THE NATIONAL DOWN SYNDROME POLICY GROUP

Data Protection Policy – GDPR

The National Down Syndrome Policy Group is committed to a policy of protecting the rights and privacy of individuals in accordance with the General Data Protection Regulation (GDPR) which became law in May 2018.

Introduction

The National Down Syndrome Policy Group needs to gather, process, store and sometimes share certain information about individuals (Data Subjects). These can include members (both individuals and organisations), officers, and other people the organisation has a relationship with or may need to contact such as Members of Parliament, those with specialist knowledge and interest. This policy describes how this personal data must be collected, handled and stored to meet our organisation's data protection standards — and to comply with the law.
This data protection policy ensures the National Down Syndrome Policy Group:

- Complies with data protection law and follows good practice
- Protects the rights of members and related parties
- Is transparent about how it stores and processes data
- Protects itself from the risks of a data breach

Data protection law

The GDPR describes how organisations, including the National Down Syndrome Policy Group, must collect, handle and store personal information.
These rules apply regardless of whether data is stored electronically, on paper or on other materials.
To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.
The GDPR is underpinned by eight important principles. These say that personal data must:

- be fairly and lawfully processed and not processed unless specific conditions are met;
- be obtained for one or more specified, lawful purposes and not processed in any manner incompatible with those purposes;
- be adequate, relevant and not excessive for those purposes;
- be accurate and, where necessary, kept up to date;
- not be kept for longer than is necessary;
- be processed in accordance with the data subject's rights under the DPA;
- be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage;
- not be transferred to countries outside the European Economic Area (EEA) unless the country or territory ensures adequate protection for the rights and freedoms of the data subjects.

Lawful bases for processing of personal data

We are able able to collect, store and process personal information on a lawful basis with the consent of our members. Members may be individuals or an organisation. Members are required to positively opt-in and are able to withdraw consent at any time by emailing lucienne@dspg.uk We have processes in place to refresh consent at appropriate intervals and regularly review consents to check that the relationship, processing and the purposes have not changed.

Collecting, storing and processing of personal data will only be undertaken by the National Down Syndrome Policy Group where we have consent. Processing personal data enables the National Down Syndrome Policy Group to contact an individual about public policy matters, current events, to join a petition, letter writing, or other sort of public policy related campaigns that we believe they would have a genuine interest in. If we did not process, store and share our data when required, it would hugely impact on our ability to campaign effectively for the objectives of the National Down Syndrome Policy Group.

Special Category Data

Special category data is personal data that needs more protection because it is sensitive. the National Down Syndrome Policy Group will only collect, store and process special category data regarding race or ethnic origin, political opinions, genetic data and data concerning health from individuals who have given explicit consent. If an individual refuses or withdraws consent they are still able to be a member of the National Down Syndrome Policy Group and participate as fully as their consent allows, and all special category data we have collected on the individual will be deleted from our records. An individual can request their special category data

be deleted from their records by contacting us at lucienne@dspg.uk Collecting specific, minimal and relevant special category data will enable the National Down Syndrome Policy Group to provide appropriate resources and information. This will enable the National Down Syndrome Policy Group to process data to ensure support for all those with Down Syndrome and their families, to raise awareness of the condition and to promote equality of opportunity and treatment.

Where we are processing children's data or data of vulnerable people we will take extra care to protect their interests.

Scope of the Policy

This policy applies to:

- All officers, and volunteers of the National Down Syndrome Policy Group
- All other organisations and people working on behalf of the National Down Syndrome Policy Group

It applies to all data that the group holds relating to identifiable individuals and organisations, which might include:

- Names of individuals, ages and dates of birth
- Contact information including addresses, email addresses and phone numbers
- Social media, Gift Aid and image preferences
- Fundraisers, supporters, funding partners
- Donations and financial data
- Any other individual or organisation who contacts us or we may need to contact

Outside agencies and organisations

In order for us to campaign effectively, or to enable us to provide the best possible service for our members, data may be shared with other organisations with the Data Subject's permission. When the National Down Syndrome Policy Group uses other agencies, that agency will be carefully selected and required to use appropriate measures to protect the confidentiality and security of personal data. Agencies will be asked to sign an agreement to this effect.

