Information Handling Policy

Document title	Information Handling Policy
Reference number	ISP-07
Version	3
Date issued	2 December 2021
Last revision	1 February 2024
Policy owner	IT and Transformation Director
Policy lead	Head of Educational ICT
Directorate	Information Technology

Contents

Introduction

This Information Handling Policy sets out the requirements relating to the handling of our charity's information assets. Our charity manages diverse sets of information impacted by a broad range of contractual obligations, legislation, and formal guidelines. In such an environment, it is essential that our information assets be properly managed in order to protect against the consequences of breaches of confidentiality, loss of integrity, service interruption, and non-compliance with legislation or contracts. Our policies and associated procedures will be routinely reviewed to ensure alignment with any changing obligations.

Inventory and ownership of information assets

An inventory of our charity's main information assets will be maintained by the IT Department. Each asset's nominated owner (see table below) has responsibility for defining the appropriate uses of that asset and ensuring appropriate security measures are in place to protect it.

Security classification

Each information asset will fall into one of three classifications which reflects the sensitivity of the asset according to the following classification scheme:

- **Public** – available to any member of the public without restriction, applies where no data protection concerns arise
  Examples: information about autism, press releases, publicity materials

- **Confidential** – available only to specified staff, with appropriate authorisation.
  Examples: staff home contact information including next of kin etc., staff appraisal information. Anything that is counted as 'personal information' under the Data Protection Act.

- **Highly Confidential** – available to only a very small set of staff, with appropriate authorisation.
  Examples: staff medical information, data on adults we support, pupil records, incident reports, board reports. Anything that is counted as 'special category' information under the Data Protection Act.

Key Information Asset groups and responsibilities:

Area	Owner	Lead	Classification
Adults currently supported	Director of Adult Services	Area Manager	Highly confidential
Pupils currently supported	Director of Education	Principals	Highly confidential
Current staff	People Director	HR Managers	Highly confidential
Customer contacts	Director of National Programmes	Head of Data Services	Confidential
Governance	Chief Finance Officer	Head of Governance	Highly confidential
Research	Director of Assurance and Compliance	Head of Research	Highly confidential
Published material	Director of National Programmes	Head of Communications	Public
Finance	Chief Finance Officer		Confidential
Commercial contracts	Chief Finance Officer	Contracts Manager	Confidential

Customer data	Director of National Programmes	Product/service owners	Highly confidential
Archived files	IT and Transformation Director	IT Archive Manager	Highly confidential
Customer intelligence or behaviour data	Director of National Programmes		Highly confidential

All staff who handle personal information are 'information handlers', and as such are expected to know the applicable policies and procedures.

Access and Processing of information

Staff and volunteers at our charity will be granted access to the information they need in order to fulfil their roles. Once granted access they must not pass on information to others unless those others have also been granted the same level of access through appropriate authorisation.

Wherever practical, information should be created, stored, processed and shared electronically rather than on paper.

Wherever practical, all information classified as confidential or above should be collected, processed and stored in an appropriate system ('application') designed to support the processes it facilitates. These systems will:

- Apply formal role-based access controls to restrict information to those who need it.
- Provide an audit trail of all changes to data.
- Be provided on devices that ensure the security of information and the safety of those who use them.

Where non-public categories of data are involved, and where a commercially sourced, IT Department-approved, data processing application with its own internal security protocols is not in use, then file level protection using Microsoft Information Protection should be used as available to classify and secure the data. Training and support for these capabilities will be provided as the tools are rolled out.

The use of email and electronic folders for managing confidential or highly confidential data requires particular care and should be very carefully managed. Our charity is investing in systems designed to handle information correctly and support business operations. While these applications are being introduced particular care is required in using the systems they are replacing.

Our charity applies several specific standards to support the handling of information. These include:

- BSI 27001 (information security)
- BSI 10012 (personal information)
- BSI 10008 (legal Admissibility electronic information management)
- BSI 22301 (Business continuity)

Although not certified to these standards for reasons of costs and economies, our charity regularly audits itself against them to ensure our policies, process and systems are compliant.

Where a system exists to process information, the export of confidential or highly confidential data into uncontrolled systems such as Microsoft Office should be avoided. Where it cannot be avoided though it should only be performed by an approved information handler and where approved by the information asset owner or their designated lead.

