Data Protection and Freedom of Information Policy

Director Responsible	**Chief Executive**
Author	**Information Governance Officer**
Approved by	**SMT**
Issue Date	**May 2018**
Review Date	**August 2019**

DOCUMENT HISTORY

Date	Author/Editor	Summary of Changes	Version No.
Sept 2009	Data Protection Group		1
June 2014	M Turner/ L McCairn	Policy Review – no major changes as legislation remains current	2
August 2016	M Turner	Update policy to include Freedom of Information legislation	3
June 2017	M Turner	Revision to SAR process; include reference to GDPR; include PECR information	4
April 2018	M Turner	Updated for GDPR compliance	5

Please note that the only valid version of the policy is the most recent one. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

CONSULTATION AND RATIFICATION SCHEDULE

Name of Consultative Body	Date of Approval
Board of Trustees	
Senior Management Team	
Policy Subgroup	April 2018
Regional Managers Forum (RMF)	April 2018
New Struan Management Team	April 2018

CROSS REFERENCE TO OTHER POLICIES / STRATEGIES

This policy should be read in conjunction with:	Detail
Policy 1	Records Management Policy
Policy 2	Information Security Policy and Security Incident Management Procedure
Policy 3	IT and Systems Usage Policy
Guidance	Volunteers Guidance

EQUALITY & PRIVACY IMPACT ASSESSMENTS

Log Number: 2018/6	**Date completed:** April 2018

KEYWORDS: DATA PROTECTION, FREEDOM OF INFORMATION, FOI, ICO, SUBJECT ACCESS, ENVIRONMENTAL INFORMATION REGULATIONS, EIR, PERSONAL DATA, DATA STORAGE

CONTENTS

1. INTRODUCTION

The General Data Protection Regulation (GDPR) replaces the UK Data Protection Act (1998) as of 25 May 2018.

This policy explains how Scottish Autism, as a Data Controller, manages personal data subject to these Regulations.

New Struan School has been designated a public authority and is therefore subject to The Freedom of Information (Scotland) Act 2002 (FOISA). The FOISA legislation applies to information we hold and publish about the School and its **educational activities**, and not our residences or the wider organisation. Alongside the Act, the Environmental Information (Scotland) Regulations 2004 (the EIRs) provide a separate right of access to environmental information we hold.

The purpose of this policy is to enable Scottish Autism to:

- Comply with the law regarding data processing
- Follow good practice
- Enable us to evaluate, respond to and monitor FOISA and EIR requests
- Protect our staff, service users and volunteers and data relating to external contacts
- Protect the organisation from the consequences of a breach of its responsibilities

2. POLICY STATEMENT

We will endeavour to be transparent with individuals whose data is processed and to provide training and support to staff who are handling data so that consistency is achieved. This will enable us to comply with law and good practice, whilst respecting individuals' rights, as well as ensuring that the public's right to access information under FOISA legislation is met.

3. SCOPE

This policy applies across the organisation to all staff, casual workers and volunteers. It is also relevant to our suppliers who may be data processors, and applies to any personal data we may process about external data subjects during the course of our business.

4. DEFINITIONS

Personal data
The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, e.g. name, identification number, location data or online identifier,

Special categories of data
See Section 6

Data Subject
A data subject is anyone who has their personal data processed by a data controller.

Data Processing
"Processing" personal data refers to any operations performed on a data subject's personal data (whether those operations are automated or not). This may include (but is not limited to) collecting, recording, storing, erasing and destroying data.

Data Controller/ Data Processor
A data controller determines the purposes and means of processing personal data.
A data processor is responsible for processing personal data on behalf of a controller.

5. PRINCIPLES OF GDPR

The Regulation is underpinned by six principles which state that data about someone must be processed with the data subject's rights at the forefront of activity. Data must be:

- Fairly, lawfully and transparently processed
- Processed for limited purposes
- Adequate, relevant and limited to what is necessary
- Kept accurate and up to date
- Not kept in a format where the data subject can be identified for longer than is necessary
- Secure to prevent the loss, destruction or unauthorised disclosure of data

In addition, organisations are required to demonstrate compliance with the above (See Section 19).

6. LAWFULNESS OF PROCESSING

Depending on how you engage with us, we may process your data for the following legitimate reasons:

- With your consent
- To fulfil a contract with you
- To comply with our legal obligations
- To protect the vital interests of a data subject
- To meet our responsibilities under the 'public interest' requirements
- Where it is in our legitimate interests to do so, and your rights and freedoms are not negatively impacted

Various types of processing activity may be undertaken for one or more of the legitimate reasons above. If you ask us about your data, we will tell you which of the above reasons apply. Further details of our legitimate bases for processing your data can be found in our Privacy Policy on our website.

