BRIGHTFIELD

ACADEMY

*Inclusion. Choice. Growth.*

# Data Protection Policy

Protecting personal data.
Upholding rights.
Building trust.

Inclusion. | Choice. | Growth. | Last Update: June 2026

# Data Protection Policy

**BRIGHTFIELD ACADEMY**
**DATA PROTECTION POLICY**
**Policy Owner:** Director
**Responsible Person:** Director / Data Protection Lead
**Data Protection Lead:** Director (or nominated representative)
**Applies To:** All employees, directors, volunteers, contractors, agency staff, consultants, students on placement, visiting professionals and anyone processing personal information on behalf of Brightfield Academy.
**Approval Date:** June 2026
**Review Date:** December 2026
**Version:** 1.0
**Last Update:** June 2026

## 1. Purpose

Brightfield Academy is committed to protecting the privacy, dignity and rights of every learner, family member, employee and stakeholder whose personal information we process.

As an Alternative Provision, we collect and use personal information to provide safe, effective and high-quality education and support services. We recognise that the responsible handling of personal data is fundamental to maintaining trust, protecting individuals and meeting our legal obligations.

This policy establishes the principles, responsibilities and procedures governing the collection, use, storage, sharing, retention and disposal of personal information across all areas of Brightfield Academy's work.

It aims to ensure that personal data is processed lawfully, fairly, transparently and securely whilst supporting the safeguarding, educational and welfare needs of children and young people.

This policy should be read alongside the Academy's:

Safeguarding and Child Protection Policy
Confidentiality Policy
Information Security Procedures
Online Safety Policy
ICT Acceptable Use Policy
Staff Code of Conduct
Records Retention Schedule
Complaints and Compliments Policy
CCTV Policy (where applicable)
Photography and Media Consent Procedures

**2. Scope**

This policy applies to every individual acting on behalf of Brightfield Academy, including:
Directors
Employees
Teachers
Learning Support Staff
Tutors
Volunteers
Contractors
Agency Staff
Consultants
Placement Students
Visiting Professionals
Governors or Advisory Board Members (where applicable)

The policy applies regardless of whether information is:
electronic;
paper based;
photographed;
audio recorded;
video recorded;
handwritten;
stored in cloud systems;
communicated verbally;
transferred electronically.

The policy covers all personal information processed during the operation of Brightfield Academy, including information relating to:
learners;
parents and carers;
employees;
applicants;
volunteers;
contractors;
referring schools;
local authorities;
visitors;
suppliers and partner organisations.

**3. Policy Statement**

Brightfield Academy believes that every individual has the right to expect that their personal information will be handled responsibly, securely and respectfully.

We are committed to:
complying fully with UK data protection legislation;
maintaining the confidentiality of personal information;
protecting individuals from unauthorised disclosure or misuse of their information;
ensuring that information is accurate and up to date;

collecting only the information that is genuinely required;
keeping information only for as long as necessary;
disposing of information securely;
maintaining effective cyber security measures;
ensuring staff understand their responsibilities;
promoting openness regarding how information is used;
supporting safeguarding through lawful information sharing where necessary.
Protecting personal information is everyone's responsibility.
Every member of staff shares responsibility for ensuring that personal information is handled appropriately.

**4. Legislative Framework**
This policy has been developed in accordance with current legislation and statutory guidance, including but not limited to:
UK General Data Protection Regulation (UK GDPR)
Data Protection Act 2018
Human Rights Act 1998
Freedom of Information Act 2000 (where applicable)
Education Act 2002
Children Act 1989
Children Act 2004
Keeping Children Safe in Education (current edition)
Working Together to Safeguard Children (current edition)
Privacy and Electronic Communications Regulations (where applicable)
Computer Misuse Act 1990
Copyright, Designs and Patents Act 1988
Equality Act 2010
Brightfield Academy will monitor changes to legislation and update this policy whenever required.

**5. Data Protection Principles**
Brightfield Academy processes personal information in accordance with the seven principles contained within UK GDPR.
**Principle 1**
**Lawfulness, Fairness and Transparency**
Personal information will always be processed lawfully, fairly and transparently.
Individuals will be informed about:
why information is collected;
how it will be used;
who it may be shared with;
how long it will be retained;
their legal rights.
Privacy Notices will be made available wherever appropriate.

**Principle 2**

**Purpose Limitation**
Information will only be collected for specified, explicit and legitimate purposes.
Personal data will never be used for unrelated purposes unless permitted by law.

**Principle 3**

**Data Minimisation**
Brightfield Academy will only collect information that is necessary for:
education;
safeguarding;
health and welfare;
employment;
legal obligations;
contractual responsibilities.
We will avoid collecting excessive or unnecessary information.

**Principle 4**

**Accuracy**
Reasonable steps will be taken to ensure that personal information is:
accurate;
complete;
current;
corrected promptly where inaccuracies are identified.
Individuals may request correction of inaccurate information in accordance with UK GDPR.

**Principle 5**

**Storage Limitation**
Information will not be retained longer than necessary.
Retention periods will be determined by:
statutory guidance;
safeguarding requirements;
educational regulations;
employment legislation;
contractual obligations;
operational need.
When records reach the end of their retention period, they will be securely destroyed.