Unfortunately, the transmission of information via the Internet or a mobile phone network connection is not completely secure. The National Down Syndrome Policy Group cannot guarantee the security of personal data transmitted using these applications: any transmission is at the data subject's own risk.

Sometimes the group uses selected third parties to provide support services in connection with its website, mobile applications or in the normal course of business. These parties may, from time to time, have access to your personal data to enable them to provide those services to The National Down Syndrome Policy Group. The National Down Syndrome Policy Group requires all third parties providing such support services to meet the same standards of data protection as The National Down Syndrome Policy Group's own. Any third- party will be prohibited from using your personal data for that third party's own purposes.

Data protection risks

This policy helps to protect the National Down Syndrome Policy Group from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the group could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works with the National Down Syndrome Policy Group has some responsibility for ensuring data is collected, stored and handled appropriately.
Each individual that handles personal data (Data Processors), including officers, volunteers and other agencies, must ensure that it is handled and processed in line with this policy and data protection principles.
However, these people have key areas of responsibility:

- The National Down Syndrome Policy Group is the Data Controller. The Founding Officers are ultimately responsible for ensuring that the National Down Syndrome Policy Group meets its legal obligations.

- The Data Protection Officer, Lucienne Cooper, is responsible for:
    - Keeping the officers updated about data protection responsibilities, risks and issues
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule
    - Arranging data protection training if needed and advice for the people covered by this policy

- Handling data protection questions from staff and anyone else covered by this policy
- Overseeing requests from individuals to see the data the National Down Syndrome Policy Group holds about them.
- Checking and approving any contracts or agreements with third parties that may handle the group's sensitive data

Officer/Volunteer/Other agency Guidelines

All officers, volunteers and contractors should adhere to the following:

- Only gather, process, access and share personal data in accordance with legitimate group needs
- The only people able to access data covered by this policy should be those who need it for their work, and this should be the minimum number possible
- Data should not be shared informally.
- All data should be kept secure, by taking sensible precautions and following the guidelines in this policy
- In particular, strong passwords must be used, and they should never be shared. Passwords should be changed regularly
- Personal data should not be disclosed to unauthorised people, either within the group or externally
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of securely
- Officers and volunteers should request help from the data protection officer if they are unsure about any aspect of data protection

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Data Protection Officer.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet
- Paper and printouts are not left where unauthorised people could see them, like on a printer
- Data printouts should be shredded and disposed of securely when no longer required

- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be protected by strong passwords that are changed regularly and never shared with unauthorised individuals
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should be backed up frequently
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones when avoidable
- This information is stored in password protected files and secure online platforms and can only be accessed by those working with The Down Syndrome Policy Group identified in this Data Protection Policy..
- All servers and computers containing data should be protected by security software and a firewall
- Prevent virus attacks by taking care when opening emails and attachments or visiting new websites

Data Use

- When using data at home, nobody in the home (children, visitors, workmen) should be given the opportunity for unauthorised access to your data.
- Personal data should not be shared informally.
- Always check intended recipients of an email are correct.
- Data must only be used for legitimate group purposes, and must strictly never be used by officers/volunteers/contractor for work not related to the National Down Syndrome Policy Group or for their own means
- Data must be password protected before being transferred electronically.
- Personal data should never be transferred outside of the European Economic Area.

Data Accuracy

The law requires the National Down Syndrome Policy Group to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all officers/volunteers/other agencies who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Unnecessary additional data sets should not be taken.
- Every opportunity to ensure data is updated should be taken, and give data subjects regular opportunities to update their information
- The National Down Syndrome Policy Group will make it easy for data subjects to update the information the National Down Syndrome Policy Group holds about them.
- Data should be updated as inaccuracies are discovered.
- It is the responsibility of each officer/volunteer/other agency to ensure databases for which they are responsible are regularly checked and are up to date.

