Deafblind Scotland INFORMATION GOVERNANCE POLICY

Deafblind Scotland vision – "A society in which deafblind people have the permanent support and recognition necessary to be equal citizens"

POLICY SUMMARY

As an employer and provider of services, Deafblind Scotland is committed to ensuring that we have the systems and procedures in place to protect all sensitive and personal information and data. Deafblind Scotland has a moral and legal duty to keep records detailing the support and care provided to each customer, records relating to the employment of each employee (team member) or stakeholder, and records related to key business activities. Deafblind Scotland has a duty to keep this sensitive information safe and secure.

Information Governance is the framework of law and best practice that regulates the manner in which this information is managed i.e. gathered, used, stored and disclosed.

The aim of this policy is to provide direction to all Deafblind Scotland employees (including Guide Communicators) on how to manage information in line with our values and within the parameters of legislation and regulation. Managing information properly is critical to the future success of the organisation as our reputation depends on it and as such this policy forms part of each employees' contract of employment.

Related legislation:

The Public Services Reform (Scotland) Act 2010, The Public Records (Scotland) Act 2011, The General Data Protection Regulation (2018), The Data Protection Act (2018), The Human Rights Act (1998), The Adults with Incapacity (Scotland) Act 2000, Mental Health (Scotland) Act 2015, Charities and Trustees Investment (Scotland) Act 2005. The Companies Act 2006, Computer Misuse Act (1990), Public Disclosure Act (1998), NMC Guidelines for Records and Record Keeping, Records Management: NHS Code of Practice, National Minimum Wage Act 1998,

National Care Standards as enshrined in the Regulation of Care Act (2001)

Deafblind Scotland Related Policies:

Codes of Conduct, Discipline and Grievance, Finance and Fundraising, Social Media, GC Good Practice, this list is not exhaustive and as such staff should be familiar with all policies and procedures to ensure the spirit of this policy is applied across all areas of practice.

CONTENTS

1.0 OUTCOME

As a result of this policy members, service users, staff, supporters and stakeholders can be confident that information held about them is obtained and managed in a manner consistent with moral, legal and regulatory requirements. References to personal information (data) made within this policy applies to the information held about staff members, members, service users, volunteers and stakeholders.

2.0 PURPOSE

The purpose of this policy is to ensure that Deafblind Scotland members, service users, staff, supporters and stakeholders understand their rights and responsibilities in relation to *Information Governance* and in line with the principles of the *General Data Protection Regulation* (GDPR) which states that:

Personal information should be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and where necessary kept up to date
- Kept in a form which permits identification of the person (known as a *data subject*) for no longer than necessary and only for the purposes of which the data is processed
- Processed in a manner that ensures appropriate security of the personal data. **members, service users, staff, volunteers and stakeholders can be confident that:**
- Their personal records are fit for purpose, held securely and remain confidential.
- Other records required to be kept to protect their and wellbeing are maintained and held securely where required.

- Deafblind Scotland will both comply with rights, including data access and data portability, and make those rights, and any relevant process, known to individuals. **To do this, Deafblind Scotland will comply with the regulations and will:**

- Keep accurate support records secure and confidential for each person who uses Deafblind Scotland services.

- Keep accurate staff and volunteer records secure and confidential in line with required legislation.

- Keep accurate stakeholder (such as fundraising supporters) records secure and confidential in line with required legislation.

- Keep accurate records in line with required legislation for all key business activities.

- Ensure that personal data will only be used for the purposes for which it was given and for which Deafblind Scotland has a lawful reason for processing.

- Keep those records for the correct amount of time.

- Keep any other records the Care Inspectorate asks them to in relation to the management of regulated activities.

- Store records in a secure, accessible way that allows them to be located quickly.

- Securely destroy records, taking into account the relevant *retention schedule*.

- Share information in a confidential and appropriate manner with relevant services, individuals, teams or agencies.

- Where applicable information will be transferred safely and securely.

3.0 MAIN POLICY POINTS

Deafblind Scotland operates this process within the parameters of the Public Services Reform (Scotland) Act 2010 which sets the standards for

health and social care delivery in Scotland and all other relevant Legislation including: The Public Services Reform (Scotland) Act 2010, The Public Records (Scotland) Act 2011, The General Data Protection Regulation (2018), The Data Protection Act (2018), The Human Rights Act (1998), The Adults with Incapacity (Scotland) Act 2000, Mental Health (Scotland) Act 2015, Charities and Trustees Investment (Scotland) Act 2005. The Companies Act 2006, Computer Misuse Act (1990), Public Disclosure Act (1998), NMC Guidelines for Records and Record Keeping, Records Management: NHS Code of Practice, National Minimum Wage Act 1998, National Care Standards as enshrined in the Regulation of Care Act (2001)

Data Protection and GDPR

3.1.1 The *Data Protection Act* (DPA) 1998 is a framework of rights and duties designed to safeguard personal information. From May 2018 this framework will be strengthened by the implementation of the General Data Protection Regulation (GDPR) and related UK legislation.

