Information Handling Policy

Document title	Information Handling Policy
Reference number	ISP-07
Version	2
Date issued	02/12/2021
Last revision	24/11/2021
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 over) 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 be assigned a security classification by the asset owner which reflects the sensitivity of the asset according to the following classification scheme:

- **Public** – available to any member of the public without restriction.
  Examples: information about autism, press releases, publicity materials

- **Open** – available to any authenticated staff
  Examples: policies and procedures, internal communications, staff lists

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

- **Sensitive and Confidential** – available to only a very small number of Staff, with appropriate authorisation.
  Examples: staff medical information, pupil records, incident reports. Usually anything that is counted as 'special category' information under GDPR.

- **Secret** – the most restricted category. It is not anticipated that many charity assets will be assigned this classification.
  Examples: anything covered by the Official Secrets Act or non-disclosure terms.

Key Information Asset groups and responsibilities:

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

Customer data	Director of Fundraising and Commercial Development	Product/service owners	Sensitive and confidential
Archived files	Director of IT	IT Archive Manager	Sensitive and confidential
Customer intelligence or behaviour data	Director of National Programmes		Sensitive and confidential

All staff who handle personal information are expected to know the policies and procedures that are applicable.

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 within our charity. Once granted access they must not pass on information to others unless those others have also been granted access through appropriate authorisation.

Wherever practical, information should be created, stored, processed and shared in electronic form rather than on paper. The key reasons for this are to:

- Allow access to information anywhere and at any time: we are a geographically dispersed organisation, and having paper records located in only one place is inefficient and has attendant risks
- Allow for indexing and searching in more effective way
- Allow workflows to be structured according to business rules ensuring legal and contractual compliance. This includes ensuring appropriate staff have access to information they need to do their job whilst facilitating audit
- Allow us to improve the quality and quantity of information captured
- Make backing up and securing our records much easier, as well as easing the disposal of records at the end of their period of use. Currently we have a range of records that are stored in dispersed locations across the NAS, meaning loss of a single location could severely impact our organisation
- Save physical space
- Save environmental resources
- Recognise that electronic copies are generally cheaper to create, store, process and dispose of than paper records

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.

The use of email, electronic folders and applications for managing personal or 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 sensitive data into uncontrolled systems such as Microsoft Office should be avoided and only done by an approved information handler and where approved by the information asset owner or their deputy.

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

Privacy impact assessments

Significant changes to any information system (electronic or paper) involving personal data requires a privacy impact assessment. This assessment needs to be conducted by a qualified person in line with Information Commission Office guidance. Our charity operates to the ICO code of practice for conducting privacy impact assessments. Information handlers may be involved in undertaking these assessments in line with IT procedures. Specific training is provided in these cases. Further details are available from our Data Protection Officer.

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 our charity data retention policy - Appendix A. No information relating to clients 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 for data disposal in line with our charity retention guidelines. In cases outside these normal procedures, 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 Compliance and the Data Protection Officer. Details of the process are in Appendix B.

The length of time information must be kept varies according to the information type (see appendix A). Directors are accountable for ensuring that information is disposed of in a legally compliant manner at the end of the retention period. Usually this will be done in

conjunction with the IT and Transformation Director. Directors may delegate responsibility in this area but remain ultimately accountable.

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, members of which can 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

Charity data which is subject to GDPR 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 to process confidential and sensitive 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.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure.

Computer screens on which confidential or sensitive 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

Security of information also includes the protection from loss. All information stored electronically requires that appropriate backup and system recovery measures are in place. Where backups are stored off site, appropriate security measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures should be tested on a regular basis.

The principles also apply to third party services such as cloud-service providers.

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 significant amounts of 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 'confidential and sensitive' may only be exchanged electronically – *within* our charity *and* in exchanges with third parties - if the information is strongly encrypted prior to exchange. Information classified as 'secret' may not be transmitted electronically except with the written permission of the CEO. Hard copies of information classified as 'confidential and sensitive' or above must only be exchanged with third parties via secure (for example, special) delivery.

When exchanging 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 GDPR 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 our 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.

Appendix A – Data Retention

Introduction

Data will be retained for periods as defined by relevant legislation and / or contractual commitments. The retention periods for specific categories of data, which are reviewed regularly, are listed below along with the actions to be taken at end of life.