**Principle 6**
**Integrity and Confidentiality**
Brightfield Academy will protect personal information through appropriate technical and organisational measures.
These include:
secure premises;
password protection;
encryption where appropriate;
controlled access permissions;
staff training;
cyber security measures;
secure disposal procedures;
regular monitoring.

**Principle 7**
**Accountability**
Brightfield Academy accepts responsibility for demonstrating compliance with data protection legislation.
We will:
maintain appropriate policies;
review procedures regularly;
provide staff training;
investigate breaches;
maintain records where required;
review risks;
continually improve our information governance arrangements.

**6. Relationship Between Data Protection and Safeguarding**
Brightfield Academy recognises that data protection legislation does not prevent appropriate information sharing for safeguarding purposes.
Protecting children and young people is our highest priority.
Where there is concern that a learner may be suffering, or is likely to suffer, abuse or neglect, relevant information will be shared lawfully, proportionately and without unnecessary delay with those agencies responsible for protecting children.
Staff should never refuse to share safeguarding information solely because they believe data protection legislation prevents them from doing so.
Safeguarding decisions will always be guided by statutory safeguarding guidance and the judgement of the Designated Safeguarding Lead.

**7. Definitions**
For the purposes of this policy:
**Personal Data**
Any information relating to an identified or identifiable living person.
Examples include:
name;
address;
date of birth;

photographs;
email address;
telephone number;
attendance records;
assessment results;
learner identifiers;
employment records.

**Special Category Data**
Information requiring additional legal protection, including:
health information;
ethnicity;
biometric information;
religious beliefs;
genetic data;
information concerning sexual orientation (where lawfully processed);
trade union membership.
Such information will only be processed where there is a lawful basis and an additional condition for processing under UK GDPR and the Data Protection Act 2018.

**Processing**
Processing includes any action carried out using personal information, including:
collecting;
recording;
organising;
storing;
retrieving;
consulting;
using;
sharing;
transmitting;
archiving;
deleting;
destroying.

**Data Subject**
The individual to whom the personal information relates.
This may include:
learners;
parents and carers;
staff;
volunteers;
applicants;
contractors;
visitors.

**8. Commitment to Continuous Improvement**
Brightfield Academy recognises that effective data protection is an ongoing responsibility rather than a one-time exercise.
We are committed to regularly reviewing our procedures, responding promptly to changes in legislation and emerging cyber security risks, learning from incidents and strengthening our information governance arrangements.
Data protection forms an integral part of our safeguarding culture, organisational governance and commitment to delivering safe, professional and accountable Alternative Provision services.

**Information Governance**
Brightfield Academy is committed to maintaining effective information governance through clear policies, regular audits, staff training, secure technology, quality assurance and continuous improvement. Information governance forms an integral part of safeguarding, organisational leadership and risk management.

**9. Roles and Responsibilities**
Data protection is a shared responsibility across Brightfield Academy. Every individual working for or on behalf of the Academy has a duty to protect personal information and ensure that it is handled lawfully, securely and respectfully.
Ultimate responsibility for compliance rests with the Director.

**9.1 The Director**
The Director is responsible for ensuring that Brightfield Academy:
complies with all relevant data protection legislation;
maintains effective information governance arrangements;
allocates sufficient resources to ensure compliance;
reviews this policy annually;
ensures appropriate procedures are implemented;
supports a culture of confidentiality and accountability;
monitors compliance through regular audits;
responds appropriately to data breaches;
ensures appropriate staff training is provided;
oversees contracts with third-party data processors;
ensures suitable technical and organisational security measures are in place.
The Director may delegate operational responsibilities whilst retaining overall accountability.

**9.2 Data Protection Lead**
Brightfield Academy will appoint a suitably experienced individual to oversee day-to-day data protection compliance. This role may be undertaken by the Director where appropriate.
The Data Protection Lead will:
provide advice and guidance to staff;
oversee implementation of this policy;
maintain privacy documentation;
support Subject Access Requests;
investigate suspected data breaches;

maintain records of data incidents;
liaise with external agencies where appropriate;
monitor legislative changes;
coordinate staff training;
undertake periodic compliance audits.

**9.3 Designated Safeguarding Lead (DSL)**
The Designated Safeguarding Lead works closely with the Data Protection Lead to ensure that information sharing supports the protection of children.
The DSL is responsible for ensuring that:
safeguarding records remain secure;
safeguarding information is shared appropriately;
confidential child protection records are stored separately where appropriate;
safeguarding decisions are recorded;
statutory safeguarding guidance is followed.
The DSL will always prioritise the safety and welfare of children over concerns about confidentiality where there is a lawful basis to share information.

**9.4 Staff Responsibilities**
Every employee, volunteer and contractor must:
understand this policy;
comply with UK data protection legislation;
complete mandatory training;
maintain confidentiality;
only access information required for their role;
protect passwords;
keep devices secure;
report suspected breaches immediately;
challenge inappropriate information sharing where necessary;
maintain accurate records;
dispose of information securely;
follow all safeguarding procedures.
Failure to comply with this policy may result in disciplinary action and, where appropriate, referral to professional or regulatory bodies.

