The Data Protection and GDPR (General Data Protection Regulations) Policy

Introduction

This policy outlines how The Dyslexia Association (TDA) collects, processes, stores, and protects personal data in compliance with the UK GDPR, Data Protection Act 2018, and the Data (Use and Access) Act 2025.

TDA holds personal data about employees, clients, suppliers, and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that employees, workers, associates, and volunteers (known as 'staff' for the purposes of this policy) understand the rules governing their use of personal data to which they have access in the course of their work. This policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

The Dyslexia Association has a commitment to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all our legal obligations.

The Principles of the General Data Protection Regulation (GDPR)

The Dyslexia Association will comply with the principles of Data Protection specified in the EU General Data Protection Regulation (GDPR). TDA (The Dyslexia Association) will make every effort possible to comply with these principles. The principles are:

1. **Lawful, fair, and transparent**
   Data collection must be fair, for a legal purpose and TDA must be open and transparent about how the data will be used.
2. **Limited for its purpose**
   Data can only be collected for a specific purpose
3. **Data minimisation**
   Any data collected **must** be necessary and not excessive for its purpose
4. **Accurate**
   The data we hold must be accurate and kept up to date
5. **Retention**
   Data must not be stored for longer than is necessary
6. **Integrity and confidentiality**
   All data held must be kept safe and secure

***TDA do not use automated decision-making systems. If, in the future, this changes TDA will inform individuals of ADM use, give individuals the right to request a human review, and we will put other safeguards in place to prevent bias or harm.**

Employee Data

TDA takes the security and privacy of your data seriously. We need to gather and use information, or 'data,' about staff as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 act') and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

This policy applies to current and former staff, apprentices, and consultants, and anyone falling into fall into these categories, is considered a 'data subject' for the purposes of this policy, and this policy should be read alongside any contract of employment (or contract for services) and any other notice we issued to data subjects in relation to their data.

TDA has separate policies and privacy notices in place in respect of job applicants, customers, suppliers, and other categories of data subject. A copy of these can be obtained from the central operations team.

TDA has measures in place to protect the security of data, and all staff are expected to familiarise themselves with their obligations under the Data Protection Act.

TDA will only hold data for as long as necessary for the purposes for which it was collected.

TDA is a 'data controller' for the purposes of personal data. This means that we determine the purpose and means of the processing of any personal data.

This policy explains how TDA will hold and process personal information. It explains the rights of a data subject, and explains obligations when obtaining, handling, processing, or storing personal data while working for, or on behalf of, TDA.

How we Define Personal Data

'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include any anonymised data. This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by the individual, or someone else (such as a former employer, a doctor, or a credit reference agency), or it could be created by TDA. It could be provided or created during the recruitment process or during the contract of employment (or services) or after its termination.

TDA will collect and use the following types of personal data:

- Recruitment information such as an application form and/or CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments.
- Contact details and date of birth.
- Contact details of emergency contacts.
- Gender
- Marital status and family details.
- Information regarding the contract of employment (or services) including start and end dates of employment, role, and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits, and holiday entitlement.
- Bank details and information in relation to tax status including national insurance numbers.
- Identification documents including passport and driving licence and information in relation to any immigration status and right to work in the UK.
- Information relating to disciplinary or grievance investigations and proceedings.
- Information relating to performance and behaviour at work.
- Training records.
- Electronic information in relation to the use of IT systems/swipe cards/telephone systems.
- Physical images (whether captured on CCTV, by photograph or video),
- Any other category of personal data which TDA may use (with notification) from time to time.

How we Define Special Categories of Data

'Special Categories of personal data' are types of personal data consisting of information as to:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic or biometric data.
- Health.
- Sexual orientation; and
- Criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

In most cases where we process special categories of personal data, we will require the data subject's explicit consent to do this unless exceptional circumstance apply, or we are required to do this by law (for example to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

How we Define Processing

'Processing' means any operation which is performed on personal data such as:

- Collection, recording, organisation, structuring, or storage.
- Adaptation or alteration.
- Retrieval, consultation, or use.
- Disclosure by transmission, dissemination or otherwise making available.
- Alignment or combination; and
- Restriction, destruction, or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

How we will Process your Personal Data

TDA will process personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.
TDA will use personal data for:

- Performing the contract of employment (or services)
- Complying with any legal obligation; or
- If it is necessary for legitimate interests (or for the legitimate interests of someone else). However, TDA can only do this if your interests or rights do not override ours (or theirs). Individuals have the right to challenge TDA legitimate interests and request that we stop this processing.