'Special Categories' of Data

Special categories of personal data include the following:

- The racial or ethnic origin of data subjects
- Their political opinions
- Their religious beliefs or other beliefs of a similar nature

- Whether they are a member of a trade union
- Health information
- Genetic or biometric data used to identify a data subject
- Data about sexual orientation or sex life

We will only process this type of data about you in the following circumstances:

- With your consent
- To meet our obligations under social security, employment and social protection law
- To protect the vital interests of a data subject if they are unable to give us their consent
- In accordance with our legitimate activities in relation to our purposes as a charity, where we will not share the information with third parties without your consent
- Where this information has already been made public by you
- In defence of legal claims
- Where there is substantial public interest benefit
- For purposes of occupational health, assessment of working capacity of an employee, or for the provision of health and social care services
- Where there is a public health reason
- For archiving, research or statistical purposes

7. YOUR RIGHTS

As a data subject you have the following rights when we process your data (see our privacy notice for full information):

- The right to be informed about how we process your data
- The right to access information we process about you – see the section on 'Subject Access requests' below
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object to us processing your data
- Rights in relation to automated decision making and profiling

8. SUBJECT ACCESS REQUESTS

Individuals have the right to access data held about them under a 'subject access request'. such requests will be dealt with by the Information Governance Manager and the relevant Regional Manager/ Principal/ Head of Department.

Any such request must be made in writing. A copy of this policy and a Subject Access Request Form (Appendix 1) may be sent to anyone making such a request. The organisation will acknowledge receipt of a request in writing and set a date by which the request will be fulfilled. The organisation must respond without undue delay, and within one calendar month.

For further information refer to the Information Commissioner's Office website or contact the Information Governance Manager.

In accordance with the regulation, Scottish Autism will provide the following information:

- Whether or not we process any data about you
- The purposes of the processing
- Categories of data processed
- Categories of third parties with whom we may have shared your data with
- Retention information
- Where we obtained your data (if not obtained from yourself) – if we know this
- Any use of automated decision-making on your data
- If your data has been transferred overseas and how we protected it

We can provide you with a copy of your personal data undergoing processing, and this will usually be supplied electronically. Supervised access to Scottish Autism's premises to access the relevant records may be granted if appropriate. The data subject must satisfy Scottish Autism of their identity prior to information being released.

Rectification and Erasure

Should any of the data we hold about you be inaccurate, you have the right to request us to rectify it and we will do so without undue delay. In certain circumstances you also have the right to request that we stop processing your personal data, and we will do this without undue delay if this is appropriate. Please note that there are some exemptions to this right and Scottish Autism will inform you as to our ability to meet this right should you choose to exercise it.

You can contact us at our Head Office: Scottish Autism, Hilton House, Whins Rd, Alloa FK10 3SA or by email: info@scottishautism.org .

9. PRIVACY AND ELECTRONIC COMMUNICATIONS REGULATIONS (PECR)

Scottish Autism's fundraising and marketing activities include electronic communications (e.g. email, phone, text, social media) with supporters. We comply with the PECR alongside the GDPR. We obtain consent for our fundraising/ marketing communications and have a valid privacy notice on our website. Our supporters may opt out of receiving marketing information at any time. We are clear on our use of cookies and have a statement explaining this.

10. FREEDOM OF INFORMATION ACT (SCOTLAND) 2002

This legislation puts an obligation on public authorities to make information readily accessible to the public and to comply with requests for information that is held but not published. It covers information relating to the educational activities of the school.

The Act requires Scottish public authorities to produce and maintain a **publication scheme**. We call this our 'Guide to Information' and it is available on the New Struan website. This outlines what information New Struan routinely publishes. Public authorities are under a legal obligation to:

- publish the classes of information that they make routinely available
- tell the public how to access the information and what it might cost.

A FOISA request may come in to any part of the organisation and does not need to quote the legislation. It does however need to be made in writing (or other reviewable format to comply with Equality Act requirements) and a contact name and address (email address is suffice) is required. Fees may apply – see our 'Guide to Information' for details.

There are formal processes for managing FOISA and EIR requests and all such requests must be forwarded to the Information Governance Manager immediately. There is a 20 day time limit for responses to requests for information.

All requests are logged and monitored, and statistics are reported quarterly to the Scottish Information Commissioner's office.

Not all information is disclosable – there are 'exemptions' which apply and any queries about the validity of a request should be directed to the Information Governance Manager as soon as possible on receipt of request.

Should they be dissatisfied with the response received from new Struan School, requestors have a right to internal review, and then a further right of appeal to the Scottish Information Commissioner. All responses to requests for information will detail these rights to enquirers.

Staff can find further information on the Intranet, New Struan school website, on the Scottish Information Commissioner's website (www.itspublicknowledge.org) or from the Information Governance Manager.

11. ENVIRONMENTAL INFORMATION REGULATIONS 2004

Alongside FOISA, the public has a right to access environmental information about New Struan School. The definition of environmental information under these Regulations is very wide. Some examples include information about air, water, land, landscaping, biodiversity, architecture, internal building environment, recycling, and energy usage. This list is not exhaustive.

If you think you may have received a request for environmental information, please forward it to the Information Governance Manager immediately.

EIR requests may be made verbally or in writing. The fee structure for EIRs is slightly different to that for FOISA requests – see our 'Guide to Information' for details.

12. RESPONSIBILITIES

The Board of Trustees has overall responsibility for ensuring the organisation complies with legal obligations under the legislation.

Scottish Autism is a Data Controller under the GDPR. The Data Controller is responsible for ensuring that necessary steps are taken to ensure compliance with the Regulation.