**9.5 Volunteers, Students and Contractors**
Individuals who are not directly employed by Brightfield Academy but who have access to personal information must:
comply fully with this policy;
complete appropriate induction;
sign confidentiality agreements where appropriate;
receive relevant safeguarding guidance;
access only information required for their role;
immediately report any concerns regarding data security.

**10. Personal Data Processed by Brightfield Academy**
Brightfield Academy processes information necessary to provide safe, effective Alternative Provision services.
Information may include:

**Learner Information**
names;
addresses;
dates of birth;
contact details;
Unique Pupil Numbers;
attendance;
assessment information;
EHCP documentation;
SEND information;
behaviour records;
safeguarding records;
medical information;
dietary requirements;
photographs;
destination information;
progress records.

**Parent and Carer Information**
names;
addresses;
contact numbers;
email addresses;
emergency contacts;
parental responsibility information;
correspondence;
financial information where required.

**Employee Information**
recruitment documentation;
DBS information;
qualifications;
references;
payroll details;
absence records;
appraisal documentation;
disciplinary records;
training records;
pension information.

**Contractor Information**
contact details;
insurance documentation;
DBS status where applicable;
qualifications;
invoices;
contracts.

**11. Special Category Data**

Brightfield Academy recognises that some personal information requires enhanced legal protection.

Special Category Data may include:

medical conditions;
disabilities;
mental health information;
ethnicity;
religious beliefs where relevant;
biometric information where lawfully used;
safeguarding information;
social care involvement.

This information will only be processed where:

there is a lawful basis under UK GDPR; and
an additional condition under the Data Protection Act 2018 applies.

Access will be strictly limited to authorised personnel.

**12. Criminal Offence Data**

Brightfield Academy may process criminal offence data where permitted by law.

Examples include:

DBS checks;
safeguarding information;
allegations;
court orders;
police disclosures.

Such information will be processed with additional safeguards and accessed only where necessary.

**13. Lawful Bases for Processing**

Brightfield Academy will always identify an appropriate lawful basis before processing personal information.

The lawful basis depends upon the nature of the activity being undertaken.

The Academy does not rely upon consent where another lawful basis is more appropriate.

**13.1 Public Task**

Most learner information is processed because Brightfield Academy is providing educational services in the public interest.

This includes:

education delivery;
attendance monitoring;
safeguarding;
assessment;
reporting;
statutory returns.

**13.2 Legal Obligation**
Information may be processed to comply with legal duties including:
safeguarding;
employment law;
health and safety;
taxation;
equality legislation;
regulatory requirements.

**13.3 Contract**
Personal information may be processed where necessary to fulfil contractual obligations.
Examples include:
employment contracts;
supplier agreements;
commissioned services;
payroll administration.

**13.4 Vital Interests**
Information may be shared where necessary to protect someone's life.
This may arise during:
medical emergencies;
safeguarding emergencies;
serious accidents;
emergency evacuations.

**13.5 Legitimate Interests**
Where appropriate, Brightfield Academy may process information under legitimate interests, provided those interests do not override the rights and freedoms of individuals.
Examples may include:
organisational planning;
quality assurance;
fraud prevention;
security monitoring.
Legitimate Interest Assessments will be completed where appropriate.

**13.6 Consent**
Consent will only be relied upon where it is genuinely appropriate.
Where consent is used, it will be:
freely given;
specific;
informed;
unambiguous;
capable of being withdrawn.
Withdrawal of consent will not affect processing already carried out lawfully.

**14. Children's Data**

Brightfield Academy recognises that children's personal information requires particular protection.

All processing involving learners will be undertaken with their welfare, dignity and best interests in mind.

Children's information will:

only be collected where necessary;
be securely stored;
be protected from unauthorised disclosure;
only be shared where lawful;
be retained only for required periods.

Particular care will be taken when processing information relating to vulnerable learners, learners with SEND and those subject to safeguarding concerns.

**15. Data Collection**

Brightfield Academy collects information directly from:

learners;
parents and carers;
referring schools;
local authorities;
previous educational settings;
health professionals;
social care;
external agencies;
employees;
contractors.

Information will only be collected where there is a lawful reason for doing so.

Individuals will normally be informed why information is being collected.

**16. Privacy Notices**

Brightfield Academy will publish clear Privacy Notices explaining:

what information is collected;
why it is collected;
the lawful basis for processing;
who information may be shared with;
how long information is retained;
individuals' legal rights;
how to raise concerns.

Separate Privacy Notices may be issued for:

learners and parents;
staff;
volunteers;
job applicants;
contractors.

Privacy Notices will be written in clear, accessible language.

**17. Data Accuracy**
Brightfield Academy is committed to maintaining accurate records.
Reasonable steps will be taken to ensure that information is:
accurate;
complete;
relevant;
up to date.
Parents, carers, employees and other individuals are encouraged to notify the Academy promptly of any changes to their personal information.
Where inaccuracies are identified, they will be corrected without unnecessary delay.

