Aspire Data Protection Policy 2018

Developed by: Aspire	*Date: March 2018*
Approved by: Board of Directors	*Date: July 2018*
Implemented on: 1st July 2018	*Review date: 1st July 2019*

1. Introduction

Aspire- The Asperger Syndrome Association of Ireland was founded in 1995 to provide support and information to people with Asperger Syndrome and their families.

1.1 Vision, mission and values

Aspire envisions a world where people with Asperger Syndrome have the same opportunities to work, socialise and participate as everyone else. Our mission is to provide supports to people with Asperger Syndrome that will help them to fulfil their goals, to provide information to them and their families, and to promote an understanding in the community.

Our values are:

Inclusion

We, in Aspire, believe that people with Asperger Syndrome have an invaluable insight and should be central to decisions regarding what supports are required and how our message is communicated.

Equality

Aspire believes that people with Asperger Syndrome have the right to access the same supports, community resources and educational and employment opportunities as everyone else.

Promote Understanding

We believe that a greater understanding of Asperger Syndrome in the community will lead to greater inclusion and awareness of the unique contribution that people with Asperger Syndrome can make.

Achieving Aspirations

People with Asperger Syndrome have the right to choose their own path and Aspire is committed to providing support to individuals and promoting a level of understanding that will make it easier to achieve this.

1.2 Asperger Syndrome

Asperger Syndrome is a condition on the Autism Spectrum which impacts on the way that individuals view the world, interact with and communicate with others.

While people who have Asperger Syndrome can have many talents and unique skills, they can experience challenges in forming relationships with others, managing anxiety, social exclusion and limited employment opportunities. Perhaps the most significant challenge is the 'hidden' element of the condition, which can make it difficult for others to understand the impact that Asperger Syndrome can have.

The characteristics of Asperger Syndrome vary from individual to individual but listed below are some examples of behaviours seen with individuals with Asperger Syndrome:

- Sensitivity to stimuli such as light, heat, smell, touch and sound
- Literal interpretation of language resulting in comprehension difficulties

- Difficulty adapting to changes and understanding social expectations
- Difficulty with social interaction
- May have difficulty reading facial expressions and body language of other people
- May have difficulty making eye contact with others
- Often have a special interest which can often consume great deals of time

2. Scope

This policy describes how Aspire meets its obligations to individuals and the law regarding the safeguarding of personal data. The policy refers to all data collected throughout Aspire Supports and Services, including:

- Services provided within **the Residential Unit** of Aspire
- **SocialEyes** Social Skills Course
- **Aspire Membership**
- **Aspire Productions**
- **Adult Social Group**
- **Information Supports** provided to members
- **Helpline**
- **Support Groups** that are organised by Aspire

This list is not exhaustive and can be updated to include further services as appropriate.

3. Purpose and Objectives

The policy addresses the core principles set out by the Office for Data Protection for compliance and good practice within the current EU Data Protection Legislation.
The document is for all Aspire Staff and Volunteers.

The office of the Data Protection Commissioner outlines eight principles of data processing which are binding on all organisations who handle personal data. These principles are to:

- Obtain and process information fairly
- Keep it only for one or more specified, explicit and lawful purposes
- Use and disclose it only in ways compatible with these purposes
- Keep it safe and secure

- Keep it accurate, complete and up-to-date
- Ensure that it is adequate, relevant and not excessive
- Retain it for no longer than is necessary for the purpose or purposes
- Give a copy of his/her personal data to an individual, on request

This policy describes how Aspire adheres to those principles. For the purposes of this policy, individuals using the services of Aspire and individuals and companies purchasing products and services from Aspire Productions are referred to as 'clients'.

3.1 Fair Obtaining

Our data collection aims to be open and transparent at all times. Individuals are made aware of the uses for their information when that information is collected. This disclosure is included in our online application forms, or by email, along with a request for consent. Personal data is not subject to secondary use or disclosed to third parties without prior consent.

Examples include: for assessment of application for services/membership, for planning service delivery, for provision of information, research and recruitment, for the purposes of sales.