3.1.2 Deafblind Scotland Staff who process or use any personal information must ensure that the principles of GDPR and the law are followed and fully implemented.

3.1.3 All staff are expected to take a proactive approach to information governance and are fully accountable for their practice.

3.1.4 Deafblind Scotland has developed procedural guidance to support staff in understanding the importance of sound information governance and their responsibilities.

Data Protection Officer (DPO)

Deafblind Scotland are required to identify a competent *Data Protection Officer* (DPO) to inform and advise the organisation and employees on data protection. The DPO for Deafblind Scotland is the Head of Finance.

The DPO’s role is to:

3.2.1 Audit and monitor compliance with the GDPR, other data protection provisions, and additional internal data protection policies.

3.2.2 Advise on privacy impact assessments (PIA).

3.2.3 Maintain a register of any information security breaches.

3.2.4 Serve as the main contact for the *Information Commissioner's Office (ICO)*.

Confidentiality and Information Sharing

3.3.1 In Deafblind Scotland confidential information includes all data about staff members, members, service users, volunteers and stakeholders of the organisation which may be deemed as private, personal, commercially sensitive or information which could identify the individual.

3.3.2 Deafblind Scotland expects all staff to maintain the principles of confidentiality and protect information from inappropriate disclosure. Deafblind Scotland has developed procedural guidance to staff in understanding their responsibilities regarding confidentiality and disclosure.

3.3.3 *Privacy Notices* set out for staff members, members, service users, volunteers and stakeholders how Deafblind Scotland will collect and use their personal data in a way that is fair, lawful and transparent.

3.3.4 There are occasions when it is necessary to share information either within the organisation or with a third party, or to ensure delivery of essential support. For people we support an annual review where we will record and acknowledge all expected sharing of information. For all unexpected or ad hoc requests to share information consent must be recorded individually.

3.3.5 Where members or service users consent either cannot be obtained or has been refused, Deafblind Scotland may in some specific circumstances, agree to disclose information. This will only happen where the sharing of information is deemed necessary for the provision of an essential service or is in the best interests of the individual. This decision will be made by the Head of Operations who will follow due protocol and report for recording by the DPO.

3.3.6 A *Privacy Impact Assessment*, should be considered for any significant changes to the way in which we collect, store or process information, for example new ICT systems which hold personal data, or

a project which analyses staff, member or service user information. On these occasions project leads should contact the DPO.

3.3.7 All staff members, members, service users, volunteers and stakeholders have a right in law to see any information Deafblind Scotland may hold about them. Deafblind Scotland will ensure that staff members, members, service users, volunteers and stakeholders. are aware of their right to access their records through *Privacy Notices* and *Consent forms* as applicable.

Breaches

3.4.1 Any data breach must be reported immediately to your line manager who will inform the DPO. Appropriate action will be taken to minimise the breach and where necessary, inform the relevant parties.

3.4.2 Breaches could have significant consequences for the person(s) whose data has been compromised. They could also result in Deafblind Scotland being fined by the ICO and cause significant reputational damage.

Information Security

3.5.1 Deafblind Scotland ensures that suitable systems are in place to secure physical and electronic data held by the organisation.

3.5.2 All electronic data must be saved on Deafblind Scotland secure drives only. The Deafblind Scotland secure drives are the shared drive, HR drive and Executive Drive. Records must not be saved on desktop hard-drives.

3.5.3 Data must not be saved on pen drives, discs or any external memory device except for encrypted devices provided by Deafblind Scotland. These secure devices must not be shared where personal data is saved therein. Guidance is available from the DPO on how to save data securely if required.

3.5.4 Staff must ensure that safe systems are used when transporting or sending information either between Deafblind Scotland staff or outside of the organisation.

3.5.5 When working off site i.e. anywhere away from Deafblind Scotland Training and Development Centre staff must have permission to do so from their line manager and be extra vigilant.

Records Management

3.6.1 Deafblind Scotland must keep records that document the support to members, records relating to the employment of staff, volunteers and the details of stakeholder supporters and records of key business activities.

3.6.2 ‘Records’ means any information recorded in any form and includes paper files, electronic files, photographs, audio and videotape. These records may relate to members, staff, volunteers, fundraising or business activities.

3.6.3 Records must be maintained and stored within the systems that Deafblind Scotland has in place. These systems ensure the integrity and security of the data is maintained.

