Data Protection: IASLT Policy and Procedure.

Policy Operational Date;	Policy Review Date
21st April 2015	2018

TABLE OF CONTENTS

1.0 Introduction

The Irish Association of Speech and Language Therapists (IASLT) is fully committed to compliance with the requirements of the Data Protection Act 1998 and The Data Protection (Amendment) Act 2003. The IASLT will follow procedures that aim to ensure that all employees, council members, contractors, consultants or other servants of IASLT who have access to any personal data held by or on behalf of IASLT, are fully aware of and abide by their duties and responsibilities under the Act.

2.0 Statement of Policy

In order to ensure the IASLT operates efficiently IASLT must access and retain information in relation to individuals. These may include members of the professional body, past and present and current and prospective employees.

The IASLT undertakes to perform its responsibilities under the legislation in accordance with the eight stated Data Protection principles outlined in the Acts as follows:

1. **Obtain and process information fairly**; IASLT obtains and processes personal data fairly and in accordance with its statutory and other legal obligations.
2. **Keep it only for one or more specified, explicit and lawful purposes**; IASLT keeps personal data for purposes that are specific, lawful and clearly stated. Personal data will only be processed in a manner compatible with these purposes.
3. **Use and disclosure only in ways compatible with these purposes;** IASLT only uses and discloses personal data in circumstances that are necessary for the purposes of for which it collects and keeps the data.
4. **Keep it safe and secure**; IASLT takes appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of data and against accidental loss or destruction.
5. **Keep it accurate, complete and up-to-date**; IASLT operates procedures that ensure high levels of data accuracy, completeness and consistency.

6. **Ensure it is adequate, relevant and not excessive**; Personal data held by IASLT are adequate, relevant and not excessive in data retention terms.
7. **Retain for no longer than is necessary**; IASLT has a policy on retention periods for personal data.
8. **Give a copy of his/ her personal data to that individual, on request**; IASLT has procedures in place to ensure that data subjects can exercise their rights under the Data Protection legislation.

3.0Responsibility

The IASLT Chairperson has overall responsibility for ensuring compliance with Data Protection legislation when it is the Data Controller of personal data. However, all employees, Council and Committee members of IASLT who separately collect and/or control the content and use of personal data are individually responsible for compliance with the legislation.

Individual Responsibilies;

- Each Committee Chair has responsibility for monitoring access to data kept for the purpose of business.
- Each committee chair must monitor access to email, shared files and data relating to the work of IASLT.
- The Chair of each committee has responsibility for the safe and secure storage of data relating to IASLT while it is stored offsite.
- The Chair of each committee is responsible for ensuring that data is transferred to the IASLT Office annually for safe and secure storage in line with the IASLT Data Retention Guidelines.
- The Chair of the Website Committee has specific responsibility for liaising with appropriate individuals and monitoring access to the IASLT Admin, email and social media accounts.

4.0 Breach of this Data Protection Policy and Procedure

All current and former members, employees, agents and contractors of IASLT will be held accountable for all personal data processed by them for or on behalf of IASLT Council. All Council members, committee chairs and employees are responsible for ensuring compliance with Data Protection within their area.

All Council and committee members, agents, contractors and employees will be required to sign a short statement indicating that they have read and understood this data protection policy and their data protection responsibilities **(Appendix 1).**

If an individual feels that this policy has not been followed they should immediately raise the issue with the IASLT Chairperson. Violation of this policy and procedure may be considered a breach of contract.

5.0 IASLT Data Protection Procedures

For the purposes of the Data Protection Act 1998, the Irish Association of Speech and Language Therapists is identified as the 'data controller'. Members and those we retain information on are referred to as 'data subjects'. In order to ensure IASLT compliance with the 8 Principles of Data Protection the following procedures must be observed all times.

5.1 Obtaining and processing personal data

The IASLT collects information about members that is relevant and necessary.
As IASLT keeps personal data, including sensitive personal data, about data subjects on paper and computer, it must ensure that all information is obtained and processed fairly.
Individuals acting for or on behalf of IASLT must;

- ✓ Obtain personal data only when there is a clear purpose for so doing, obtain only whatever personal data is necessary for fulfilling that purpose and ensure data is used only for that purpose.
- ✓ Inform data subjects of what personal information is held by IASLT, what it will be used for and to whom it may be disclosed.
- ✓ Personal data should only be disclosed in ways that are necessary or compatible with the purpose for which the data are kept.

5.2 **Keep the data only for one or more specified purposes;**

- ✓ IASLT holds personal data for a number of purposes.