3.2 Purpose Specification

Aspire recognizes the need to hold personal data about individuals for the following purposes:

- Service Provision to People with AS and family members
- Information mailings
- Research
- Human Resources
- To accommodate ordering and processing of products to clients of Aspire Productions

At each point of data collection we are clear to individuals about the purposes to which that information is being put. For example, the Aspire online membership form states:

'I understand that Aspire Ireland will store the data that I have provided for the purposes of providing me with information regarding supports and services, providing me with updates about the organisation and my membership and occasionally providing me with requests for research. I understand that my personal data will not be disclosed to a third party without prior consent, and my data will only be stored for the duration of my membership of the Association, and subsequent periods of membership. By ticking this box, I consent to being contacted and receiving such relevant information from Aspire Ireland'.

3.3 Use and Disclosure

Use and disclosure of personal data, including health and medical data, is in line with the requirements of the Data Protection Acts, under which personal data must be obtained for a specified purpose, and must not be disclosed to any third party except in a manner compatible with that purpose.

3.3.1 Disclosures to 3rd Parties and Consent for Secondary Uses

I. Individuals are made aware of all disclosures to third parties, and consent is always sought for such disclosures.

II. Disclosures are typically related to the further provision of service (i.e. for the purposes of referral to an outside professional) to an individual and consent for this explicitly sought.

III. Information disclosed to third parties may be in written or verbal form.

IV. If disclosure of personal data to a third party is required which exceeds the terms of the provision within the consent declaration on the service application form, consent will always be sought in such cases.

V. Letters to external agencies containing personal data about an individual (e.g. letters of referral) form part of an individual's record and are maintained as part of the person's record.

There are special circumstances under which disclosure of personal data to third parties is allowed. These are provided for under the Data Protection legislation and are:

- As ordered by the Gardaí, or army personnel
- For the purpose of investigating an offence
- To protect the state's international relations
- To prevent urgent injury or damage to person or property
- Under a court order or other rule of law
- Required for the purposes of obtaining legal advice or for legal proceedings in which the person making the disclosure is a party or a witness
- Made at the request of and with the consent of the subject of the data

In all such cases, full reference will be made to the current legislation via approval by the Aspire CEO.

In these additional circumstances personal information may be released without the consent of persons served under the following conditions:

- For use by any Aspire employee who has a need for the information in the performance of their duties to ensure continuity of care.
- To medical personnel who have a need for the information for the purpose of treating a condition which poses an immediate threat to the health of a person served (e.g. in the case of a seizure, or sudden collapse)
- To recover or collect the costs of medical care from third party health care insurance carriers contracted with by the persons served and required by the health plan to be disclosed.
- To government agencies or entities charged under applicable laws with the protection of public health and safety. In such cases, the information may be released with the consent of the individual whose records are being requested, or upon receipt of a written request from the relevant and appropriate representative of the government entity.
- To relevant government agencies in relation to concerns regarding the health and wellbeing of minors. (See Aspire Child Protection Policy).
- To relevant health care professionals and/or designated next of kin if the person served presents with a significant risk to their own health or wellbeing (e.g. suicide risk).
- To relevant government agencies and/or health care professionals (e.g. An Garda Síochána, Psychiatric services), in situations where the person served is deemed to pose a credible threat to the health/wellbeing of another person (e.g. staff member, another person served, member of the public)

3.4 Security

Personal data is held within a number of secure systems within Aspire, according to application. Personal data for client service provision and research is held within a cloud based storage systems, Microsoft Office 365 (Aspire) and Google Drive (Aspire Productions), and in hard copy client files. All personal data is maintained in a secure manner. The following physical and software safeguards are in place to protect personal data:

3.4.1 Confidential Client Records

I. Hard copies of medical and health data relating to clients are maintained on site in locked cabinets. Access is limited to management and staff providing services directly to clients.

II. Electronic records are held on secure, password protected cloud based systems. Access is granted to management and staff providing services directly to clients.

3.4.2 Human Resource Management System

I. Human Resource paper files are maintained securely in locked cabinets with access controlled and limited to the CEO, relevant service managers and the Board of Directors.

II. Electronic records are maintained securely on a secure, password protected cloud based system.

3.4.3 Network Data

I. All data held on Aspire Networks is maintained behind a secure firewall on password protected PCs and is restricted access only to authorized employees.

3.4.4 Laptop and PC Security

I. All Laptops and PCs for use with client personal data are password protected. No data is stored on hard drives.

3.4.5 Data Transfers Abroad

I. Aspire uses web based systems for hosting personal data which involves transfers of that data to countries outside the EU. To comply with Data Protection Legislation, the countries must be considered as offering an adequate level of protection in accordance with Article 25 of the Data Protection Directive.