3.6.4 Records that are over 12 months old and no longer required for daily reference are considered as ‘semi-current’ and must be stored appropriately in the Archive and Records store.

3.6.5 For guidance on transfer and storage of ‘semi-current’ records please refer to your line manager.

3.6.6 Standards of record keeping will be routinely monitored by the DPO through the auditing process.

CCTV and Surveillance

3.7.1 Personal data refers to anything that can identify an individual; this includes CCTV and employee monitoring. Such data is also subject to the principles and requirements of the Data Protection Act 1998 and GDPR.

3.7.2 Where Deafblind Scotland uses CCTV or other electronic monitoring processes, it will make clear the grounds on which it is undertaking this monitoring, which will normally be based on *legitimate interest* (such as security) or legal obligations.

3.7.3 Where Deafblind Scotland operate CCTV in premises this will be for the purpose of safety and security. CCTV will not be used for monitoring people using services or team members when carrying out work duties.

3.7.4 Access to the footage is restricted to the Senior Management Team and stored securely. Footage will be reviewed only in the event of an incident, accident or as required for investigation purposes e.g. vandalism.

3.7.5 Staff or members requests for access to footage will be managed as a usual data subject access request.

4.0 RESPONSIBILITIES

Deafblind Scotland recognises that GDPR exists to protect all of our personal data as citizens and offers us a governance framework that we must comply with. Consequently, we will ensure that Deafblind Scotland staff members have the appropriate systems and governance arrangements are in place to support all colleagues to carry out their duties and responsibilities in relation to information governance.

All line managers have an absolute responsibility to develop their own and their staff' understanding and practices in respect of this policy.

Compliance with this policy forms part of the formal contract of employment for Deafblind Scotland staff. Deliberate failure to comply with this policy will be considered as misconduct and may result in action in line with the Disciplinary Policy. Accidental or unintentional failure to comply with this policy may also be considered as misconduct and result in action in line with the Disciplinary Policy.

Staff with concerns that this policy has not been adhered to should refer the matter to their line manager in the first instance, who will report the matter to the Head of Finance. In the event that the line manager is the subject of the concern staff should escalate their concern to a member more senior staff member.

5.0 EQUALITY and DIVERSITY

This policy will be applied in line with our Equality and Diversity policy and will be monitored to ensure compliance with our values.

6.0 HEALTH AND SAFETY

Staff must have regard for their own and others' health and safety when implementing this policy and procedures. This includes the need to ensure that paper records are handled in line with safe manual handling guidance and with due care.

Risk assessments should be conducted as required by the line manager and records should be stored in appropriate conditions.

7.0 POLICY ACCESS, MANAGEMENT AND REVIEW

As this policy is part of employee contracts of employment, all employees must sign a declaration to say that they have received and understood their responsibilities in line with this policy.

This policy will be updated from time to time and in any event reviewed every three years as a minimum. The appendices which accompany this policy may be updated more frequently to reflect changes in practice, regulation etc. The most up to date version of this policy and appendices is available for reference to all employees via Deafblind Scotland's Web Page.

Line managers are responsible for ensuring that all their staff are made aware of this policy and any changes to it through induction, training, team meetings and signposting in one to ones as appropriate.

8.0 ENVIRONMENTAL

Please consider the environment before you print this document and wherever possible copies should be printed double-sided and in black and white. (Please also consider setting the Page Range in the Print properties, when relevant to do so, to avoid printing the policy in its entirety. I.e. printing all appendices)

9.0 SUPPORT FOR IMPLEMENTATION

Employees will be supported in their understanding and appropriate implementation of this policy through induction, supervision, appraisal

and training, taking account of additional service specific guidance as required.

Members and Service Users will be supported in their understanding of this policy by input through SAGOD, Board meetings, individual reviews etc.

Appendix 1

Data Protection guidelines Deafblind Scotland vision – "A society in which deafblind people have the permanent support and recognition necessary to be equal citizens" NB this guideline should be read in conjunction with but not exclusively DbS Information Governance Policy and Privacy Notices

1. Information about Deafblind members
All requests for information must be authorised by a manager.

Deafblind Scotland do not disclose information to any unauthorised third party without the express consent of the member/service user, or if the member/service user is unable to judge, the member/service user's immediate family or advocate.

Confidential information will not be sought from a member/service user unless expressly in the interests of that member/service user.
Staff will always consult management if they are unclear with respect to any item concerning confidentiality, or when made privy to confidential information that may have legal and / or criminal connotations.
See the Protection of Vulnerable Adults policy.

2. By a deafblind person or carer
Staff should advise that all requests for information must be authorised by a manager and that we cannot disclose information without the consent of the individual.