- ✓ Data about individuals may not be kept unless it is held for a specific lawful and clearly stated purpose.
- ✓ All data subjects will be made aware of the purposes for which information relating to them is collected.
- ✓ If IASLT has data about persons and wishes to use it for a new purpose individuals will be given an option to indicate whether or not they wish their data to be used for the new purpose.

5.3 **Use and Disclose only in ways compatible with the specified purpose**

- ✓ Information obtained for a particular purpose should not be used for any other purpose.
- ✓ Information may not be divulged to a third party unless it is comparative with the specified purpose.

- ✓ Except where there is a statutory obligation to comply with a request for personal data, or where a data subject has already been made aware of disclosures, do not disclose to any third party any personal data without the consent of the data subject.
- ✓ Verbal consent to disclosure of personal data to the data subject may be obtained by telephone in the case of non-sensitive personal data, but must include asking the subject to confirm facts that should be known only to them, such as date of birth, student number, etc. The date and time of the giving of the verbal consent should be recorded in writing.

- ✓ Verbal consent to disclosure of personal data to a third party is not permitted unless there is a statutory obligation to disclose, or the information is released, to the Gardaí for example, for the prevention of crime and if informing the subject of the disclosure would prejudice the enquiries, or unless it is in the vital interest of the data subject.
- ✓ Personal data should only be disclosed to work colleagues where they have a legitimate interest in the data in order to fulfil the functions of the organisation.

- ✓ Data subjects will be made aware of actual or potential disclosures of their personal information.

5.4 **Keep Safe and Secure**

The security of personal information is crucial and high standards of security is important for all personal information.

IASLT must protect personal data from unauthorized access.

- ✓ Access to personal data will be restricted to authorised personnel on a "need to know" basis.
- ✓ Access to storage areas for manual data will be restricted to IASLT Chair, officers and employees.
- ✓ Committees holding manual data should ensure it is held securely. Committees should store data securely as long as it is required. Once the material is no longer directly required by the Committee it should be transported to the IASLT Office for safe storage/archiving in line with the IASLT Data Retention Guidelines.
- ✓ Appropriate swipe card security and physical safeguards will be put in place.
- ✓ Electronic files containing personal data should be subject to appropriate controls such as password protected.
- ✓ Screens, printouts, documents, and files showing personal data should not be visible to unauthorized persons.
- ✓ Subject to retention guidelines, personal manual data should be destroyed by confidential shredding when the retention period has expired.
- ✓ IASLT Council/employees should not disclose laptop password for your laptop or IASLT Admin to any other member of staff or individual; all individuals who need access, should use their own login;
- ✓ If it is necessary to hold a printout of personal data for a period of time, lock it away securely when not working on it and destroy by shredding as soon as possible;
- ✓ An IASLT laptop should be used for work only.
- ✓ Disclosing personal data to a Data Processor should be done only under a written contract specifying security rules to be followed.

- ✓ Employees will endeavor as far as possible to minimise the number of working files on desks.
- ✓ Hardcopy files will be stored securely in a locked filing cabinet/press and will be retained/disposed in accordance with IASLT's Data Retention Guideline.
- ✓ Files taken and held off site will be subject to the same data protection and file retention and disposal procedures.

5.5 **Kept accurate and up to date**

- ✓ Personal information must be kept accurate and up to date.
- ✓ The IASLT membership system provides members with the facility to review personal data to ensure that records are accurate, complete and kept up-to-date. This is done annually on renewal of membership or at the data subject's behest.
- ✓ All staff, members and other data subjects are entitled to be informed how to keep their personal data up to date.
- ✓ All staff, and members are responsible for checking that any information that they provide to the IASLT is accurate and up to date; informing the IASLT of any changes or errors in information that they have provided.

5.6 **Be adequate, relevant and up to date**

- ✓ In order to comply with this principle each Council member, committee member and agent of IASLT should ensure that the personal data held is;

  a. Adequate in relation to the purpose for which it is kept.
  b. Relevant in relation to the purpose for which it is kept
  c. Not excessive in relation to the purpose for which it is kept.

5.7 **Retain for no longer than necessary**

- ✓ Data should not be kept for longer than is necessary for the purpose for which they were collected.

- ✓ Data already collected for a specific purpose should not be subject to further processing that is not compatible with the original purpose.
- ✓ The Data Protection Office does not give any clear guidelines on periods of retention. IASLT has devised a Data Retention Guideline.
- ✓ All employees, Council members and individuals acting for or on behalf of IASLT must be familiar with IASLT Data Retention Guidelines, 2014.
- ✓ The IASLT Chairperson will assign specific responsibility to an individual for ensuring that files are purged regularly and that personal information is not retained longer than is necessary.