TDA can process your personal data for these purposes without the knowledge or consent of the individual. TDA will not use personal data for any unrelated purpose without telling the data subject about it and the legal basis intended to rely on for the processing of it.

Examples of processing personal data

TDA must process personal data in various situations during the recruitment process, employment (or engagement) and even following termination of employment (or engagement):

- To decide whether to employ.
- To decide how much to pay, and the other terms of an employment contract with us.
- To check the legal right to work.
- Training and reviewing performance
- To decide whether and how to manage absence, or conduct
- To carry out a disciplinary or grievance investigation or procedure
- To determine if reasonable adjustments in the workplace are helpful and/or necessary
- To monitor and protect the security (including network security) of TDA, staff, customers, and others.
- To monitor and protect the health and safety of staff, customers and third parties
- To pay you and provide pension and other benefits in accordance with the employment contract
- Paying tax and national insurance.

- To provide a reference upon request from another employer.
- Monitoring compliance
- To comply with employment law, immigration law, health and safety law, tax law and other laws which affect us
- To answer questions from insurers in respect of any insurance policies which related to the data subject
- Running our business and planning for the future.
- The prevention and detection of fraud or other criminal offences.
- To defend the organisation in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure
- For any other reason which we may notify you of from time to time.

We will only process special categories of personal data in certain situations in accordance with the law. For example, we can do so if there is explicit consent. If we asked for your explicit consent to process a special category of personal data, then we would explain the reasons for our request.

TDA does not need consent to process special categories of personal data when we are processing it for the following purposes, which we may do:

- Where it is necessary for carrying our rights and obligations under employment law.
- Where it is necessary to protect vital interests or those of another person where you/they are physically or legally incapable of giving consent.
- Where the data has been made public by the data subject
- Where processing is necessary for the establishment, exercise, or defence of legal claims, and
- Where processing is necessary for the purposes of occupational medicine or for the assessment of working capacity.

Details about criminal convictions, and reasons

We might process special categories of personal data in relation to:

- Race, ethnic origin, religion, sexual orientation, or gender to monitor equal opportunities.
- Sickness absence, health, and medical conditions to monitor absence, assess fitness for work, to pay benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after health and safety; and
- Trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

Sharing Your Personal Data

Sometimes TDA might share personal data with contractors or agents to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

TDA does not send personal data outside the European Economic Area. If this changes those affected will be notified and the protections which are in place to protect the security of your data will be explained.

Your Data Subject Rights

Data subjects have the right to information about what personal data TDA processes, how and on what basis as set out in this policy.

Data subjects have the right to access their own personal data by way of a subject access request.

Data subjects can correct any inaccuracies in their personal data. To do so, anyone can request this via the DPO.

Data subjects have the right to request to erase personal data where TDA is not entitled under the law to process it, or it is no longer necessary to process it for the purpose it was collected. To do so, anyone can request this via the DPO.

While requesting personal data is corrected or erased or are contesting the lawfulness of our processing, restrictions to information while the application is made can be requested. To do so, anyone can request this via the DPO.
Data subjects have the right to object if we process your personal data for the purposes of direct marketing.

Data subjects have the right to receive a copy of their personal data and to transfer their personal data to another data controller. TDA will not charge for this and will in most cases aim to do this within one month.

With some exceptions, data subjects have the right not to be subjected to automated decision-making.

Data subjects have the right to be notified of a data security breach concerning their personal data.

In most situations TDA will not rely on consent as a lawful ground to process personal data. If we do request consent for the processing of personal data for a specific purpose, data subjects have the right not to consent or to withdraw consent later. To withdraw consent, contact the DPO.