**18. Data Minimisation**
Brightfield Academy will only collect information that is genuinely required.
Staff should consider:
Is this information necessary?
Why is it needed?
Who requires access?
How long will it be needed?
Is there a less intrusive way of achieving the same purpose?
Unnecessary duplication of records should be avoided.
Staff must not retain unofficial copies of personal information beyond operational need.

**19. Accountability and Good Practice**
Every member of staff is expected to demonstrate good information governance by:
respecting confidentiality;
following Academy procedures;
maintaining secure working practices;
asking for advice where unsure;
reporting concerns immediately;
participating in ongoing training.
Effective data protection supports safeguarding, strengthens trust with families and partner organisations, and underpins the professional standards expected of everyone working within Brightfield Academy.

**20. Information Security**
Brightfield Academy is committed to maintaining appropriate technical and organisational measures to protect all personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access.
Information security is fundamental to safeguarding, maintaining public confidence and complying with UK data protection legislation.
Appropriate security measures will be proportionate to the sensitivity of the information being processed and will be reviewed regularly to address emerging risks.
Security arrangements include, but are not limited to:

•secure buildings and controlled access;
•password-protected systems;
•role-based access permissions;
•encrypted devices where appropriate;
•secure cloud-based services;
•anti-virus and malware protection;
•firewalls and software updates;
•regular backups;
•secure disposal procedures;
•staff training and awareness;
•incident reporting procedures.

**21. Physical Security**
Brightfield Academy will take reasonable steps to prevent unauthorised physical access to confidential information.
This includes:
•locking offices when unattended;
•securing filing cabinets containing confidential records;
•controlling visitor access;
•operating sign-in procedures;
•ensuring confidential discussions take place in private;
•protecting records during transport;
•preventing documents from being left unattended in public areas or vehicles.
Visitors must not have unsupervised access to confidential records unless authorised.

**22. Access Control**
Access to personal information will be granted only where there is a legitimate professional need.
Access permissions will:
•be role-specific;
•be regularly reviewed;
•be removed promptly when employment or contracts end;
•be restricted to the minimum level required.
Staff must never access records out of curiosity or for personal reasons.
Unauthorised access to personal information may result in disciplinary action and, where appropriate, referral to regulatory authorities.

**23. Password Management**
Strong password management is essential to protecting Academy information.
All staff must:
•use unique passwords;
•create passwords of appropriate complexity;
•keep passwords confidential;
•change passwords when instructed or where compromise is suspected;
•use multi-factor authentication where available;
•never share passwords;
•never write passwords where they may be accessed by others.
Passwords must not be stored in unsecured documents or shared by email or text message.

**24. Electronic Devices**
Personal information may only be accessed on authorised devices that meet the Academy's security requirements.
Users must:
•lock devices when unattended;
•install updates promptly;
•maintain anti-virus protection where applicable;
•report lost or stolen devices immediately;
•avoid leaving devices visible in vehicles or public places.
Where personal devices are authorised for work purposes, they must comply with Academy security requirements.

**25. Mobile Working and Remote Working**
Brightfield Academy recognises that staff may occasionally work remotely or access Academy systems from external locations.
When working remotely, staff must:
•access only authorised systems;
•use secure internet connections wherever possible;
•avoid using public Wi-Fi for confidential work unless protected by secure encryption or a VPN;
•ensure screens cannot be overlooked by unauthorised individuals;
•securely store paper records;
•avoid discussing confidential matters in public places;
•log out of systems when work is complete.
Confidential documents should not be printed at home unless authorised and must be disposed of securely.

**26. Email Security**
Email is a common source of accidental data breaches.
Staff must:
•verify recipients before sending confidential information;
•use secure methods for transmitting sensitive information where appropriate;
•check attachments carefully;
•avoid including unnecessary personal information;
•report incorrectly addressed emails immediately.
Personal email accounts must not be used to conduct Academy business involving personal data.
Where encryption is available and appropriate, it should be used for transmitting sensitive information.

**27. Cloud-Based Systems**
Brightfield Academy uses secure digital platforms to support education, safeguarding and organisational management.
Cloud-based services will only be used where appropriate security measures and contractual safeguards are in place.
Examples may include:

•learner management systems;
•assessment platforms;
•attendance systems;
•secure document storage;
•communication platforms;
•educational software.
Only authorised staff will be granted access.
Access permissions will be reviewed regularly.
Data processing agreements will be maintained with external providers where required by law.

**28. Paper Records**
Although many records are stored electronically, paper records remain important.
Paper records containing personal information must:
•be stored securely;
•remain accessible only to authorised personnel;
•not be left unattended in public areas;
•not be removed from Academy premises unless authorised;
•be transported securely;
•be disposed of using confidential waste arrangements when no longer required.
Photocopies containing personal information should be collected immediately from printers.

**29. Secure Disposal**
When information is no longer required and has reached the end of its retention period, it will be securely destroyed.
Appropriate disposal methods include:
•confidential shredding;
•secure destruction services;
•permanent deletion of electronic records;
•destruction of storage media where appropriate.
Staff must never dispose of confidential information using ordinary waste bins.

