Bristol Dyslexia Centre

11 Upper Belgrave Road
Clifton, Bristol BS8 2XH
Tel: 0117 973 9405
office@dyslexiacentre.co.uk
www.dyslexiacentre.co.uk

Principal: Mrs Pat Jones OBE B.Ed (Hons) S.E.N.,Sp.L.D.Ir.Sc.CMBDA

Co. Registration: 4061265

Reviewed: September 2024

Bristol Dyslexia Centre - Data Protection Policy

Our Commitment:

Bristol Dyslexia Centre is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act 1998 (DPA).
https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/
Changes to data protection legislation (GDPR May 2018, UK Data Protection Bill 2018) shall be monitored and implemented in order to remain compliant with all requirements.
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

BDC is not required to appoint a DPO under the GDPR but we have decided to do so voluntarily. We understand that the same duties and responsibilities apply had we been required to appoint a DPO.

The members of staff responsible for data protection are Pat Jones (Director) assisted by Cate Hewitt (Manager). However all staff must treat all student information in a confidential manner and follow the guidelines as set out in this document. The centre is also committed to ensuring that its staff are aware of data protection policies, legal requirements and that adequate training is provided.

The requirements of this policy and the signing of a confidentiality agreement are mandatory for all staff employed by the centre and any third party contracted to provide services within the centre.

Notification:

Our data processing activities are registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. This will be done within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will also inform those individuals without undue delay.

We will keep a record of any personal data breaches, regardless of whether we are required to notify.

Personal Data:

All personal data within the centre's control is handled in compliance and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

Lawful Basis for Processing Data:

The lawful basis for Bristol Dyslexia Centre processing personal and sensitive data are as follows –

Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract. This is used for the provision of all services within the centre, waiting lists for services and for staff contracts.

Consent: the individual has given clear consent for processing their personal data for a specific purpose. This is used for sharing of educational information with a child's school and the taking and use of photos of services users for publication or promotional purposes.

Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

Data will only be shared with external parties in circumstances where it is a legal requirement to provide such information. The intention to share data relating to individuals to an organisation outside of our centre shall be clearly defined with details of the basis for sharing given.

Any proposed change to the processing of individual's data shall first be notified to them.

Photographs and Video:

Images of service users may be captured at appropriate times and as part of educational activities. Photographs are for use within the centre only. Consent will be obtained before the centre uses such images for publication or communication to external sources.
It is the centre's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

Data Security:

We shall undertake an assessment of the associated risks of proposed processing and the impact on an individual's privacy in holding data related to them to comply with the protection of all data being processed and any decisions in the changing of that process.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

There may be circumstances where the centre is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authorities. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The security arrangements of any organisation with which data is shared shall also be considered and these organisations shall provide evidence of the competence in the security of shared data:

For Bristol City Council see:
https://www.bristol.gov.uk/data-protection-foi

For South Gloucestershire Council see:
http://www.southglos.gov.uk/council-and-democracy/data-protection-and-freedom-of-information/data-protection-policy/

For North Somerset Council see:
https://www.n-somerset.gov.uk/my-council/data-protection-foi/data-protection/dataprotection/

Microsoft:
https://www.microsoft.com/en-us/trustcenter/privacy/gdpr
https://www.microsoft.com/en-us/trustcenter/privacy/gdpr/solutions

Office 365 Cloud storage
https://products.office.com/en-us/business/office-365-trust-center-compliance

Windows
https://www.microsoft.com/en-us/TrustCenter/CloudServices/windows-gdpr

Apple – (iPads)
https://www.apple.com/uk/legal/privacy/en-ww/

Nessy – online reading and spelling programme: Only information are names, date of birth and progress information from using the software
https://www.nessy.com/us/privacy-policy/

Doodle Maths – online maths programme. Only information are names and progress information from using the software: https://www.doodlemaths.com/privacy-policy/
For Atlantic data (secure registered service used for DBS disclosure applications) see:
https://gdpr.disclosures.co.uk/

Location of Information and Data:

Hard copy data, records, and personal information are stored in an office with keycode entry. This is made available only to appropriate staff members. Within the office, folders are stored in locked filing cabinets. The only exception to this is medical information that may require immediate access during the day. This will be stored with the first aid kits in the staff room.