II. Aspire uses one country which have been subject to EU approval, the US (under Safe Harbor Principles).

3.4.6 Microsoft Office 365

Full breakdown of data privacy tools and certifications (including EU Safe Harbor agreement) for Microsoft Office 365 (SharePoint) can be found at https://www.microsoft.com/en-us/legal/intellectualproperty/copyright/default.aspx

3.3.7 Google Drive

Full breakdown of data privacy tools and certifications (including EU Safe Harbor agreement) for Google Drive (G-Suite) can be found at https://support.google.com/googlecloud/answer/6056694?hl=en.

3.5 Adequate, relevant and not excessive

I. We collect and maintain sufficient information for the declared purpose in order to provide a fair and comprehensive service to each person.

II. We only hold that information which is adequate and relevant to the purpose it serves. If we are in receipt of personal data e.g. in the form of medical records, which is extra to requirement, we ensure that the information is returned to the referring agent or destroyed as appropriate.

III. Annual reviews are conducted of the information collected to ensure that it is sufficient and not excessive.

IV. All records of staff client interactions are maintained in a professional manner and done so with the expectation that the information can be shared with the person served.

3.6 Accurate and up-to-date

Aspire employees who maintain personal data are responsible for correcting and maintaining that information on an ongoing basis. For example:

- Service managers and co-ordinators are responsible for maintaining the contact information and the personal data held.
- The Administrator is responsible for maintaining the accuracy of distribution lists for newsletters.
- The CEO is responsible for maintaining the accuracy of the HR Management system.
- The Business Development Manager is responsible for ensuring that client contact details are relevant.

Data is reviewed annually or when change or development to a service renders a review necessary.

3.7 Data Retention

I. Personal information (e.g. about a client) processed/kept for any purpose should not be kept longer than is necessary for that purpose.

II. This gives some flexibility and Aspire occasionally needs to make a professional judgement about how long is "necessary". The minimum period set down for the retention of records is eight years generally, 20 years in the case of persons with mental health challenges or disability. Because litigation may occur sometime after contact has finished, any destruction of material must be considered carefully if it is to be carried out before the minimum time period. Any such actions may need to be justified to others including the client. Consultation is made with relevant professionals (i.e. psychologists, GP's) if required to gain advice on the recommended duration of retention of records. It is advisable for clinicians within Aspire to follow the following guidelines on retention of notes, records etc.

Purpose	Retention Schedule
Support and Service Provision to members	8 Years following final closure of case, or duration since final contact, whichever most recent. Exception to this is in case of death by suicide, in which case duration is 10 years after death. See appendix 2.
Information mailings	Data is retained for as long as mailing list is relevant, then subsequently deleted.
Fund-raising and development	Data is retained for as long as mailing list is relevant, then subsequently deleted.
Research	Subject to same retention schedule as Client Records (see above and appendix 2)
Human Resources	See appendix 1 HR record retention schedule.

3.8 The Right of Access

I. All individuals have the right to access all the personal data held on them by Aspire and to have that information corrected and deleted. Personal data will normally be accessible under the terms of the Data Protection Acts, using the procedure outlined below (see Personal Data Access Procedure).

II. Aspire takes the stance that individuals may need assistance to request access to their own personal data. Aspire will provide advice on the easiest route to achieve this.

3.9 Training & Education

I. This policy is circulated to all new staff as part of their induction process

II. Awareness of Data protection issues is through updates from the Information and Support Manager.

3.10 Co-ordination and Compliance

I. The data protection co-ordinator and compliance person is the CEO (Data Protection Officer)

II. All staff are made aware of this role via email updates

III. All breaches of this policy will be reported to the Data Protection Officer following the Data Loss Notification Procedure below.

IV. A formal review by the co-ordinator of data protection activities within Aspire will take place annually across the organization.

4. Procedures

4.1 Personal Data Access Procedure

I. All requests must be made in writing with the consent of the person served (except for the conditions outlined under section 3 this policy).

II. All requests should be made using the form attached (appendix 3) and sent to:

Aileen Cruise- Aspire CEO

Aspire

Carmichael Centre, Coleraine House, Coleraine Street, Dublin 7.

III. Where requests are received in writing not using the standard form, e.g. from solicitors, staff should check the validity of the request before notifying the Data Protection Officer. The request must quote the Data Protection legislation and also include the person served written consent. When in doubt, revert to the requestor with the standard form in appendix 3.