Data Requests

All individuals who are the subject of personal data held by the National Down Syndrome Policy Group have the right to:

- Ask what information the group holds about them and why
- Ask how to gain access, and be given access to it
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations

If an individual contacts the organisation requesting this information, this is called a Subject Access Request.

Subject Access Requests from individuals should be made by email, addressed to the data controller at lucienne@dspg.uk There should be no charge for this. The data controller will aim to provide the relevant data within 28 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the National Down Syndrome Policy Group will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the officers and from the company's legal advisers where necessary.

Providing information

The National Down Syndrome Policy Group aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the group has a privacy statement, setting out how data relating to individuals is used by the National Down Syndrome Policy Group and outlining the Data Subject's rights which includes the right to see their personal data, the right to know how it is used, stored and processed, and the right to withdraw their consent or change their preferences at any time. It is available on request from the Data Controller at lucienne@dspg.uk

The National Down Syndrome Policy Group may contact an individual via post, email, telephone or SMS text. However, we will only contact an individual by the channel they have told the National Down Syndrome Policy Group they wish to receive communications by and where we have received their consent to do so.

The National Down Syndrome Policy Group will aim to capture an individual's voluntary consent for Direct Marketing purposes at the data collection point. If they do consent, we will also aim to capture their contact channel preferences at the data collection point. As a default position the National Down Syndrome Policy Group will consider consent to remain valid while an individual is financially supporting us or receiving our regular communications and have not objected to doing so. Consent can be withdrawn at anytime by emailing lucienne@dspg.uk

An individual can give or withdraw consent to Direct Marketing, or change their contact channel preferences, at any time by emailing us at lucienne@dspg.uk

Data breach procedure

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

This might include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;

- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data

In the event of a data breach or suspected breach, it is essential that officers, volunteers or agents notify the Data Protection Officer immediately.

When a personal data breach has occurred, there is a need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk then the ICO must be notified; if it's unlikely then the incident does not need to be reported, but the decision must be justified and documented.

In the event of a breach the following actions might be taken depending on the nature of the breach:

- Identify the breach and carry out an assessment to assess the likely risk to individuals https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
- Notifying the data subject of the disclosure of their personal information without undue delay
- Requesting that any unintended recipients delete or destroy the data immediately
- Notifying the Independent Commissioner's Office of any serious breach https://ico.org.uk within 72 hours, or document decision not to inform the ICO
- Logging all Data Breach incidents even if they don't have to be reported to the ICO and record follow up actions to address it
- Meeting with relevant individuals to discuss how to prevent further breaches/training
- Review of policy and procedure if required (usually every 2 years)

It is the responsibility of all volunteers/officers/other agencies to ensure that the collection, maintenance and processing of personal data concerning volunteers, officers, members, contractors, related organisations, suppliers and any other individuals with whom the National Down Syndrome Policy Group has dealings, follows the GDPR rules on good data protection practice, and the guidance in the National Down Syndrome Policy Group Protection Policy.

All data processors working with the National Down Syndrome Policy Group, including officers, employees, volunteers and other agencies will be asked to sign a sheet saying they have read our Data Protection Policy. (Appendix 1)

This Data protection Policy may be revised to take account of changes in working practice or applicable law. If so, this policy will be amended. The National Down Syndrome Policy Group volunteers/officers/other agencies will be made aware of any amendments by email and asked to read the policy changes and sign a sheet saying they have done so. (Appendix 1)

This National Down Syndrome Policy Group Data Protection Policy is reviewed every two years. The next review is due March 2023.

Appendix 1

THE NATIONAL DOWN SYNDROME POICY GROUP DATA PROTECTION POLICY SIGNATURE SHEET
(Employees/volunteers/officers)

Please return only this sheet to Data Officer Lucienne Cooper at lucienne@dspg.uk

This is to confirm that I have read, understood and accepted the National Down Syndrome Policy Group's Data Protection Policy for volunteers/officers. I will only use personal data collected by the National Down Syndrome Policy Group for legitimate purposes and will use appropriate measures to protect the confidentiality and security of this data in line with the GDPR.

Name: _____

Signature: _____

Position in Organisation: _____

Date: _____