying out the next policy review (in 12 months).
Procedure	The Management team will be consulted in any policy review
Timing	Policy review will be timetabled into the agenda on Management Team meetings.