**30. Photography and Video Recording**
Brightfield Academy recognises the educational value of photography and video whilst respecting individuals' privacy rights.
Images and recordings will only be taken where appropriate and in accordance with Academy procedures.
Appropriate consent will be obtained where required.
Photographs and videos must:
•support legitimate educational or promotional purposes;
•be stored securely;
•only be accessible by authorised individuals;
•not be retained longer than necessary.
Staff must not use personal devices to photograph learners unless specifically authorised under Academy procedures.

**31. CCTV (Where Applicable)**
Where CCTV operates within Academy premises, it will be used only for legitimate purposes such as:
•safeguarding;
•site security;
•crime prevention;
•protection of staff, learners and visitors.
Clear signage will inform individuals that CCTV is in operation.
Images will be retained only for as long as necessary and accessed only by authorised personnel.
The use of CCTV will comply with relevant legislation and the Academy's CCTV procedures.

**32. Social Media**
Personal information relating to learners, families, staff or partner organisations must never be shared through personal social media accounts.
Staff must:
•maintain professional boundaries;
•avoid identifying learners online;
•avoid discussing confidential matters electronically;
•comply with the Staff Code of Conduct;
•follow Academy social media guidance.
Breaches may result in disciplinary action.

**33. Artificial Intelligence and Digital Tools**
Brightfield Academy recognises that artificial intelligence (AI) and other digital technologies may support education and administration.
Before using AI or similar technologies with personal information, staff must ensure that:
•the use is authorised by the Academy;
•personal data is processed lawfully;
•confidential information is not entered into unauthorised systems;
•appropriate contractual and security safeguards are in place;
•the privacy rights of learners, families and staff are protected.
Staff must not upload identifiable learner, parent or employee information to unauthorised AI platforms or publicly available generative AI tools.
Where AI-assisted systems are approved for educational or administrative use, staff will receive appropriate guidance and training.

**34. Information Sharing**
Brightfield Academy recognises that effective information sharing supports education, safeguarding and partnership working.
Information will only be shared where:
•there is a lawful basis;
•sharing is necessary;
•sharing is proportionate;
•the information is accurate;
•only relevant information is disclosed;
•appropriate security measures are used.

Information may be shared with:
•referring schools;
•local authorities;
•children's social care;
•police;
•health professionals;
•educational psychologists;
•CAMHS and mental health services;
•youth justice services;
•other agencies supporting the learner.
All information sharing decisions should be capable of being justified and, where appropriate, recorded.

**35. Safeguarding Information Sharing**
Where there are concerns regarding the safety or welfare of a child or young person, Brightfield Academy will share relevant information without unnecessary delay in accordance with statutory safeguarding guidance.
Staff must not refuse to share safeguarding information solely because they believe data protection legislation prevents them from doing so.
The Designated Safeguarding Lead will determine the most appropriate course of action and maintain appropriate records of safeguarding decisions.
Protecting children always takes priority over maintaining confidentiality where there is a lawful safeguarding basis to share information.

**36. Third-Party Data Processors**
Where Brightfield Academy engages external organisations to process personal data on its behalf, appropriate contractual arrangements will be established.
The Academy will seek assurance that third-party processors:
•comply with UK GDPR and the Data Protection Act 2018;
•implement appropriate security measures;
•process information only on documented instructions;
•report data breaches promptly;
•assist the Academy in meeting its legal obligations;
•securely return or destroy data at the end of the contractual relationship.
Examples may include providers of educational software, payroll services, IT support, secure document storage and commissioned specialist services.

**37. Monitoring Information Security**
Brightfield Academy will regularly review the effectiveness of its information security arrangements through:
•internal audits;
•compliance checks;
•password and access reviews;
•safeguarding audits;
•ICT security reviews;
•incident analysis;
•staff supervision and training.
Lessons learned from audits, incidents or emerging cyber security threats will be used to strengthen the Academy's information governance arrangements and reduce future risk.

**38. Individual Rights**
Brightfield Academy recognises and respects the rights of individuals under the UK General Data Protection Regulation (UK GDPR).
Requests relating to personal data will be handled promptly, fairly and in accordance with statutory timescales.
Individuals will not be disadvantaged for exercising their legal rights.

**39. Right to be Informed**
Individuals have the right to understand:
•what personal information is collected;
•why it is collected;
•the lawful basis for processing;
•who information may be shared with;
•how long information will be retained;
•how information is protected;
•how to exercise their rights.
Brightfield Academy fulfils this obligation through clear Privacy Notices and transparent communication.

**40. Right of Access (Subject Access Requests)**
Individuals have the right to request access to personal information held about them.
Requests may be made in writing, electronically or verbally.

**Making a Subject Access Request**
Requests for access to personal information should normally be directed to:

*Data Protection Lead***,** Brightfield Academy or alternatively to Nik Larcombe (07395 111919)
Email: **office@brightfieldacademy.co.uk** **or nik@brightfieldacademy.co.uk**

Requests may be made verbally or in writing and do not need to use the words “Subject Access Request” to be valid. Any member of staff receiving such a request must promptly forward it to the Data Protection Lead.