Data subjects have the right to complain to the Information Commission. This can be done by contacting the Information Commissioner's Office directly. TDA are registered with the ICO (Information Commissioners Office) in accordance with the General Data Protection Regulations. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

When working with TDA client data

Business Purposes

The business purposes for which personal data may be used by TDA include the following:

- Compliance with our legal, regulatory, and corporate governance obligations and good practice
- Ensuring business policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording client information for delivering services and quality control
- Marketing our business
- Improving services

Personal Data

'Personal data' means any information relating to an identified or identifiable natural person or 'data subject.' An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as:

1. Name
1. Date of birth
2. Address
3. Name of employer
4. Parent/guardian details
5. Name of school/college/university
6. Telephone number
7. National insurance number
8. Racial or ethnic origin
9. Political opinions
10. Religious beliefs
11. Trade-union membership
12. Details of physical & mental health
13. Sexual orientation

Children's data

TDA aim to apply enhanced protections when processing the data of indiduals under the age of 18 including age-appropriate consent, and clear privacy notices on our website.

Data Controller

The data controller is a person, group, or organisation (in this case TDA) who determines the purpose and way any personal data is processed.

Data Processor

The data processor is the person, group or organisation who processes personal data on behalf of the data controller.

Supervisory Authority

This is the national body responsible for data protection. The supervisory authority for TDA is the Information Commissioners Office (ICO).

Scope

This policy applies to all staff, and all staff must be familiar with this policy and comply with its terms.

This policy supplements other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

The appointed DPO and CEO have overall responsibility for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy if necessary.

Accountability and Transparency

TDA must ensure accountability and transparency in the use of personal data. We must show how we comply with each principle of GDPR. TDA are responsible for keeping a written record of how all the data processing activities they are responsible for complying with each of the principles. This must be kept up to date and must be approved by the DPO.

To comply with data protection laws and the accountability and transparency principle of GDPR, TDA must demonstrate compliance. Staff are responsible for understanding their responsibilities to ensure TDA meets the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation for all processing activities
- Conducting Data Protection Impact Assessments (where relevant)
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Anonymisation
    - Transparency
    - Allowing individuals to monitor processing
    - Creating and improving security and enhanced privacy procedures on an ongoing basis

Our Procedures

Fair and Lawful Processing

TDA must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle of GDPR. This means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

If TDA cannot apply a lawful basis, our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

Controlling vs. Processing Data

TDA is classified as a data controller and data processor. We must maintain our appropriate registration with the ICO to continue lawfully controlling and processing data.

Data processors must comply with TDA's contractual obligations and act only on the documented instructions of the data controller.

If anyone in TDA is in any doubt about how to handle TDA data, please approach and discuss with the appointed DPO.

Lawful Basis for Processing Data

TDA must establish a lawful basis for processing data. Staff should ensure that any data they are responsible for managing has a written lawful basis which has been approved by the DPO and CEO. It is your responsibility to check the lawful basis for any data you are working with. At least one of the following conditions must apply whenever personal data is processed:

Consent
We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
This basis is most used when collecting information for marketing purposes.

Contract
The processing is necessary to fulfil or prepare a contract for the individual.

Legal obligation
We have a legal obligation to process the data (excluding a contract).

Vital Interests
Processing the data is necessary to protect a person's life or in a medical situation.

Public Function
Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

Legitimate Interest
The processing necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

TDA process data under several of the principles above but the majority are processed for contractual purposes to enable us to deliver specific services for an individual.

Deciding Which Condition to Rely On

When assessing the lawful basis, TDA will always first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose.

More than one basis may apply, and TDA will always rely on what will fit the purpose, not what is easiest.

TDA will consider the following factors:

1. What is the purpose of processing the data?
2. Can it be done in a different way?
3. Is there a choice as to whether to process the data?
4. Who does the processing benefit?
5. After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
6. What is the impact of the processing on the individual?
7. Are you in a position of power over them?
8. Are they a vulnerable person?
9. Would they be likely to object to the processing?

10. Are you able to stop the processing at any time on request, and have
11. you factored in how to do this?

TDA's commitment to the first principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose and fully justify these decisions.

Please consult the Data Retention Policy for guidelines on which lawful basis may apply to the processing of TDA documents.

