Document Title	**Data Retention Policy**
Date written	12th July 2018
Date last revised	5th December 2019
Type of document	Corporate
Brief summary of contents	To provide: • Privacy information relating to how the Group handles data • Identifies the length of time data should be retained • Protecting and storage of data • Safe disposal of personal data • Data subject rights • Identify the technical measures that should be employed for data retention and destruction
SLT member responsible for policy	Tony De'Ath
This document replaces	Any previous Rotherham, North Notts., Dearne or subsidiary retention policies
Approval route/consultation	Data Protection Officer, SLT Member
Head of Department (HOD) responsible for policy	Data Protection Officer
Author of policy	Ian Headley
Contact details	ianheadley@rnngroup.ac.uk
Publication location	Public and portal
Date of final approval	1st May 2019
Date policy becomes live	5th December 2019
Review period	Annual
Links to external standards	ICO The National Archives
Related documents	Data Protection policy Data Subject Access Request (DSAR) policy Security policy
Keywords	Privacy, data, retention, information, security, data subjects, protection, storage, rights,
Training needs	Data Protection

This document is only valid on the day of printing

Data Retention Policy

Version 1.3

5th December 2019

Version Control Table

Date	Version No	Summary of Changes	Changes Made By
12th July 2018	1.0	Birth of policy	Ian Headley
30th January 2019	1.1	Legislation update, annual review	Ian Headley
14th February 2019	1.2	Removal of appendices	Ian Headley
5th December 2019	1.3	References changed to Information Governance web site for additional information and schedule	Kelly Condon

All or part of this document can be released under the Freedom of Information Act 2000

Table of Contents

Appendices

1. Purpose, Scope, and Users

Under the Data Protection Act 2018 (incorporating the General Data Protection Regulations (GDPR)), data controllers (i.e. anyone determining the collection of personal data) should not retain personal data for any longer than necessary.

Furthermore, the DPA2018 gives data subject's additional rights in relation to the collection, maintenance and destruction of their personal data, which the RNN Group is mandated to uphold.

There are additional benefits to just meeting the legislative requirements in regards to effective records management and these are promoted for use throughout the Group to:

- protect our business critical records and improving business resilience
- ensure our information can be found and retrieved quickly and efficiently
- comply with legal and regulatory requirements
- reduce the risk of data breach or litigation and potentially audit or government investigations
- minimise storage requirements therefore reducing costs

Minimising data retention and having clear procedures in place to determine how and when to dispose of personal data is therefore key to complying with the DPA2018. Not only that, but a well-managed data retention plan can help to avoid the information overload and high storage costs resulting from the retention of unnecessary (and often redundant) data.

This Data Retention Policy is designed primarily to set out the limits that apply to the various types of personal data held by the RNN Group, to establish the criteria by which those limits are set, and to outline how personal data should be deleted or disposed of.

In addition, this policy indicates where, and how, personal data is held within the RNN Group, it provides a brief overview of data subject's key rights under the DPA2018, and gives a summarised overview of the various technical and organisational data protection measures that the Group has in place.

This policy describes both the required legislative retention periods for specified categories of personal data along with Group retention decisions for data and sets out the minimum standards to be applied when destroying certain information throughout the RNN Group. Further detailed retention periods are set out in the complete Data Retention Schedule available on the staff portal and RNN Group Information Governance web site.

This policy applies to all business units, processes and systems in all locations that the Group conducts business or has dealings in, or any other business relationships with third parties.

The policy applies to all RNN Group employees, agents, affiliates, contractors, consultants, advisors or service providers that may collect, process, or have access to data that the Group has determined the purpose for acting as data controller (including personal data and/or special categories of personal data). It is the responsibility of all of the above to familiarise themselves with this policy and to ensure adequate compliance.