Archiving

The term archiving applies to the process of moving data from one place to another for the purposes of long-term retention. The process is most commonly used to refer to the moving of data no longer operationally used into a more efficient and more secure location. The most common example of this is data associated with staff who have left or clients who we no longer support. Their data is no longer needed for operational purposes and so can be archived "offline" where it can be retained for reference purposes. This applies to paper and digital data.

It is important to note that archiving should not be used to retain data beyond their retention periods. Our charity will be scanning documents where the data is subject to longer retention periods to convert historic paper archives to digital (client records for example). It is critical to note that only scanning process that meet the BSI 10008 (legal admissibility and electronic information management) standard will allow us to destroy the original paper records. Ordinary scans do not meet this standard and so the paper needs to be retained as well.

The processes around digital archiving and in particular the digitisation of paper records are still being ratified in the charity, and until that is complete no client records or staff records should be destroyed without explicit trustee approval. These records will be securely stored until approval is provided. This may mean some records will be retained beyond the retention periods below.

National Autistic Society information data retention periods (v0.2 May 2018)

Note: Additional HR and finance data to be added.
Breakdown of customer data to be provided to include Customer intelligence and specifically derived Customer data

Type of data	Law(s) pertaining/guidance	Retention period	Action at end of life
Personnel record – summary information	Common Practice, allows references to be provided	Permanent	None

Personal employment record	Section 5 Limitation Act 1980 and Data Protection Act 1998	years from end of employment	Secure disposal

Governance

Type of data	Law(s) pertaining/guidance	Retention period	Action at end of life
Trusts and Endowments managed by the Governing Body (trustees)	Information and Records Management Society 2016	Archived when the school closes.	Archived
Records relating to complaints dealt with by the Governing Body (trustees)	Information and Records Management Society 2016	Date of the resolution of the complaint + a minimum of 6 years, then review for further retention in case of contentious disputes	Secure disposal
Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	Information and Records Management Society 2016	Date of the meeting + 3 years then review	Secure disposal
Correspondence created by senior managers	Information and Records Management Society 2016	Date of correspondence + 3 years then review	Secure disposal
For trading parts of the NAS: company accounts, books and records.	Section 388(4)(a)(b) Companies Act 2006	6 years	Secure disposal

HR

All records leading up to the appointment of a new member of staff – unsuccessful candidates	Information and Records Management Society 2016	Date of appointment of successful candidate + 6 months	Secure disposal

All records leading up to the appointment of a new member of staff – successful candidate	Information and Records Management Society 2016	Add relevant information to the staff personal file, all other information retained for 6 months	Secure disposal
Pre-employment vetting information – DBS Checks	DBS Update Service Employer Guide June 2014: Keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education) Sections 73, 74	The NAS does not have to keep copies of DBS certificates. If the NAS does so the copy must NOT be retained for more than 6 months	Secure disposal
Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Information and Records Management Society 2016	Where possible these should be checked and a note kept of what was seen and checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file	As per personal file below
Pre-employment vetting information – Evidence proving the right to work in the United Kingdom	An employer's guide to right to work checks [Home Office May 2015]	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	Secure disposal
Staff Personal File	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	Secure disposal
Reports on employee performance, review meetings, appraisals, MSDs, training records, employment contracts (and amendments), correspondence, details of	Section 5 Limitation Act 1980 and Data Protection Act 1998	Termination of Employment + 6 years	Secure disposal

promotions and demotions, sick leave records.			
Allegation of a child protection nature against a member of staff including where the allegation is unfounded	Currently, The Independent Inquiry into Child Sexual Abuse (IICSA) guidance to not destroy any record relating to child sexual abuse means we keep records until they say otherwise. If not related to sexual abuse, then applicable legislation is: "Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	Sexual abuse: indefinitely while the Independent Inquiry into Child Sexual Abuse (IICSA) continues. Otherwise, Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	See details to left.
Disciplinary Proceedings: oral warning		Where the warning relates to child protection issues see above. Otherwise Date of warning + 6 months	Secure disposal. [If warnings are placed on personal files then they must be weeded from the file]
Disciplinary Proceedings: written warning – level 1		Date of warning + 6 months	Secure disposal. [If warnings are placed on personal files then they must be weeded from the file]
Disciplinary Proceedings: written warning – level 2		Date of warning + 12 months	Secure disposal. [If warnings are placed on personal files then they must be weeded from the file]

Disciplinary Proceedings: final warning		Date of warning + 18 months	Secure disposal. [If warnings are placed on personal files then they must be weeded from the file]
Disciplinary Proceedings: case not found		If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	Secure disposal.

Financial records

Type of data	Law(s) pertaining/guidance	Retention period	Action at end of life
Payments cash book or record of payments made	Companies Act 2006; Charities Act 2011	Six years from the end of the financial year in which the transaction was made	Secure disposal
Purchase ledger	Companies Act 2006; Charities Act 2011	Six years from the end of the financial year in which the transaction was made	Secure disposal
Invoice - revenue	Companies Act 2006; Charities Act 2011	Six years from the end of the financial year in which the transaction was made	Secure disposal
Petty cash records	Companies Act 2006; Charities Act 2011	Six years from the end of the financial year in which the transaction was made	Secure disposal
Invoice - capital item	Companies Act 2006; Charities Act 2011	Ten years	Secure disposal
Bank paying in counterfoils	Companies Act 2006; Charities Act 2011	Six years from the end of the financial year in which the transaction was made	Secure disposal
Bank statements	Companies Act 2006; Charities Act 2011	Six years from the end of the financial year in which the transaction was made	Secure disposal

Remittance advice	Companies Act 2006; Charities Act 2011	Six years from the end of the financial year in which the transaction was made	Secure disposal
Correspondence re donations	Companies Act 2006; Charities Act 2011	Six years from the end of the financial year in which the transaction was made	Secure disposal
Deeds of covenant/ Gift Aid declarations	Companies Act 2006; Charities Act 2011	Six years after the last payment made or twelve years if	Secure disposal
		payments outstanding or in dispute	
Legacies	Companies Act 2006; Charities Act 2011	Six years after the estate finalised	Secure disposal
Receipts cash book	Companies Act 2006; Charities Act 2011	Ten years	Secure disposal
Sales ledger	Companies Act 2006; Charities Act 2011	Ten years	Secure disposal
All payroll documentation (including tax records)	Taxes Management Act 1970	Six years plus current year	Secure disposal

Admissions to schools or services

Type of data	**Law(s) pertaining/guidance**	**Retention period**	**Action at end of life**
All records relating to the creation and implementation of the School/Service Admissions' Policy	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Life of the policy + 3 years then review	Secure disposal

			enquiries from past pupils/users to confirm the dates they attended.
Admissions – if the admission is successful	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels December 2014	Date of admission + 1 year	Secure disposal
Admissions – if the appeal is unsuccessful	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools 'adjudicators and admission appeals panels December 2014	Resolution of case + 1 year	Secure disposal
Register of Admissions	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.	The school or service may wish to consider keeping the admission register permanently as often schools and services receive

Operational administration

Type of data	**Law(s) pertaining/guidance**	**Retention period**	**Action at end of life**
Visitors' Books and Signing in Sheets	Information and Records Management Society 2016	Current year + 6 years then REVIEW	Secure disposal
Records relating to the creation and publication of the school/service brochure or prospectus	Information and Records Management Society 2016	Current year + 3 years	Standard disposal
Records relating to the creation and distribution of circulars to staff, parents or pupils	Information and Records Management Society 2016	Current year + 1 year	Standard disposal

Care records in residential

Note that the judgement in R(C) v Northumberland County Council (NCC) and Information Commissioner's Office (Interested Party) stated that the minimum that a child's care record should be kept for is 35 after they leave. This should inform all the retention periods below.

Type of data	Law(s) pertaining/guidance	Retention period	Action at end of life
Residential care children's file	Section 50 of SI 2010 No 959 The Care Planning, Placement and Case Review (England) Regulations 2010; Children's Act 1989 The Arrangement of Placement of Children (General) Regulations 1991: Regulation 9 Fostering Service Regulations 2002/SI 2002 No 57	75 years from 18th birthday	Secure disposal
Records in respect of children in Children's Homes as described in Schedule 4 of the Children's Homes Regulations 2001 Amendment 2011	Children's Homes Regulations 2001, (Reg. 29 (1)) Schedule 4.	At least 15 years after the child is discharged from the home	Review, secure disposal (The primary purpose of retention is to provide information to enquire and to assist in the investigation of allegations of abuse made by
			those formerly looked after in children's homes)
Documents relating to the operation of the establishment. This covers diaries, rotas etc.	Records Management Society of Great Britain, Local Government Group 2002	25 years from date last record added to file.	Secure disposal
Children Looked After	The arrangements for Placement of Children (General) Regulations 1991 and the Children's Homes (Amendment) Regulations 2011.	Until child is 75. If they die before 18, keep for 15 years from date of death.	Secure disposal. (The primary purpose of retention of these records is as a service to the child.)

Medical records	Records Management: NHS Code of Practice Part 2	Retain until the person's 25th birthday	Secure disposal

Child Protection

Type of data	Law(s) pertaining/guidance	Retention period	Action at end of life
Child Protection files	Currently R(C) v Northumberland County Council (NCC) and Information Commissioner's Office (Interested Party). Previously: Education Act 2002, s175, related guidance "Safeguarding Children in Education", September 2004	35 years after leaving school or service	Secure disposal

Pupil Records

Type of data	Law(s) pertaining/guidance	Retention period	Action at end of life
Pupil's Educational Record	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437	Transfer to new provider. No files need be retained. If any child leaves and goes to different provider then either transfer to new school or return to the LA. If any child leaves education at transfer that child's record is kept for 25 years.	Transfer
Attendance registers	Information and Records Management Society 2012	Transfer copy and keep copy from date of register for 3 years	Secure disposal

Special Educational Needs files, reviews and Individual Education Plans	Information and Records Management Society 2012	DOB of the pupil + 25 years then review. This retention period is the minimum period that any pupil file should be kept. It may be wise to keep SEN files for a longer period of time to defend against a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period.	Secure disposal
Examination results (public)	Information and Records Management Society 2012	Year of examinations + 6 years	Secure disposal
Statement maintained under The Education Act 1996 - Section 324	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	Secure disposal unless legal action pending
Proposed statement or amended statement	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	Secure disposal unless legal action pending
Advice and information to parents regarding educational needs	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	Secure disposal unless legal action pending
Accessibility Strategy	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	Secure disposal unless legal action pending
Parental permission slips for school trips where there has been a major incident	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	Secure disposal

Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Secondary Schools	3-part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 10 years	Secure disposal

Health and Safety

Accessibility Plans	Disability Discrimination Act	Last plan + 6 years	Secure disposal
Accident Reporting - adults	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	Date of incident + 6 years	Secure disposal
Accident Reporting – children	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	DOB of child + 25 years	Secure disposal
COSHH	Information and Records Management Society 2012	Closure + 10 years	Secure disposal
Incident reports	Information and Records Management Society 2012	Closure + 25 years	Secure disposal
Risk Assessments	Information and Records Management Society 2012	Daye of assessment + 3 years	Secure disposal
Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	Information and Records Management Society 2012	Last action + 40 years (note: even if no asbestos exists a clean asbestos report should be kept)	Secure disposal
Fire Precautions log books	Information and Records Management Society 2012	Date of log + 6 years	Secure disposal

Admin

Type of data	**Law(s) pertaining/guidance**	**Retention period**	**Action at end of life**
Employer's Liability certificate	Information and Records Management Society 2012	Closure of the school + 40 years	Secure disposal
Type of data	**Law(s) pertaining/guidance**	**Retention period**	**Action at end of life**

	Administration Act 1992 Section 8. Limitation Act 1980	when youngest child will be 25 and use that date).	
Accident Reporting - adults	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	Date of incident + 7 years	Secure disposal
Accident Reporting – children	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security	DOB of child + 7 years from child's 18th birthday (work out	Secure disposal

Appendix B

Process for destruction of archived materials

Data owners who identify data that they think needs to be securely destroyed which is currently stored either at NAS premises or with third party companies need to provide the following information:

Which Directorate does the data come from
Where the information is currently stored
What physical form does it take (boxes of paper files, electronic files, loose paper, photographs, bound books. etc.)
What does the information consist of – a description of all the information in reasonable detail
When does the information date from
If personal data are the people it refers to employees, volunteers, pupils, people we care for or some other category
Are these people still with the NAS – if not when did they leave
What retention period applies to the data contained
Are there any outstanding complaints or investigations relating to any of the people on whom data is held

This information should be sent to the Director of IT and Transformation and they will liaise with the Director(s) who are data owners, the Director of Compliance and the Data Protection Officer. A decision on permission (or request for further information) will be provided within 14 days.

Destruction can only be carried out by approved third party suppliers and certificates of destruction must be provided.