Data Protection Policy

Date	Revised By:	Summary

DYSPRAXIA FOUNDATION

DATA PROTECTION POLICY & GUIDANCE
Incorporating the new Data Protection Act
October 2000

Scope

This policy applies to personal data (e.g. names and addresses, email addresses, home and mobile phone numbers, children & young people's details) that are held by the Dyspraxia Foundation ("the Foundation") and any Branches and Support Groups (hereinafter referred to collectively as Branches) operating under the name of or auspices of the Foundation and works in conjunction with the Foundation's Confidentiality Policy

The policy applies both to records held on paper (e.g. hand-written or typed index files) and those held in computer systems and to the storing, copying, sharing, communicating or transmitting of data

General Principles

1) Details of members and supporters must not be exchanged with third parties e.g. membership lists/mailing lists cannot be passed to universities or other organisations to aid them in their research
2) Members to be made aware on providing information that they should advise us of any changes to their personal details or contact us to unsubscribe from our Mailing List.
3) Permission must be sought from individual members before personal details (e.g. name and address, email etc) can be passed on to another member
4) No data must be used for a purpose for which it was not gathered

Operation

1) The membership forms of the Foundation and, where applicable, local groups will have an "opt out" box allowing members to indicate that they do not want their details passed to other members
2) Where the Foundation uses local member details for mailshot purposes, a mechanism for removal from the general Mailing List is included with their invitation to renew.
3) The annual check is carried out by sending members a fresh membership form for them to complete
4) Following the annual check records are amended to reflect the new details received.

5) Where members do not renew their membership and are subsequently removed from the Membership Database, we request permission to retain their details on our general Mailing List, for the purposes of sending details of DF events/activities and information, as and when appropriate.

6) Once lapsed members have received such an invitation to renew and failed to respond, their details must be removed from the Membership Database within 3 months of the reminder to renew letter being sent out.

Telephone/Email/Postal Enquiries

When the Foundation is contacted by non-members for information, the Foundation seeks permission either verbally or by way of a letter contained in outgoing Information Packs, to retain the enquirers name and address on our general Mailing List for the purpose of sending further relevant information as and when appropriate.

……..

GUIDANCE

Keeping Information Secure:

Data must be in a room or environment that is secure and able to be locked, and access must be for authorised users of the data only. Users should not be authorised unless they have a valid reason for needing access, and they should only be given levels of access for the specific functions they need.

Awareness and Behaviour:

All staff, volunteers and officers of the Foundation need to understand how important data security is to the Foundation, and to our members. The Foundation promotes a policy of zero tolerance towards misuse, unauthorised access or disclosure, or loss of personal data.

Movement of Data:

Every attempt must be made against the unsafe movement of data, including the individual actions of those representing the Foundation when travelling. You must protect both hard copy and electronic data from loss or theft, including from vehicles.

Putting data on unencrypted memory sticks, laptops, or any portable devices is never acceptable – unless it is something which has been previously authorised by the General Manager.

Security Incidents:

Any suspected incident of data loss or misuse, including unauthorised use of or accessing of data, must be notified to the General Manager without delay.

IT Systems and Administration:

It is recommended that a Password access system should be operated for all users who collect, or have access to personal data, and that Passwords must be regularly changed.