This policy applies to all personal content collection and processing processes within the Group. Examples of documents collecting this type of data include, but is not limited to:

- Emails
- Hard copy documents
- Electronic documentation
- Video and audio recordings
- Photographic or video data
- Data generated by physical access control systems
- CCTV systems

The RNN Group defines a record as information collected, created, received and maintained as evidence and information in pursuance of legal obligations or in the transaction of its business.

You can find more information about what comprises a record in The National Archives introductory guide What is records management?

2. Reference Documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Data Protection Act 2018
- National Archives – Information Management Code
- Joint Information Systems Committee (JISC) – Guidelines for data retention
- Various other Acts of Parliament, including, but not restricted to, Human Rights Act 1998, The Limitation Act 1980, Disability Discrimination Act 1995 and the Freedom of Information Act 2000

3. Data Retention

3.1. Retention General Principle

For any category of documents not specifically defined elsewhere in this policy (or within the publicised RNN Group Data Retention Schedule) and unless otherwise mandated differently by applicable law, the required retention period for such documents will be deemed to be 2 years from its date of creation.

3.2. Retention General Schedule

The Data Protection Officer in conjunction with other managers of the Group, defines the time period for which documents and electronic records should to be retained and full details are made available to staff through the Group's publicised Data Retention Schedule.

As an exemption, retention periods within the Data Retention Schedule can be prolonged in cases such as:

- Ongoing investigations from EU authorities, if there is a possibility that records of personal data are needed by the RNN Group to prove compliance with any legal requirements; or
- When exercising legal rights in cases of lawsuits or similar court proceedings recognised under local law; or
- Ongoing investigations or storage requirements relating to safeguarding; or
- Ongoing medical investigations

3.3. Safeguarding of Data During Retention Period

The possibility that data media chosen for archiving may wear out should always be considered, normally directed by the retention period itself. If electronic storage media is chosen, any procedures and systems ensuring that the information can be accessed during the retention period (with respect to the media, the recovery device and readability of formats) shall also be stored in order to safeguard the information against loss as a result of future technological changes. The overall responsibility for the storage of personal data falls to the Data Protection Officer.

Consideration should also be taken in regards to the data subject rights, information must be made available within the legal timeframes should a right be exercised against the Group, within the data retention period itself.

3.4. Destruction of Data

The RNN Group and its employees should review all data on a regular basis, whether held electronically on their device, stored on the network or filed in paper format. To decide whether to destroy or delete any data once the purpose for which those documents were created is therefore no longer relevant.

The full data retention schedule is published on the staff portal and the RNN Group Information Governance web site.

Overall, lawful responsibility for the destruction of personal data ultimately falls to the Data Protection Officer but it is the individual's responsibility to ensure that retention periods are maintained as detailed on the Data Retention Schedule.

Once the decision is made to dispose of personal data according to the retention schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others, the risk to the Group and their level of confidentiality.

The method of disposal varies and is dependent upon the nature of the document. For example, any documents that contain business sensitive or confidential information (and particularly special category personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some expired or superseded contracts may only warrant in-house shredding. The Document Disposal Schedule section below defines the mode of disposal.

In this context, the member of staff shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way.

The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the Data Protection Officer subcontracts for this purpose. Any applicable general provisions under relevant data protection laws and the RNN Group's Data Protection Policy shall be complied with and will be stipulated as contract clauses should the destruction be actioned by a third party.

Appropriate controls shall be in place that prevents the permanent loss of essential information of the Group as a result of malicious or unintentional destruction of information – any incidents of this nature must be reported to the Data Protection Officer as soon as they are discovered, as this type of incident would be considered to be a data breach.

The Data Protection Officer shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed at all times.

3.5. Breach, Enforcement and Compliance

The person appointed with responsibility for Data Protection is the Data Protection Officer and has the responsibility to ensure that each of the Group's operating locations complies with this policy. It is also the responsibility of the Data Protection Officer to assist with enquiries from any local data protection or governmental authority such as the Information Commissioners Office (ICO).