Brightfield Academy will:
•acknowledge requests promptly;
•verify the identity of the requester where appropriate;
•locate all relevant information;
•consider any applicable exemptions;
•provide the information without undue delay and normally within one calendar month, unless legislation permits an extension.
Where requests are complex or numerous, the individual will be informed if additional time is required.
The Academy may refuse or limit disclosure only where permitted by law.

**41. Right to Rectification**
Individuals may request correction of inaccurate or incomplete personal information.
Brightfield Academy will:
•investigate the request;
•amend inaccurate information where appropriate;
•inform relevant third parties where required and practicable;
•explain any decision where the request cannot be fulfilled.

**42. Right to Erasure**
Individuals may request deletion of personal information in circumstances permitted by UK GDPR.
However, Brightfield Academy may be legally required to retain information where:
•safeguarding obligations apply;
•education legislation requires retention;
•employment legislation applies;
•legal proceedings are anticipated or ongoing;
•statutory record retention requirements exist.
Requests for erasure will therefore be considered carefully on a case-by-case basis.

**43. Right to Restrict Processing**
Individuals may request that processing of their information is restricted where:
•accuracy is disputed;
•processing is believed to be unlawful;
•information is no longer required but must be retained for legal purposes;
•an objection is under consideration.
Where processing is restricted, information will continue to be stored securely but will not normally be used unless legally permitted.

**44. Right to Data Portability**
Where applicable, individuals may request that personal information they have provided is transferred to another organisation in a structured, commonly used and machine-readable format.
This right applies only in circumstances defined by UK GDPR.

**45. Right to Object**
Individuals may object to certain forms of processing where permitted by law.
Brightfield Academy will consider each objection carefully and will cease processing where legally required.
This right does not normally prevent the Academy from carrying out its statutory educational or safeguarding functions.

**46. Automated Decision Making and Profiling**
Brightfield Academy does not make significant decisions about learners or employees based solely on automated processing.
Professional judgement will always be applied to decisions affecting:
•education;
•safeguarding;

•welfare;
•employment.
Where technology supports decision making, appropriate human oversight will always be maintained.

**47. Records Management**
Accurate record keeping supports safeguarding, education, accountability and legal compliance.
Brightfield Academy will ensure that records are:
•accurate;
•factual;
•objective;
•securely maintained;
•appropriately indexed;
•accessible only to authorised individuals;
•retained only for appropriate periods.
Staff must not create unofficial record systems outside authorised Academy processes.

**48. Records Retention**
Personal information will only be retained for as long as necessary.
Retention periods will reflect:
•statutory guidance;
•Department for Education guidance;
•safeguarding requirements;
•employment legislation;
•contractual obligations;
•operational necessity.
A detailed Records Retention Schedule forms part of this policy.
Once retention periods expire, information will be securely destroyed.

**49. Data Breaches**
A personal data breach is any security incident leading to the accidental or unlawful:
•destruction;
•loss;
•alteration;
•unauthorised disclosure;
•unauthorised access
to personal information.

Examples include:
•sending information to the wrong recipient;
•lost paperwork;
•lost laptops or mobile devices;
•unauthorised access to records;
•cyber attacks;
•phishing incidents;
•accidental publication of confidential information.
All staff have a duty to report suspected breaches immediately.

**50. Reporting Data Breaches**
Any actual or suspected breach must be reported immediately to the Director or Data Protection Lead.
The Academy will:
•contain the incident;
•assess potential harm;
•preserve evidence where appropriate;
•investigate the circumstances;
•identify affected individuals;
•determine whether reporting to the Information Commissioner's Office (ICO) is required;
•implement corrective actions;
•record lessons learned.
Failure to report known breaches may result in disciplinary action.

**51. Information Commissioner's Office (ICO)**
Where a personal data breach presents a risk to the rights and freedoms of individuals, Brightfield Academy will notify the ICO without undue delay and, where required by law, within 72 hours of becoming aware of the breach.
Where a breach presents a high risk to affected individuals, they will also be informed unless an exemption applies.
All reportable breaches will be documented, regardless of whether notification to the ICO is required.

**52. Complaints**
Individuals who believe their personal information has been handled incorrectly are encouraged to raise concerns with Brightfield Academy in the first instance.
Complaints will be investigated fairly, promptly and confidentially.
Where concerns cannot be resolved internally, individuals have the right to complain to the Information Commissioner's Office.

**53. Staff Training**
Effective data protection depends upon knowledgeable and confident staff.
Brightfield Academy will provide:
•data protection awareness during induction;
•regular refresher training;
•safeguarding training;
•cyber security awareness training;
•guidance on secure information handling;
•updates following legislative changes.
Additional training will be provided where roles involve increased responsibility for personal information.

**54. Monitoring and Audit**
Compliance with this policy will be monitored through:
•internal audits;
•safeguarding audits;
•information security reviews;
•records management checks;
•password and access audits;
•quality assurance activities;
•incident reviews;
•staff supervision;
•policy reviews.
Monitoring findings will be used to improve organisational practice and reduce future risk.

The Director or Data Protection Lead will complete the **Annual Data Protection Compliance Checklist (Appendix G)** at least annually.
Any actions identified will be recorded, allocated to an appropriate individual and monitored through Brightfield Academy's Quality Assurance Framework until completed.
Monitoring outcomes will be reported as part of the Academy's annual governance and policy review process.