The Information Governance Manager fulfils the role of Data Protection Officer (DPO). We are required to have a named DPO due to the nature of the data we routinely process. The DPO has responsibility for ensuring that the organisation maintains day-to-day

compliance with the legislation and for reporting any breaches to the Information Commissioner. They also have responsibility for reporting quarterly statistics for FOISA/ EIR requests to the Scottish Information Commissioner.

The IT Manager has responsibility for ensuring that our electronic systems are maintained in line with the legislation.

All staff and volunteers are required to read, understand and accept any policies and procedures relating to the processing, recording and storage of data about individuals that the organisation supports. Staff also have a duty to report any data breaches in line with the Security Incident Management procedure. Breaches of the Data Protection policy may be dealt with under the organisation's disciplinary procedures.

All staff are required to be aware of the FOISA and EIRs legislation, the obligations it puts on New Struan School as a public authority, and how to deal with any such request.

In general, access to personal information will be dealt with as a subject access request by the Information Governance Manager and the Head of Service within the region or department concerned. In limited cases personal data may be disclosed under FOISA - the Information Governance Manager can provide guidance on which legislation applies.

13. CONFIDENTIALITY

Confidentiality applies to a wider range of information than that subject to Data Protection legislation, and as such the organisation has a separate Confidentiality policy statement.

14. DATA RECORDING AND STORAGE

Data on any individual will be recorded in as few places as possible, and duplication of data sets is discouraged. Procedures to ensure that all relevant systems are updated when personal information changes will be regularly reviewed.

Scottish Autism has developed a document retention schedule as part of the Records Management Policy and this should be referred to when records are being stored or are to be archived.

Closed Circuit television (CCTV) is used on limited Scottish Autism sites. The majority of CCTV equipment is used to control access to premises and does not routinely record images. At New Struan School, CCTV footage is recorded, and information retained for one week, after which it is automatically deleted. This information may be shared with law enforcement authorities if required in the aims of security or for the protection of our pupils, staff and visitors to the school.

The GDPR expects anyone handling personal information to protect it and ensure that it is not lost, stolen or misused. Should any information be lost, this may be reportable to the Information Commissioner's Office. Our Information Security Policy has further details on how we protect data organisationally, and what we do should a data breach occur

15. USE OF PORTABLE DEVICES TO RECORD AND TRANSPORT ELECTRONIC DATA

Our IT Usage Policy contains guidance on our policies on use of mobile phones and other portable items.

16. THIRD PARTY INFORMATION

Some information held about a person may also contain information about other people, who are then known as a 'third party'. If the organisation cannot provide the data requested under a subject access request without disclosing information that would identify that third party, then the organisation does not have to disclose this information. This does not apply if permission to disclose the information has been given by the third party.

The Section 60 Code of Practice provides information to public authorities on good practice and requirements relating to the FOISA and EIR legislation. This includes informing third parties, including suppliers, that their information may be the subject of a FOISA/ EIR request for information. Scottish Autism aims to be as transparent as possible with suppliers and will include appropriate clauses in relevant contracts and tender documents.

17. CONSENT

Scottish Autism's privacy notice can be found on our website. We will ask people's permission to use their data for specific purposes, e.g. communications about organisational activities, and send an 'unsubscribe' option with every such communication.

Some information about volunteers may be made public, depending on their role. Consent from volunteers will be sought for this (see Volunteers Guidance documents). An example of this would be where photographs are taken of activities involving service users and volunteers, and the organisation wishes to publish these. Information about members and supporters will only be made public with their consent.

Scottish Autism acknowledges that consent to use certain information can be withdrawn at any time. This will apply from the date of receipt of such notification and cannot be backdated. There may be occasions where it would be necessary to retain data for a specific period of time, even though consent for using it has been withdrawn. The organisation will respect the rights of the individual in this regard, unless doing so would endanger the person concerned.

18. PROCUREMENT/ DATA PROCESSORS

Whenever a data controller uses a processor to process data on its behalf, a written contract needs to be in place, which will define responsibilities and liabilities. We will only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects are protected.

The GDPR imposes restrictions on the transfer of personal data outside the European Union. Personal data may be transferred outside of the EU if appropriate safeguards are

in place, as defined by the ICO on their website. Scottish Autism contracts with data processors who are either based in the EU or provide adequate evidence of the safeguarding of our data in line with ICO requirements.

Our standard terms and conditions contain clauses relevant to Data Protection.

19. EVIDENCING COMPLIANCE/ ACCOUNTABILITY

Article 5(2) of the GDPR places a duty on a data controller to "be responsible for, and be able to demonstrate, compliance with the principles." Scottish Autism has implemented appropriate technical and organisational measures to demonstrate compliance. These include:

- Maintenance of relevant documentation on processing activities
- Appointing a data protection officer
- Working to the principles of data protection by design and data protection by default
- Ensuring policies and procedures about appropriate data management are in place
- Using data protection impact assessments where appropriate.

20. POLICY REVIEW

This policy will be reviewed during 2019 to ensure compliance with legislative references linked to the UK's departure from the European Union