IV. The Data Protection Officer must be notified of all requests for disclosure of personal information.

V. The Data Protection Officer will record the request and notify the Service Manager(s) connected with the case.

VI. The Service Manager will coordinate the file duplication and disclosure.

VII. The information will be supplied within 40 days.

4.2 Requests made under the Freedom of Information Act (1997 and 2003)

I. Aspire is not prescribed body under the terms of the Freedom of Information Act. However, records that are created in dedicated services subject to contracted service level agreements with HSE are deemed to be held by the HSE and thus, may be subject to come within the scope of the act.

II. “Section 6(9) provides that the records of contractors to public bodies are deemed, insofar as they relate to the contracted service, to be held by the public body concerned.”

III. Aspire's policy is to comply fully in a timely manner with all Freedom of Information requests made by the HSE under the terms of the service level agreements.

IV. If a request is received by Aspire under the terms of the Freedom of Information Acts, it should be immediately forwarded to the Data Protection Officer for further action and processing.

4.3 Procedure for Data Loss Notification

A breach is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, for an authorized purpose, have access or potential access to personal data in usable form, whether manual or automated.
This could mean:

- Loss of a laptop, memory stick or mobile device that contains personal data
- Lack of a secure password on pc's and applications
- Emailing a list of service users to someone in error
- Giving a system login to an unauthorised person
- Failure of a door lock or some other weakness in physical security which compromises personal data

What happens if a breach occurs?

Actual, suspected, or potential breaches should be reported immediately to the Aspire Data Protection Officer. Any employee who becomes aware of a likely data breach and fails to notify the DPO will be subject to Aspire's disciplinary procedure.
A team comprising the DPO and other relevant staff will be established to assess the breach and determine its severity. Depending on the scale and sensitivity of data lost and the number of Data Subjects impacted, the Office of the Data Protection Commissioner and relevant regulatory bodies will be informed as quickly as possible following detection.
In certain circumstances Aspire may (e.g. if required by the Office of the Data Protection Commissioner), inform the data subjects of the loss of their data and provide them with an assessment of the risk to their privacy. Aspire will make recommendations to the data subjects which may minimise the risks to them. Aspire will then implement changes to procedures, technologies or applications to prevent a recurrence of the breach.

When will the Office of the Data Protection Commissioner be informed?

All incidents in which personal data has been put at risk will be reported to the Office of the Data Protection Commissioner. The only exceptions to this policy are when the data subjects have already been informed, where the loss affects fewer than 100 data subjects, and where the loss involves only non-sensitive, non-financial personal data.
Where devices or equipment containing personal or sensitive personal data are lost or stolen, the Data Protection Commissioner is notified only where the data on such devices is not encrypted.

Data Loss Incident logging

All data breaches will be recorded in an incident log as required by the Office of the Data Protection Commissioner. The log will maintain 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 will include a brief description of the nature of the incident and an explanation of why the Office of the Data Protection Commissioner was not informed (if relevant). Such records will be provided to the Office of the Data Protection Commissioner.

5. Persons responsible for implementation

The Board of Aspire is responsible for approval and oversight of policies.
The CEO is responsible for communicating policy and review to all management and staff.
Service Managers/Co-Ordinators are responsible for security of data relating to their services.
The DPO is responsible for overall security, reviews, investigating, reporting and addressing breaches.
Staff are responsible for adhering to the policy and maintaining security of the data they access.

5. Definitions

General Data Protection Regulation (GDPR): The GDPR came into effect on 25 May 2018, replacing current Irish and EU data protection legislation. New concepts, such as 'data protection by design and default', are legislated for. This means that Privacy Impact Assessments should be used to embed data privacy directly into the design of projects at an early stage

Data Protection Officer (DPO): A Data Protection Officer is a designated person appointed by an organisation to advice on data protection practices. The DPO for Aspire Ireland is the CEO.

Personal Health Information: Personal data relating to the physical or mental health of an individual; including its use for the provision or registration of health and social care services, which reveal information about a person's physical or mental health status. May also be referred to in this policy as Medical/Health Information.