**55. Non-Compliance**
Failure to comply with this policy may result in:
•additional training;
•management action;
•disciplinary procedures;
•termination of contracts;
•referral to professional bodies where appropriate;
•legal action where required.
Deliberate or reckless misuse of personal information may constitute gross misconduct.

**56. Related Policies**
This policy should be read alongside the following Brightfield Academy policies and procedures:
•Safeguarding and Child Protection Policy

•Confidentiality Policy
•Online Safety Policy
•ICT Acceptable Use Policy
•Staff Code of Conduct
•Health and Safety Policy
•Complaints and Compliments Policy
•Safer Recruitment Policy
•Records Retention Schedule
•Business Continuity Plan
•Information Security Procedures
•Photography and Media Procedures
•CCTV Policy (where applicable)

**57. Policy Review**

This policy will be reviewed:
•annually;
•following significant legislative changes;
•following serious data breaches;
•following recommendations arising from audits or inspections;
•where operational changes require revision.
The Director is responsible for ensuring that the policy remains current, effective and reflects best practice.
**Last Update:** June 2026

**APPENDIX A**

**Data Breach Reporting Procedure**

Any member of staff who becomes aware of a suspected or actual personal data breach must:
1.Take immediate steps to contain the breach where safe to do so.
2.Inform the Director or Data Protection Lead immediately.
3.Do not attempt to conceal or delete evidence.
4.Record:
    1. what happened;
    2. when it occurred;
    3. who was involved;
    4. what information may have been affected.
5.Cooperate fully with any investigation.
6.Implement any corrective actions identified.

**APPENDIX B**

**Subject Access Request Procedure**

Requests should normally be directed to the Data Protection Lead at office@brightfieldacademy.co.uk or to Nik Larcombe at nik@brightfieldacademy.co.uk

However, a Subject Access Request received by any member of staff must be recognised and forwarded promptly to the Data Protection Lead.

Upon receiving a Subject Access Request, Brightfield Academy will:

•verify identity where appropriate;
•record the request;
•locate all relevant information;
•consider any legal exemptions;
•prepare the information securely;
•respond within the statutory timescale;
•retain a record of the request and response.

**APPENDIX C**

**Education Records Retention Schedule**

Brightfield Academy will retain records in accordance with statutory guidance, Department for Education requirements and operational need.

Examples include:

•learner educational records;
•safeguarding records;
•attendance records;
•personnel files;
•recruitment documentation;
•DBS records;
•accident records;
•complaints;
•health and safety documentation;
•financial records.

Detailed retention periods will be maintained separately and reviewed regularly to reflect current legislation.

**APPENDIX D**

**Staff Data Handling Standards**

Every member of staff is expected to:

•protect confidential information;
•challenge poor practice;
•use authorised systems only;
•maintain secure passwords;
•lock devices when unattended;
•report incidents immediately;
•comply with Academy procedures;
•complete mandatory training.

**APPENDIX E**

**Data Protection Quick Reference Guide**

Before handling personal information, ask yourself:

•Do I need this information?
•Am I authorised to access it?
•Is it accurate?
•Is it stored securely?
•Am I sharing it lawfully?
•Does the recipient genuinely need to know?
•Am I complying with safeguarding responsibilities?
•Would I be comfortable explaining my actions during an inspection or audit?

If the answer to any question is **No** or **I'm not sure**, seek advice from the Director or Data Protection Lead before proceeding.

**Policy Statement**

Brightfield Academy is committed to protecting the personal information entrusted to us by learners, families, staff and partner organisations. We will process personal data lawfully, fairly, transparently and securely while ensuring that information is shared appropriately to safeguard children and support high-quality education.

Protecting personal information is everyone's responsibility, and safeguarding the welfare of children and young people will always remain our highest priority.

## 58. Data Protection Impact Assessments (DPIAs)

Brightfield Academy will undertake a Data Protection Impact Assessment (DPIA) whenever a new project, system or process is likely to result in a high risk to the rights and freedoms of individuals.

Examples include:

* introducing new learner management systems;
* implementing CCTV in new locations;
* adopting new digital learning platforms;
* introducing biometric technologies;
* significant changes to existing data processing activities.

**A DPIA will:**

- describe the proposed processing;
- identify lawful bases;
- assess risks to individuals;
- identify measures to reduce or eliminate those risks;
- be reviewed before implementation.

## 59. Information Asset Management

Brightfield Academy will maintain an overview of the personal information it holds.

Information assets include:

* learner records;
* safeguarding records;
* staff personnel files;
* attendance systems;
* assessment systems;
* finance records;
* email systems;
* cloud storage;
* paper archives.

Each information asset will have an identified person responsible for ensuring that information is:

* accurate;
* secure;
* appropriately accessed;
* retained correctly;
- disposed of safely.

## 60. Procurement and Third-Party Suppliers

Before purchasing or using new software or digital services, Brightfield Academy will consider:

* compliance with UK GDPR;
* security standards;
* data hosting arrangements;
* contractual protections;
* availability of Data Processing Agreements;
* cyber security credentials;
* safeguarding implications.