We must ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This will be in the form of a Privacy Statement published on the TDA website. This applies whether we have collected the data directly from the individual, or from another source such as an employer or educational establishment.

Responsibilities

TDA's responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

Staff responsibilities

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with this policy and are justified e.g., only use official work emails, or designated electronic systems
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Always comply with this policy
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

Responsibilities of the Data Protection Officer (DPO)

- Keeping the CEO/Trustees updated about data protection responsibilities, risk, and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, managers, and trustees
- Responding to individuals such as clients and employees who wish to know which data is being held on them by TDA

- Checking and approving with third parties that handle the company's data, any contracts or agreement regarding data processing
- Provide rigorous follow up of any potential reports of data breaches including maintaining a log of incidents

Responsibilities of the CEO

- Ensure all systems, services, software, and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering storing or process data

Responsibilities of the Operations Manager

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients or target audiences
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

Accuracy and Relevance

Staff will ensure that any personal data they process is accurate, adequate, relevant, and not excessive, given the purpose for which it was obtained. Where personal data has been obtained for one purpose, it will not be processed for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Data Security

Personal data must be kept secure against loss or misuse. Where other organisations process personal data on TDA's behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing Data Securely

- In cases where data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly
- Personal data should never be stored on memory sticks
- The CEO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Comply with the Cyber Security Policy regarding data storage on mobile devices such as laptops, tablets, smartphones, data sticks and external hard drives (see bring your own device)
- All servers containing sensitive data must be approved and protected by security software - TDA currently use cloud-based systems
- All possible technical measures must be put in place to keep data secure

Data Retention

Retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, but should be determined in a manner consistent with TDA's Data Retention guidelines.

Transferring Data Internationally
There are restrictions on international transfers of personal data. You must not transfer personal data abroad or anywhere else outside of normal rules and procedures without express permission from the DPO.

Rights of Individuals
Individuals have rights to their data which must be respected and complied with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

Right to be informed
Providing privacy notices which are concise, transparent, intelligible, and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.

Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency

Right of access
Enabling individuals to access their personal data and supplementary information

Allowing individuals to be aware of and verify the lawfulness of the processing activities

Right to rectification
We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete

This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO

Right to erasure
We must delete or remove an individual's data if requested and there is no legal reason for its continued processing

Right to restrict processing
We must comply with any request to restrict, block, or otherwise suppress the processing of personal data

We are permitted to store personal data if it has been restricted but not process it further. We must retain enough data to ensure the right to restriction is respected in the future. For example, retain the individual's name and record the fact that they have requested a restriction.

Right to data portability
We must provide individuals with their data so that they can reuse it for their own purposes or across different services

We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested

Right to object
We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.

We must respect the right of an individual to object to direct marketing, including profiling

We must respect the right of an individual to object to processing their data for scientific and historical research and statistics

Rights in relation to automated decision making and profiling
We must respect the rights of individuals in relation to automated decision making and profiling

Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention

Privacy Notices

When to Supply a Privacy Notice
A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within one month (considered to be a reasonable period).

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place. If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

What to Include in a Privacy Notice
Privacy notices must be concise, transparent, intelligible, and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children.

The following information must be included in a privacy notice to all data subjects:

- Identification and contact information of the data controller and the DPO
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information on any transfers to third countries and safeguards in place
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures

- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and consequences for any failure to provide the data (only for data obtained directly from the data subject)

Subject Access Requests

What is a Subject Access Request?

An individual has the right to obtain:

- Confirmation that their data is being processed
- Access to their personal data

How We Deal with Subject Access Requests

TDA will provide an individual with a copy of the information requested, **free of charge**. This must occur without delay and within one month of receipt. We endeavour to provide data subjects access to their information in a commonly used electronic format, and where possible, provide direct access to the information through a remotely accessed secure system.

If complying with the request is complex, the deadline can be extended to two months, but the individual must be informed within one month. Approval for an extension of the deadline must be obtained from the DPO.

We can refuse to respond to certain requests and can charge a fee of a maximum of £10 if the request is manifestly unfounded or excessive. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.