5.8 **Right of Access to Personal Data**

All data subjects have the right to access the information held about them and must be made aware of how to gain access to their personal data. A data subject is entitled to the following on written application within forty days of receipt of a completed application:

- ✓ A copy of his or her personal data;
- ✓ The purpose of processing the data;
- ✓ The persons to whom the IASLT discloses the data;
- ✓ An explanation of the logic used in any automated decision-making;
- ✓ A copy of recorded opinions about him or her, unless given in confidence.

A maximum fee of €6.35 will be charged for accessing the data.

5.9 **Exemptions to right of access**

The right of access is restricted where the data is:

- ✓ required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State;
- ✓ subject to legal professional privilege;

- ✓ kept only for statistical or research purposes and the results are not made available in a way that identifies data subjects;
- ✓ Back-up data.

6.0 Protocol for reporting any breaches

Any breach of data security must be reported immediately to the IASLT Chairperson and an incident report completed **(Appendix 2).**

In the event of a security breach the IASLT Chairperson will give consideration to informing any data subjects affected by the breach **(Appendix 3).**

REFERENCES;

Website; www.dataprotection.ie

The following guidance documents were accessed;

http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/responsibilities/3bii.htm&CatID=54&m=y

Data Protection Self-Assessment Checklist;
http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/responsibilities/3k.htm&CatID=55&m=y

Marketting Guidance; http://www.dataprotection.ie/viewdoc.asp?DocID=905

Glossary of Terms;

Data; refers to electronic and manual data. It includes data held on mobile phones or other electronic devices.

Personal Data; refers to data, including sensitive personal data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of IASLT.

Data Subject; means an individual who is the subject of personal data and includes Council Members, committee members, employees, members, advisors and anyone contacted by IASLT.

Data Controller; for the purpose of this policy and procedure means the IASLT.

Appendix 1

IASLT Data Protection Policy and Procedure.

I have read and understand the IASLT Data Protection Policy and Procedure.

I understand my data protection responsibilities.

Name	IASLT Role	Signature	Date

Appendix 2

IASLT Data Breach Incident Report Form

Any breach of the IASLT Data Protection Policy and Procedure should be reported immediately to the IASLT Chairperson. A data breach refers to any unauthorised disclosure, loss, destruction or alteration of personal data, and includes inappropriate access to personal information on IASLT's systems or the sending of personal data to the wrong individuals.
Date of Incident;
Details;
Who was informed?
Action taken;
Signature of IASLT Chairperson; **Date;**

Appendix 3

Personal Data Security Breach Code of Practice

[Approved by the Data Protection Commissioner under Section 13 (2) (b) of the Data Protection Acts, 1988 and 2003]

1. The Data Protection Acts 1988 and 2003 impose obligations on data controllers [1] to process personal data entrusted to them in a manner that respects the rights of data subjects to have their data processed fairly (Section 2(1)).Data controllers are under a specific obligation to take appropriate measures to protect the security of such data (Section 2(1) (d)).**This Code of Practice does not apply to providers of publicly available electronic communications networks or services**. [2]

2. This Code of Practice addresses situations where personal data has been put at risk of unauthorised disclosure, loss, destruction or alteration. The focus of the Office of the Data Protection Commissioner in such cases is on the rights of the affected data subjects in relation to the processing of their personal data.

3. Where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, the data controller must give immediate consideration to informing those affected.[3] Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures. In appropriate cases, data controllers should also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, financial institutions etc.

4. If the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the data controller may conclude that there is no risk to the data and therefore no need to inform data subjects.Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.

5. All incidents of loss of control of personal data in manual or electronic form by a data processor must be reported to the relevant data controller as soon as the data processor becomes aware of the incident.

6.All incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner as soon as the data controller becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) **and** it affects no more than 100 data subjects **and** it does not include sensitive personal data or personal data of a financial nature.[4]In case of doubt- in particular any doubt related to the adequacy of technological risk-mitigation measures - the data controller should report the incident to the Office of the Data Protection Commissioner.

7. Data controllers reporting to the Office of the Data Protection Commissioner in accordance with this Code should make initial contact with the Office within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact may be by e-mail (preferably), telephone or fax and must not involve the communication of personal data. The Office of the Data Protection Commissioner will make a determination regarding the need for a detailed report and/or subsequent investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.