Any suspicion of a breach of this Policy must be reported immediately to the Data Protection Officer via the online reporting form, by telephone, via email or directly to a member of the data protection team. All instances of suspected breaches of the policy shall be investigated and appropriate action taken.

Failure to comply with this policy may result in adverse consequences, including, but not limited to, loss of learner or customer confidence, litigation and loss of competitive advantage, financial loss and damage to the Group's reputation, personal injury, harm or loss.

Non-compliance with this policy by permanent, temporary or contract employees, or any third parties, who have been granted access to Group premises or information, may therefore result in disciplinary proceedings or termination of their employment or contract. Such non-compliance may also lead to legal action against the parties involved in such activities.

4. Document Disposal

4.1. Routine Disposal Schedule

Records that may be routinely destroyed when personal data is not a factor, or unless they are required to be retained as part of a larger record set, or subject to an ongoing subject access request, legal, safeguarding, medical or regulatory inquiry are as follows:

- Announcements and notices of day-to-day meetings and other events including acceptances and apologies;
- Requests for 'ordinary' information such as travel directions;
- Reservations for internal meetings without charges or costs;
- Transmission documents such as letters, fax cover sheets, email messages, routing slips, compliments slips and similar items that accompany documents but do not add any value or reference;
- Manual hand-written notes, when relevant electronic records are created
- Message slips;
- Superseded address lists, distribution lists etc.;
- Duplicate documents such as CC and FYI copies, unaltered drafts, snapshot printouts or extracts from databases and day files;
- In-house publications which are obsolete or superseded; and
- Trade magazines, vendor catalogues, flyers and newsletters from vendors or other external organisations.

In all cases, disposal is subject to any disclosure requirements, which may exist in the context of litigation for example.

4.2. Destruction Method

Level I documents are those that contain information that is of the highest security and confidentiality and those that include any personal or special category personal data. These documents shall be disposed of as confidential waste (shredded or incinerated, either internally or by an approved RNN Group contractor for this type of service) and shall be subject to secure electronic deletion. Disposal of the documents should include proof of destruction.

Level II documents are proprietary documents that contain confidential information such as parties' names, signatures, or information that could be used by third parties to commit fraud or may pose a risk to the rights and freedoms of the data subjects themselves. These documents should be shredded and electronic documents will be subject to secure electronic deletion.

Level III documents are those that do not contain any confidential information or personal data and are published RNN Group documents. These should be shredded or disposed of through a recycling company and include, among other things, advertisements, catalogues, flyers, and newsletters. These may be disposed of without an audit trail.

5. Data Subject Rights and Data Integrity

It is the Group's responsibility to uphold all of the rights of the data subject as described in UK Data Protection legislation. These specific rights are:

- Transparent communication
- Information to be provided to the data subject e.g. controller details, DPO, third parties with access etc.
- Information to be provided where personal data was not obtained from the data subject
- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Notification of rectification or erasure
- Right to data portability
- Right to object to processing
- Right to object to automated profiling decision making

Individuals have the right to be informed about the collection and use of their personal data, this includes awareness of the destruction processes followed by the RNN Group and is a key transparency requirement under UK Data Protection regulations.

The RNN Group has an obligation to provide individuals with information including our purposes for processing their personal data, retention periods for that personal data, and to whom it will be shared with, destruction of records is considered to be data processing.

It is the RNN Group's responsibility to ensure that individuals are kept informed that their personal data records may be stored in different locations and on different media (depending on operational benefits and efficiency) and for different periods of retention. The RNN Group must put steps in place to ensure all personal data records, including copies or duplicates, are always properly managed.

6. Technical and organisational data security measures

The destruction and disposal of valuable IT assets (including the data created and stored on the assets) when they are no longer required, for example hardware, portable media, non-paper based information or electronically shared items are just as important as paper based records, if not more so due to their very nature of easy portability.

This type of data and equipment requires the appropriate level of sanitisation to the information that was stored on the media itself.