3. About a service user
Requests for information from funders of services should be directed to the service manager. Returns, invoices and applications should be anonymised so that individuals cannot be identified.

4. About staff members or volunteers

Requests for information should be directed to the individual's line manager. References should be stored in individual personnel files. Retention of Data; Deafblind Scotland requires to store personnel records for 5 year from ceasing employment. Including information necessary in respect of payments, pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. Deafblind Scotland requires to store certain

information about its employees, clients and other users to allow it to monitor progress, achievements, and health and safety.

Therefore, all prospective staff will be asked to consent to their data being processed when an offer of employment is made. A refusal to sign such a form will result in the offer being withdrawn. See recruitment policy.

5. Storage of information
All staff are responsible for ensuring that: • Confidential information in line with DbS Information Governance policy. • Computerised information be held in line with DbS information Governance policy • no confidential information should be held on personal storage equipment or removed from the premises

6. IT and Emails
Deafblind Scotland may take any measure it deems necessary to reduce or eliminate risk to its IT and electronic communication systems and prevent their misuse. Employees should not expect complete privacy while utilising these systems. Authorised individuals within Deafblind Scotland may monitor and access IT facilities, IT systems, telecommunication systems, email, internet, network traffic and machine activity at any time in the interest of protecting these resources and Deafblind Scotland.

Staff members who fail to comply with this policy and/or related procedures and guidelines or who misuse or abuse Deafblind Scotland's IT systems or electronic communication may face disciplinary action (up to and including summary dismissal) in accordance with Deafblind Scotland's disciplinary action.

Deafblind Scotland emails must carry a legal disclaimer attached at the bottom of every mail. This is to ensure that recipients are informed that the email is intended for their sole use only and to give them an option to send the mail back, have their name taken out of mailing lists and talk to Deafblind Scotland's IT department if they have a query about reasons why they have received the email.

In light of third party access rights which may arise under applicable GDPR and Freedom of Information legislation proper care must be taken when drafting emails. Some emails, particularly emails to government and other public bodies may be accessible under applicable Freedom of Information legislation. Thus emails should be regarded as company

documents which may be made public, potentially giving rise to legal liability for Deafblind Scotland and for the sender, who may also be subject to disciplinary action in the event of failure to comply with email acceptable usage policy.

Email messages might be forwarded to persons other than the original recipients or sent in error. Therefore senders must take their time before sending emails to ensure that the following are adhered to:

• Check you are using the correct email address
• Take time and care when writing emails.
• Writing emails are equivalent to writing a formal letter and appropriate etiquette applies.
• Do not make defamatory, obscene or other inappropriate remarks.
• Remember that anything stated in an email could be used in legal proceedings in the same way as anything in a memo or a letter.
• Remember that emails can be forwarded easily and should not be treated as confidential.
• Use of email to transmit confidential information and/or content which may give rise to legally enforceable obligations should be avoided where possible as security cannot always be guaranteed – if it cannot be avoided, extra care, such as encryption of content and password protecting documents should be taken. Refer to Information Governance Policy.
• Avoid forwarding email and disclaimers from previous email correspondence unless it is relevant and necessary to do so.
• Where previous correspondence is being forwarded, check that it does not contain confidential, commercially sensitive or other information (e.g. disparaging remarks) inappropriate to the intended recipient(s) and that it does not purport to bind Deafblind Scotland to any particular course of action or legally enforceable obligations.
• Where possible, limit the use of attachments to reduce the risk of releasing information unintentionally.

7. Photographic images

Consent to publish or use images of people must be received in writing. Photographs stored on the internet should be password protected.

8. Contact lists

List of contacts for colleagues, customers, donors, trainees, service users, staff or volunteers should only be held with explicit consent and

should be stored in the relevant password protected databases and not as lists in public folders.

9. Staff Responsibilites
Individual staff members are responsible for ensuring the data they hold is protected and is not shared inappropriately.

11. The Data Controller
Deafblind Scotland as an organisation is the data controller under the Act, and as such is ultimately responsible for the implementation of the Act.

12. Requests for information by the police or other agencies.

Examples including crime and taxation. Information should be given provided certain conditions are met; Acts protecting children or vulnerable adults which require you to inform social services must be complied with. See Child and Adult Protection policies.

13. Good house keeping
Clear your desk before you leave of any confidential documents. Lock your computer (using CTRL, ALT, DEL keys). Memory sticks and laptops should hold no personal data. Ensure documents for shredding are kept securely.

14. Rights to Access Information
Staff, clients and other users of Deafblind Scotland have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should contact their manager.

15. Conclusion
Compliance with the Data Protection Act 1998 and General Data Protection Regulation Act 2017 is the responsibility of all staff. Any deliberate breach of the data protection policy will lead to disciplinary action being taken.