Personal Data: "personal data" shall mean any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

6. Relevant legislation

Freedom of Information Acts 1997 & 2003

Data Protection Acts, 1988 & 2003

7. Appendix

Appendix 2: Records held in HR		
Records held in HR	**Default retention period**	**Final action**
Annual/sick leave records	1 years	Destroy by confidential shredding
Time sheets	1 year (unless alternate period specified by funder)	Destroy by confidential shredding
Records of staff training	5 years	Destroy by confidential shredding
Job description	Retain indefinitely	Archive
Applications and CV's of candidates who are called for interview	Retain for 2 years after closing of competition	Destroy by confidential shredding
Selection criteria	Retain indefinitely	Archive
Candidates not qualified or short listed	Retain list of candidates who applied, but destroy material such as application forms and CV's after 2 years.	Destroy by confidential shredding
Candidates short listed but not successful at interview or who are successful but do not accept offer	Retain for 1 year (with candidates permission) then destroy	Destroy by confidential shredding
Interview Board marking sheet and interview Board notes	Retain for 2 years then destroy	Destroy by confidential shredding
Finance/pension/ retirement records	Retain until pensioner and dependent spouse are deceased and dependent children are finished full time education plus 3 years.	Destroy by confidential shredding
Staff Personnel Files	Retain for duration of employment. On retirement or resignation hold for a further six years but retain service records for finance/pension purposes. Destroy remainder listed below.	Destroy by confidential shredding
Application/CV	See above	
References	See above	

Recruitment medical	See above	
Contract/Job specification/ Job description	See above	
Probation forms	See above	
Parental leave	Retain for 8 years	Destroy by confidential shredding
Discipline records	Hold on personal file/disciplinary file for duration of employment plus six years after resignation/retirement, then destroy. Where disciplinary policy provides for earlier removal destroy but keep a record that a warning was issued. Where the matter involved criminal activity these records should be retained indefinitely.	Destroy by confidential shredding
Allegations and complaints	Where the complaint is found to be untrue or unwarranted make a note on personal file index that a complaint was made, but there is no need to keep detailed documentation or refer back to previous cases if further separate allegations are made in the future.	
Occupational health records	Depending on the types of materials to which the staff member was exposed (e.g. carcinogens) the health screening reports may need to be retained for up to 40 years. Consult with your local Health & Safety Officer about retention periods for this class of record.	
Industrial relations files	Hold policy documents and the history of their evolution indefinitely.	Archive
Agreements-pay and others	Retain indefinitely	Archive
Leave policy	Retain indefinitely	Archive
Employment policy	Retain indefinitely	Archive
Surveys/reports	Retain indefinitely	Archive
Union correspondence	Retain indefinitely	Archive

Individual industrial relations issues	Retain indefinitely	Archive
Minutes of meetings	Retain indefinitely	Archive
Labour Court Recommendations	Retain indefinitely	Archive
Contracts for services Examples of contracts for services that may be held by Personnel/HR departments include EAP contracts with service providers and contracts with healthcare professionals.	Retain for the duration of the contract plus six years	Destroy by confidential shredding

Appendix 2: Guidelines on Retention of Client Records		
Type of information	**Schedule**	**Notes**
Individual records of the persons accessing Aspire services	Destroyed on completion of the service.	Paper and electronic media
Health and medical records	8 years after completion of service	
Application forms for services and supports	Destroyed on completion of the service	Paper and electronic media
External referral forms for referrals to Aspire	To be included in the record for persons admitted and will be retained for the same period as the record itself (see above)	
Information for statistical/ Audit purposes	There will be no time limit on such information being retained at this generally will be anonymous.	Information to be held anonymously where possible. Exceptions may need to be made for purposes of funder reports, accreditation audits.
Membership forms	Retention for 2 years after non-renewal of membership	Paper and electronic media

Appendix 3: Personal Data Request Form

Aileen Cruise- CEO
Aspire
Carmichael Centre, Coleraine House, Coleraine Street, Dublin 7

[**Date**]

Dear Madam,

I wish to make an access request under the Data Protection Acts 1988 and 2003 for a copy of any information you keep about me, on computer or in manual form. I am making this request under section 4 of the Data Protection Acts.

Regards

[Your Name]

Name (Print)	
Address	

Please Note:

Request in writing should be made and signed by the applicant in person.
Within the terms of the Data Protection Act 1988/2003, Aspire will respond to your request for personal data within 40 days.

Requests should be submitted to: CEO, Aspire, Carmichael Centre, Coleraine House, Coleraine Street, Dublin 7.