6.1. What is sanitisation?
Any data, which is sensitive to our business, or personal data of data subjects should be removed from the media that stored it, just hitting 'Delete' is not enough.

Sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. Some forms of sanitisation will allow you to re-use the media data was originally stored on, while others are destructive in nature and render the media unusable.

6.2. When should I think about sanitising media?
There are a number of circumstances in which the Group will want to sanitise storage media:

- **Re-use:** When we want to allocate a device to a different user or repurpose some equipment within our organisation. We may also want to re-sell unwanted equipment so that it can be re-used elsewhere.
- **Repair:** We may need to return a faulty device to the vendor for repair or replacement.
- **Disposal:** We may wish to sanitise unwanted media before being passed outside our organisation — especially if there is limited confidence in the third party that is contracted to dispose of it on the Group's behalf.
- **Destruction:** We may have the means to destroy some media on our own site, or the Group may wish to send the media off site for destruction.

In all cases, the media will be outside its normal operating environment and is therefore subject to greater risk — from a different set of users, from third parties, or from less trusted organisations and individuals.

6.3. The risks of not sanitising
If data bearing surfaces are not treated properly, sensitive data may remain. This could result in the following problems for our business:

- unknown whereabouts of sensitive corporate data or personal data of data subjects
- loss of control over information assets
- critical data could be recovered and used by adversaries or competitors
- private or personal data about our learners, customers or staff could be used to commit fraud or identity theft
- intellectual property and personal data could be recovered and published openly, leading to potential fines, loss of reputation and revenue

6.4. Lost or stolen equipment
While this is not strictly a sanitisation issue, there are technical safeguards that the Group uses to manage the impact of loss or theft of devices containing personal or special category of data and confidential Group information.

One such technique is encryption. When data is stored in encrypted form, it is safe from all but the most sophisticated threats. It is therefore important to have data encryption enabled on laptops, smartphones and other mobile computing devices that are at greatest risk of loss or theft.

6.5. Managing storage media risks

In order to best manage the risks associated with data held on storage media, all staff should:

- understand the data on the storage media itself and its potential value outside our organisation
- understand the cost of sanitisation and add it to any procurement costs. Set aside some budget to address sanitisation.
- have a re-use and disposals policy in place, with key roles understood by everyone
- understand what technologies are being used
- retain the manufacturer manuals so it is known how to sanitise the media when necessary
- record the lifecycle of the storage media (what is it being used to store, where, and for how long)
- use trusted third parties and hold them to recognised standards
- obtain destruction certificates from third party destruction services
- ensure destruction processes and equipment are periodically tested
- verify that the data is being sanitised appropriately
- before disposal, remove all labels or markings that indicate ownership of the device (or the nature of the data contained)

6.6. Factors guiding the IT Services disposal policy

The following cost and risk considerations are used to help inform policy regarding the disposal of storage media:

- obligations to comply with environmental policy (for example WEEE).
- the availability of disposals companies, their services and their pricing schemes. Which services are they using? What is happening to the equipment when it leaves our organisation?
- geographic distance; if the suppliers' vans have to make stops en-route, risks are introduced that must be managed (for example using the 'two person rule').
- staff to have the skills to dismantle equipment onsite or to perform sanitisation on some types of equipment
- plan to get the most out of equipment during its useful life. For example, expensive smartphones will be reset and re-used within our business until they reach the end of their useful lives
- policy constraints around the donation or re-sale of certain equipment
- physical storage space needed to store end-of-life equipment, and what are the security arrangements around this storage
- time to store end-of-life equipment before accumulating a volume which is economically viable to dispose of
- assurance from cloud providers that our data will continue to be adequately protected from unauthorised users after a contract expires (that is, until remnants of the data are eventually overwritten).

7. Linked policies

- Data Protection Policy
- Data Subject Access Request Policy
- Mobile Phone Policy
- CCTV Policy
- Security Policy