Personal information will not be entrusted to suppliers that cannot demonstrate appropriate security and legal compliance.

## 61. International Transfers

Brightfield Academy will take appropriate steps before transferring personal information outside the United Kingdom.

Where international transfers are necessary, the Academy will ensure that appropriate safeguards are in place in accordance with UK GDPR.

Staff must not independently upload Academy information to overseas services that have not been approved.

## 62. Business Continuity and Disaster Recovery

Personal information must remain protected during emergencies.

In conjunction with the Business Continuity Plan, Brightfield Academy will:

* maintain secure backups where appropriate;
* protect critical records from loss;
* ensure continuity of safeguarding information;
* restore access to essential systems as quickly as reasonably possible;
* review lessons learned following significant incidents.

## 63. Monitoring Compliance

Compliance will be evaluated through:

* annual policy review;
* safeguarding audits;
* information governance audits;
* file sampling;
* records management checks;
* cyber security reviews;
* staff supervision;
* quality assurance activities;
* inspection preparation.

Where weaknesses are identified, an action plan will be implemented and monitored.

## 64. Responsibilities of All Staff

Every person working for Brightfield Academy is expected to:
* understand this policy;
* complete required training;
* handle information professionally;
* challenge unsafe practices;
* report concerns promptly;
* support continuous improvement;
* contribute to a culture of confidentiality and accountability.

Compliance with this policy forms part of every employee's professional responsibilities.

## 65. Equality, Inclusion and Accessibility

Brightfield Academy will apply this policy fairly and consistently.
Information relating to protected characteristics will be processed only where necessary and lawful.
Privacy information and data protection guidance will be made available in accessible formats where reasonably required.

## 66. Quality Assurance

The effectiveness of this policy will be measured through:
* audit outcomes;
* inspection findings;
* incident trends;

* staff training completion rates;
* feedback from learners, families and commissioning bodies;
* internal quality assurance reviews.

Recommendations arising from these activities will inform future policy development.

**67. Approval**

This policy has been approved by the Director of Brightfield Academy and applies to all staff, volunteers, contractors and others working on behalf of the Academy.

All personnel are required to confirm that they have read, understood and will comply with this policy.

**APPENDIX F**

**Staff Declaration**

I confirm that I have:

* read the Brightfield Academy Data Protection Policy;
* understood my responsibilities under UK GDPR and the Data Protection Act 2018;
* understood my responsibilities regarding confidentiality and safeguarding;
* agreed to handle personal information securely and professionally;
* agreed to report any actual or suspected data breach immediately.

**Name:** _____

**Role:** _____

**Signature:** _____

**Date:** _____

**Policy Commitment**

Brightfield Academy is committed to protecting personal information with integrity, professionalism and respect. Through robust governance, secure systems, well-trained staff and a culture of accountability, we will ensure that personal data is handled lawfully and responsibly in support of our learners, families, staff and partner organisations.

The Academy recognises that effective data protection is fundamental to safeguarding children, maintaining public confidence and delivering high-quality Alternative Provision services.

# Appendix B: Subject Access Request (SAR) Procedure

## How to Make a Subject Access Request

Requests should normally be directed to the Data Protection Lead at **dataprotection@brightfieldacademy.co.uk**. However, a Subject Access Request received by any member of staff must be recognised and forwarded promptly to the Data Protection Lead.

Requests may be made verbally or in writing and do not need to use the words "Subject Access Request" to be valid.

## Brightfield Academy will:

1. Acknowledge requests promptly (within 5 working days).
2. Verify the identity of the requester.
3. Retrieve relevant information.
4. Provide the information within 1 month of receipt.
5. Extend the timescale by up to 2 months where the request is complex (rare).
6. Inform the requester of their right to complain to the ICO if unhappy with the response.

## Important Notes

- We will not charge a fee unless the request is manifestly unfounded or excessive.
- Third-party information (relating to other individuals) will be redacted.
- Safeguarding information relating to other children, staff or adults will not be disclosed.

# APPENDIX G

## ANNUAL DATA PROTECTION COMPLIANCE CHECKLIST

The Director or Data Protection Lead should review the following at least annually:

| CHECK | COMPLETED |
|---|---|
| 1. Policy reviewed and updated | ☐ |
| 2. Privacy Notices reviewed | ☐ |
| 3. Staff training completed | ☐ |
| 4. New starters inducted | ☐ |
| 5. Leavers' access removed | ☐ |
| 6. Password and access review completed | ☐ |
| 7. Data sharing agreements reviewed | ☐ |
| 8. Third-party processors reviewed | ☐ |
| 9. Records retention audit completed | ☐ |
| 10. Secure disposal procedures checked | ☐ |
| 11. Data breach log reviewed | ☐ |
| 12. Cyber security measures reviewed | ☐ |
| 13. Business continuity arrangements tested | ☐ |
| 14. Safeguarding records storage reviewed | ☐ |
| 15. Quality assurance audit completed | ☐ |

**REMINDER:** Any areas identified as incomplete or requiring improvement should be recorded in the action plan, with timescales and responsibilities agreed and monitored.