8. Should the Office of the Data Protection Commissioner Request a data controller to provide a detailed written report of the incident, the Office will specify a timeframe for the delivery of the report based on the nature of the incident and the information required. Such a report should reflect careful consideration of the following elements:

- the amount and nature of the personal data that has been compromised;
- the action being taken to secure and / or recover the personal data that has been compromised;
- the action being taken to inform those affected by the incident or reasons for the decision not to do so;
- the action being taken to limit damage or distress to those affected by the incident;
- a chronology of the events leading up to the loss of control of the personal data; and

the measures being taken to prevent repetition of the incident.

9. Depending on the nature of the incident, the Office of the Data Protection Commissioner may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where a data controller has not already done so. If necessary, the Commissioner may use his enforcement powers to compel appropriate action to protect the interests of data subjects.

10. Even where there is no notification of the Office of the Data Protection Commissioner, the data controller should keep a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record should include a brief description of the nature of the incident and an explanation of why the data controller did not consider it necessary to inform the Office of the Data Protection Commissioner. Such records should be provided to the Office of the Data Protection Commissioner upon request.

11. This Code of Practice applies to all categories of data controllers and data processors to which the Data Protection Acts 1988 and 2003 apply.

29 July 2011

---

[1] Unless otherwise indicated, terms used in this Code – such as? Personal data? Sensitive personal data? Data controller? Data processor? – have the same meaning as in the Data Protection Acts 1988 and 2003.

[2] The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (SI 336 of 2011) place specific obligations on providers of publicly available electronic communications networks or services to safeguard the security of their services. Further information is available in the Guidance Note that accompanies this Code of Practice.

[3] Except where law enforcement agencies have requested a delay for investigative purposes. Even in such circumstances consideration should be given to informing affected data subjects as soon as the progress of the investigation allows.

[4] 'personal data of a financial nature' means an individual's last name, or any other information from which an individual's last name can reasonably be identified, in combination with that individual's account number, credit or debit card number.

APPENDIX 4

DATA PROTECTION CHECKLIST (adapted from www.dataprotection.ie)

Each IASLT Council member, employee and committee member should monitor their compliance with this policy using this Basic Data Protection Checklist;

Principle		**Circle Yes/No/NA**
Fair Obtaining	• At the time when we collect information about individuals, are they made aware of the uses for that information? • Are people made aware of any disclosures of their data to third parties?	**Yes/No/NA** **Yes/No/NA**
Purpose Specification	• Are we clear about the purpose (or purposes) for which we keep personal information? • Are the individuals on our database also clear about this purpose?	**Yes/no/NA** **Yes/No/NA**
Use and disclosure of information.	• Are there defined rules about the use and disclosure of information? • Are all staff/committee members aware of these rules? • Has consent been obtained for these uses and disclosure?	**Yes/No/NA** **Yes/No/NA** **Yes/No/NA**
Security	• Is data kept securely? • Are these provisions appropriate to the sensitivity of the personal data?	**Yes/No/NA** **Yes/No/NA**

	• Are our computers and our databases password-protected? • Are our computers, servers, and files securely locked away from unauthorised people? • Is committee members change ate rights to access removed promptly?	**Yes/No/NA** **Yes/No/NA** **Yes/No/NA**
Adequate, relevant and not excessive.	• Do we collect all the information we need to serve our purpose effectively, and to deal with individuals in a fair and comprehensive manner? • Have we checked to make sure that all the information we collect is relevant, and not excessive, for our specified purpose? • If an individual asked us to justify every piece of information we hold about him or her, could we do so?	**Yes/No/NA** **Yes/No/NA** **Yes/No/NA**
Accurate and up to date.	• Do we check our data for accuracy? • Do we take steps to ensure our databases are kept up-to-date?	**Yes/No/NA** **Yes/No/NA**
Retention time.	• Have all employees/committee members read and understood the IASLT Data Retention Guideline? • Do we regularly purge our databases of data which we no longer need?	**Yes/No** **Yes/No/NA**
Right of Access	• Are there clear procedures in place for dealing with information access requests? • Do these procedures guarantee compliance	**Yes/No/NA**

	with the Act's requirements?	**Yes/No/NA**
Training and Education	• Are all employees aware of the IASLT Data Protection policy and Data Retention Guidelines? • Are our staff aware of their data protection responsibilities - including the need for confidentiality? • Is data protection included as part of an induction for new staff, Council members and employees?	**Yes/No/NA** **Yes/No/NA** **Yes/No/NA**