Information handlers are responsible for ensuring that where they have export (reporting) capabilities that these adhere to our charity information policies. ISP-05 addresses the training mandated for information handlers.

Privacy impact assessments

The introduction of new information systems or significant changes to existing information systems (electronic or paper) involving personal data requires a privacy impact assessment. Details about these are provided in the Data Protection Impact Assessment Guidance IGG-01.

Disposal of information

Great care needs to be taken to ensure that information assets are disposed of securely. Information can only be disposed of in line with the charity's retention guidelines as advised by the Data Protection Officer (see IGP-04). No information relating to pupils, people we support or staff is to be destroyed without the consent of the IT and Transformation Director. Usually this consent will be granted by delegated approving procedures, but in cases outside these normal procedures, specific approval must be sought.

For information that is archived or held in long term storage, permission to destroy must be sought from the IT and Transformation Director who will liaise with the Director of Assurance & Compliance and the Data Protection Officer. For details of the process see Appendix A2 of IGP-04.

Data within systems can be set for review or to automatically expire after a set time. Information held outside systems (e.g. in shared folders) must be reviewed regularly to ensure legal and contractual compliance.

Data that needs to be kept for an extended period without being needed for operational reasons will be archived digitally in the NAS archive. Details of how this is done are available from the IT Department, whose members can also advise about archive access.

Electronic information must be securely erased (or otherwise rendered inaccessible) before leaving the possession of our charity. Usually this is undertaken by an NAS-approved contractor. In cases where a storage system (for example a computer hard drive) is required to be returned to a supplier it should be securely erased before being returned unless contractual arrangements are in place with the supplier which guarantee the secure handling of the returned equipment. If this is not possible, then the storage system should not be returned to the supplier and should remain in the possession of our charity until it is disposed of securely. The IT Department will advise.

Removal of information from NAS premises

Charity data which is subject to the Data Protection Act or which has a classification of confidential or above should be stored using charity facilities. However, it may be stored with third parties subject to a written contract with our charity. All third-party processors must be approved by the Director of IT. Usually our charity will expect approved third parties processing such data to have ISO27001. In all cases where it is necessary to remove data from our charity, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss.

Care needs to be taken when information assets are in transit. Charity supplied mobile devices must always be fully encrypted.

Using personally owned devices

Any processing or storage of charity information using personally owned devices must comply with our Mobile and Remote Working Policy (ISP-14).

Information on desks, screens and printers

Members of staff who handle confidential paper documents should take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times. (Also refer to ISP-14 for remote and home workers.)

Care should also be taken when printing confidential documents to prevent unauthorised disclosure, for example the use of "follow me" printing where available.

Computer screens on which confidential information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be screen-locked while unattended.

Backups

The Director of IT is responsible for ensuring that appropriate back up arrangements are in place for all information systems. Backup polices are included within the IT service continuity policy (ISP – 02).

Exchanges of information

Whenever any personal data or other confidential information are exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred. Regular exchanges must be covered by formal agreements. Information classified as 'highly confidential' may only be exchanged electronically – both *within* our charity *and* in exchanges with third parties - if the information is strongly encrypted prior to exchange. (*Hard* copies of information classified as 'highly confidential' must only be exchanged with third parties via secure (for example, special) delivery and marked "addressee only".)

When exchanging any information by email, file transfer process or fax, recipient addresses should be carefully checked prior to transmission.

All exchanges of personal data into or out of our charity must be logged in accordance with the Data Protection Act and so only undertaken by an approved information handler.

Unsolicited emails, faxes, telephone calls, instant messages or any other communication requesting information which is not classified as public should not be acted upon unless the authenticity and validity of the communication has been verified.

Compliance Monitoring

Audits of information compliance will be carried out periodically in line with the sensitivity of information being processed. While the primary purpose of these audits is to ensure legal and contractual compliance, they will also be carried out with the aim of improving charity efficiency and efficacy in information handling. Advice and suggestions for improvement will be offered as well as ensuring legal and contractual compliance.

While being supportive around data handling it is important to understand that failure to comply with this policy is a disciplinary offence and actions which jeopardise the personal data of others may be dealt with as gross misconduct.

Reporting losses

All staff and volunteers of the National Autistic Society have a duty to report the loss, suspected loss or unauthorised disclosure of any charity information asset to the Data Protection Officer.