Once a Subject Access Request has been made, you must not change or amend any of the data that has been requested. **Doing so is a criminal offence.**

Data Portability Requests

TDA must provide the data requested in structured, commonly used, and machine-readable format. This would normally be a CSV file, although other formats are acceptable. The data must be provided either to the individual who has requested it or to the data controller they have requested it be sent to. This must be done free of charge and without delay and **no later than one month**. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and express permission must be received from the DPO first.

Right to Erasure

What is the right to erasure?

Individuals have the right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn

- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

How we deal with the right to erasure
TDA can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right to freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research, or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed on to other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, TDA must inform them of those recipients.

The Right to Object
Individuals have the right to object to their data being used on grounds relating to their situation. TDA must cease processing unless:

- There are legitimate grounds for processing which override the interests, rights, and freedoms of the individual
- The processing relates to the establishment, exercise, or defence of legal claims
-

Individuals must always be informed of their right to object at the first point of communication, i.e., privacy notice. This is available on the TDA website.

Third Parties

Using Third-Party Controllers and Processors
As a data controller, there must be written contracts in place with any third-party data controllers and / or data processors used by TDA. The contract must contain specific clauses which set out TDA's and their liabilities, obligations, and responsibilities.

As a data controller, TDA only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected. This is met by registration with the ICO by all associates and workers (e.g. third-party contractors)

As a data processor, TDA must only act on the documented instructions of a controller, for example where we are contracted to provide services to an organisation. TDA acknowledges their responsibilities as a data processor under GDPR and will protect and respect the rights of data subjects.

Contracts

Contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. The TDA (The Dyslexia Association) contracts with data controllers and / or data processors must set out the subject matter and duration of the processing, nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, contracts must include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments.
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspects, and provide whatever information necessary for the controller and processor to meet their legal obligations
- Nothing will be done by either the controller or processor to infringe on GDPR.

Criminal Offence Data

Criminal Record Checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. TDA cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is a special category of personal data and must be treated as such. Approval from the DPO must be obtained prior to carrying out a criminal record check.

Monitoring

All TDA staff must observe this policy. The DPO and CEO have overall responsibility for this policy. TDA will keep this policy under review and amend or change it as required. The DPO must be notified of any breaches under this policy.

Training

All TDA staff will receive adequate training on provisions of data protection law specific to their role. All training must be completed as requested. In the case of a change of role or responsibilities, staff are responsible for requesting new data protection training relevant to the new role or responsibilities.

If additional training is required on data protection matters, contact the DPO.

Personal Data Breaches

What is a Personal Data Breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than losing personal data.

Example
Personal data breaches can include:

- sending personal data to an incorrect recipient.
- access by an unauthorised third party.
- deliberate or accidental action (or inaction) by a controller or processor.
- computing devices containing personal data being lost or stolen.
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity, or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted, or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware or accidentally lost or destroyed.

Reporting Breaches
Any breach of this policy or of data protection laws must be reported as soon as possible. This means as soon as you have become aware of a breach. TDA has a legal obligation to report any data breaches to the ICO within 72 hours.

A breach should be reported by using the safeguarding concern reporting form, or discussing with the DPO 0115 9246880 without delay. The concern, or report, will then be tracked, with all actions and decision points recorded by the DPO. The lead trustee for safeguarding will audit data breaches annually to ensure correct procedures have been/are being followed and understand if any lessons have been learnt and assimilated into the relevant TDA policies.

TDA will conduct a self-assessment immediately on report of any breach using the ICO tool ICO: self-assessment for data breaches to determine if the breach is reportable to the ICO.

All TDA staff and Associates have an obligation to report actual or potential data protection compliance failures. This allows TDA to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either or as part of a pattern of failures.
- Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Failure to Comply
TDA takes compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal for TDA employees.

If there are any questions or concerns about anything in this policy, please contact the DPO or CEO.

Contacts:
Chief Executive Officer (CEO) and Data Protection Officer (DPO):

Kay Carter
Kay@thedyslexia.co.uk
0115 9246880

Policy owner	CEO (Chief Executive Officer) DPO (Data Protection Officer)
Policy updated/reviewed	28.07.25
Next review	27.07.26