Electronic records are stored on a secured encrypted server and backed up to secure encrypted cloud storage service. Students' records are stored on a separate hard drives only accessible by staff members via staff log in and password. Children use a student only profile where no sensitive data is stored.

Sensitive or personal information and data should not be removed from the centre, however the centre acknowledges that some staff may need to transport data between the centre and their home in order to access it for work in the evenings and non-work days. This may also apply in cases where staff have offsite meetings.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off site. If there is no way to avoid taking a paper copy of data off site (i.e. it is to be taken to a meeting), the information should be signed out in the office record book; should not be on view in public places, or left unattended under any circumstances.

- Electronic documents needed for working from home should be uploaded to office 365 and accessed through your office 365 account. If this is not possible (ie. no internet access) then information may be downloaded onto an encrypted (password protected) USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only.

- Office 365 is used to access staff email and stored documents remotely, personal emails are not be used when sending info relating to students at the centre.

- Sensitive documents sent as attachments, (reports, action plans, etc) must always be sent in a secured format and password protected, sending a separate message to the receiver with the password. Only use initials for the student if emailing the child's school and always CC the parents into any communication with the school.

- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.

- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

- These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal:

Teaching records will be stored for 5 years from the year of the pupil's departure from the centre; Psychologist and specialist assessment reports carried out at BDC will be stored electronically for a period of 10 years.

Records will be audited annually and those exceeding the holding period will be securely destroyed.

The centre recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall be destroyed securely and only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

Disposal of IT assets holding data shall be in compliance with ICO guidance:
https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

The centre has identified a qualified source for disposal of IT assets and collections. Details can be found here: http://www.prmgreentech.com/

User Rights:

Information Right – the right to receive the information contained in this policy and our data collection forms about the way we process your personal data.

Personal Data Access Right – the right to know that we are processing your personal data and, in most circumstances, to have a copy of the personal data of yours that we hold. You can also ask for certain other details such as what purpose we process your data for and how long we hold it.

Personal Data Correction Right – You have the right to request that we correct inaccurate data or complete incomplete data that we hold on you.

Personal Data Erasure Right – Known as the right to be forgotten. Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the centre including any data held by contracted processors.

Personal Data Restriction Right – You have the right to restrict the way we process your personal data in certain circumstances, for example: if you contest the accuracy of the data, if our processing is unlawful, to pursue legal claims, where we are relying on legitimate interests to process data.

Data Processing Objection Right – You have the right to object to us processing your data for (i) direct marketing purposes (ii) scientific or historical research or statistical purposes and (iii) purposes of profiling related to direct marketing or based on our legitimate interests or on the performance of a task in the public interest.

Data Portability Right – you have the right to receive a copy of certain personal data or to have it transferred to another organisation in some circumstances.

Right to Withdraw Consent - Where we use your personal information based on your prior consent, you can withdraw your consent at any time by contacting us.

Data Access Requests (Subject Access Requests):

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within 40 days and they should be made in writing to: P. Jones, Bristol Dyslexia Centre 11 Upper Belgrave Rd, Clifton, Bristol BS8 2XH or office@dyslexiacentre.co.uk

Data will be provided free of charge. A reasonable administrative fee may be applied to process the request where it is deemed to be manifestly unfounded, excessive or repetitive.

Personal data about service users will not be disclosed to third parties without the consent of the person, or child's parent or carer if under 18 years, unless it is obliged by law or in the best interest of the child.

Data may be disclosed to the following third parties without consent:

- Police and courts: If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

- Social workers and support agencies: In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

We may be obliged to share your name and contact details with the Track and Trace service.

ICO Code of practice for SARs:
https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf