Information Handling Policy

Document title	Information Handling Policy
Reference number	ISP-07
Version	1
Date issued	02/08/2019
Last revision	02/08/2019
Policy owner	IT and Transformation Director
Policy lead(s)	Head of Educational ICT
Directorate	Information Technology

Contents

Introduction

This Information Handling Policy forms a part of the Information Security Policy (ISP-01) and sets out the requirements relating to the handling of our charity's information assets. Information assets must be managed in order to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance with legislation (or contracts) which would otherwise occur. Our charity manages a diverse set of information covered by a broad range of legislation, contractual obligations and formal guidelines. This policy and associated procedures are routinely reviewed to ensure they are in line with these obligations. Please note that where the term staff is used this includes contract or agency staff as well as volunteers etc.

Inventory and ownership of information assets

An inventory of our charity's main information assets will be developed and maintained and the ownership of each asset clearly stated.

Each asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect it.

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	Principles	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 Centre of Autism	Head of Research	Sensitive and confidential
Published material	Director of External Affairs	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 External Affairs		Sensitive and confidential

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

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.

Access and Processing of information

Staff and volunteers of our charity will be granted access to the information they need in order to fulfil their roles within our charity. Staff or volunteers who have been granted access must not pass on information to others unless the 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:

- Allowing access to information anywhere and at any time: we are a geographically dispersed organisation, having paper records located in only one place is inefficient and risky
- Allows for indexing and searching in more effective way
- Allows 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 as well as allowing our charity to audit access
- Collecting information electronically allows us to improve the quality and quantity of information captured
- Electronic records make backing up and securing our records much easier, as well as easing the disposal of them at the end of their use. Currently we have a range of records that are stored in single locations across the NAS, meaning loss of a single location could severely impact our organisation
- Using electronic copies saves physical space
- Using electronic copies saves environmental resources
- 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 that need it.
- Provide an audit trail of all changes to data.
- Be provided on devices that ensure the security of information and safety of those that use them.

The use of email, office products and folders 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 for these standards our charity is regularly audited to ensure we are meeting them and that our policies, process and systems meet them. All organisations that process our information are expected to meet these standards and most of our local authority and NHS commissioning bodies audit us to these standards as well.

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 SIRO or their delegate.

Information handlers are responsible for ensuring that where they have export (reporting) capabilities that they apply our charity information policy.

Privacy impact assessments

Significant changes to any information system (electronic or paper) involving personal data requires a privacy impact assessment to be conducted in line with GDPR. This assessment needs to be conducted by a qualified person in line with ICO 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.

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 can be destroyed without the consent of the IT and Transformation Director. Usually this consent will be granted by approving procedures for data disposal in line with our charity retention guidelines. In cases outside these normal procedures, approval must be sought.

The length of time information must be kept varies according to the information (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 to expire after a set time or be set to flag for review after a set time. Information held outside systems (e.g.: in shared folders) must be reviewed regularly to ensure legal and contractual compliance in this area.

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 can be done are available from the IT Department, who can also guide staff on how data may be accessed from archives.

Advice and support in this matter is available from the SIRO (Senior Information Risk Owner), the Head of Data Protection and the IT Department.

Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of our charity, unless the disposal is undertaken under contract by an 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.

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 or with third parties subject to a formal, written legal contract with our charity, wherever possible. All third-party processors must be approved by the SIRO to check their information security provisions. Usually our charity will expect third parties used to process confidential and sensitive data will be expected to have ISO27001 compliance throughout its service model. In cases where it is necessary to otherwise 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 follow our charity 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 locked while unattended.

Backups

Security of information also includes the protection from loss. All information stored electronically requires 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.

This also applies to third party services specifically the cloud. 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)
Information which is entrusted to the care of IT Services will meet these requirements.

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 a formal written agreement with the third party.
Information classified as confidential and sensitive may only be exchanged electronically both 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 explicit 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 checked carefully prior to transmission.
All exchanges of personal data into or out of our charity must be logged in accordance with GDPR and 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 until and 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.

References and further guidance

Conducting Privacy impact assessments – Code of practice (ICO)

Related policies

ISP 02 IT service continuity policy
ISP 04 Outsourcing and third-party compliance policy.
ISP 16 Encryption policy
IGP 02 Data protection Policy

Appendix A – Data Retention policy

Introduction

Data will be retained for periods as define by relevant legislation and or contractual commitments. These are reviewed regularly the retention periods for specific categories of data 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 move data that is no longer operationally used to a more efficient and more secure method or location. The most common example of this is data associated with staff that have left or Clients that we no longer support. The data is no longer needed for operational purposes and can be archived "offline" where it can be retained for the purposes that remain. Once data is no longer operationally required it will be archived for the remainder of the period, we need to retain it for. 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. Please see point below
Our charity will be using scanning processes to convert historic paper archives to digital ones where we have long retention periods (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 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 and until that is complete no client records or staff records can be destroyed without explicit trustee approval. These records will be securely stored until approval is provided. This may mean some long term 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

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

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	7 years from end of employment	Secure disposal

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
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

			enquiries from past pupils/users to confirm the dates they attended.

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

Type of data	**Law(s) pertaining/guidance**	**Retention period**	**Action at end of life**

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
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

	Administration Act 1992 Section 8. Limitation Act 1980	when youngest child will be 25 and use that date).	

Appendix B - Legislation

The following appendix lays out some of the legislative framework under which this Policy has been produced.
Note that, in most cases, an action that is illegal if committed offline is also illegal if committed online. For this reason, not, all laws are covered here, only those that specifically relate to online behaviour.

Privacy and Electronic Communications Regulations 2003

The Privacy and Electronic Communications Regulations specifically regulate the use of electronic communications (email, SMS text, cold calls etc.) as a form of marketing and allow individuals to prevent further contact.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority
- Obtain unauthorised access to a computer
- "Eavesdrop" on a computer
- Make unauthorised use of computer time or facilities
- Maliciously corrupt or erase data or programs
- Deny access to authorised users

General Data protection Regulations (GDPR) And 2018 Data protection Act.

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights

- Secure
- Not transferred to other countries without adequate protection

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

This amendment obliges website owners to inform users about their use of cookies and seek consent for setting more privacy intrusive cookies.

Counter-Terrorism and Security Act 2015

Accessing websites or other material which promotes terrorism or violent extremism or which seeks to radicalise individuals to these causes is likely constitute an offence under this act.

Digital Economy Act 2010

The Digital Economy Act regulates the use of digital media in the UK and deals with issues such as online copyright infringement. It provides obligations on Internet Service Providers to prevent infringement.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against them is guilty of an offence if they know, or ought to know, that their course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice including by phone or using the Internet. It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, that they are in a position of trust with. (Typically, teachers, social workers, health professionals, fall in this category of trust).

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

Human rights to be aware of in this area include:

- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The NAS is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Principals, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Retention periods are set out in the following legislation, regulations and guidance
An employer's guide to right to work checks [Home Office May 2015]
Children's Act 1989
Children's Homes Regulations 2001, (Reg. 29 (1)) Schedule 4.
Control of Asbestos at Work Regulations 2012
Control of Substances Hazardous to Health Regulations 2002.
DBS Update Service Employer Guide June 2014
Education Act 2002
Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance).
Health & Safety of Pupils on Educational Visits (HASPEV) (1998).
Keeping children safe in education statutory guidance for schools and colleges March 2015
Limitation Act 1980
Records Management: NHS Code of Practice Part 2
Regulation 9 Fostering Service Regulations 2002
Safeguarding Children in Education, September 2004
School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014
School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014
Social Security (Claims and Payments) Regulations 1979.
Social Security Administration Act 1992
Special Educational Needs and Disability Act 2001
Statutory Maternity Pay (General) Regulations 1986 as revised 1999
The Arrangement of Placement of Children (General) Regulations 1991
The arrangements for Placement of Children (General) Regulations 1991
The Care Planning, Placement and Case Review (England) Regulations 2010
The Children's Homes (Amendment) Regulations 2011.
The Education (Pupil Information) (England) Regulations 2005