POLICY INFORMATION (Policy no FR003)	
Subject	**Information Security and Data Protection Policy** *(This policy is non-contractual and is subject to periodic review and will be amended according to service development needs).*
Applicable to	All staff and volunteers of Nottinghamshire Hospice
Target Audience	Others such as agents, consultants and other representatives of Nottinghamshire Hospice may be required to comply with the policy as a condition of appointment.
Date issued	30 July 2024
Next review date	30 July 2025
Lead responsible for Policy	Director of Finance & Resources
Policy reviewed by	Director of Finance & Resources
Notified to (when)	Strategy and Corporate Governance Committee (16 July 2024)
Authorised by (when)	Strategy and Corporate Governance Committee (16 July 2024)
CQC Standard if applicable	
Links to other Hospice Policies	Risk Assessment Policy OP004 Use of Equipment Policy HR009 Disciplinary Policy and Procedure HR024
Links to external policies	
Summary	This Policy sets out how Nottinghamshire Hospice meets their obligations regarding retention of personal data collected, held, and processed and disposed of in accordance with General Data Protection Regulations (GDPR 2018).
This policy replaces	Data Protection Policy HR0005 Data Retention Policy OP006 Information Security Policy OP007 Confidentiality Policy HR00018

IMPORTANT NOTICE

Staff should refer to the Hospice website for the most up to date Policy. If the review date of this document has passed it is still valid for 3 months. After that staff should seek advice from their clinical lead or manager.

VERSION CONTROL		
Status	**Date**	**Review date**
Original policy (Information Security) written by Kate Rogers, Governance and Operations Manager	Oct 2021	
Policy reviewed by Rachel Hucknall, Chief Executive Director of Finance & Resources	Oct 2021 Nov 2022	
Policy ratified by Strategy and Corporate Governance Committee and added to website	Oct 2021	Oct 2022
Policy notified to Strategy and Corporate Governance Committee	16 July 2024	
Policy ratified by Strategy and Corporate Governance Committee	16 July 2024	16 July 2027
Updated control sheet and published on website	July 2024	

1.	**Introduction** Information Security and Data Protection are key components of Nottinghamshire Hospice management framework. This Policy sets out how Nottinghamshire Hospice meets their obligations regarding retention of personal data collected, held, and processed and disposed of in accordance with General Data Protection Regulations (GDPR 2018).
2.	**Aim and Scope** The aim of this policy is to set out the requirements and responsibilities for maintaining the security of information and data protection within Nottinghamshire Hospice. This includes: • preserving the **confidentiality, integrity and availability** of our business information • ensuring that all members of staff are aware of and fully comply with the relevant **legislation** as described in this and other policies • ensuring an approach to security in which all members of staff fully understand their own **responsibilities** • creating and maintaining within the organisation a level of **awareness** of the need for information and data protection • detailing how to **protect** the information assets under our control This policy applies to all information/data, information systems, networks, applications, locations and staff of Nottinghamshire Hospice or supplied under contract to it (Appendix 1).
3.	**Responsibilities** **Chief Executive Officer** has ultimate responsibility for information security at Nottinghamshire Hospice. **Director of Finance & Resources (Senior Risk Information Officer)** is responsible for: • Managing and overseeing the policy and related procedures on a day-to-day basis.

The business Information Risk Register and for recommending appropriate risk management measures.

- Reviewing the Policy and the Risk Register at least annually.

Line Managers are responsible for ensuring that all staff (permanent, temporary and contractors) are aware of:

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

Line managers shall be individually responsible for the security of information within their business area. Access to departmental information is controlled by access being approved on an individual basis by the line manager and/or the Director of Finance & Resources.

Line Managers must undertake a regular audit of files to ensure that the data they contain is:

- Adequate, relevant and not excessive
- Accurate and up to date
- Processed fairly and in accordance with GDPR
- Be obtained only for one or more specific lawful purposes
- Not kept longer than necessary
- Be held securely and not shared

Line Managers must be sure that adequate measures are taken to ensure the security of files and to ensure their employees understand their rights and responsibilities under the General Data Protection Regulations 2018.

In order to allow reasonable freedom of access to personal data, Line Managers are required to ensure their processing is undertaken on a regular basis to ensure that, through a wish to be open, The Hospice is not compromised under the GDPR.

Staff and Volunteers must understand their responsibilities to protect the company's data. Failure to do so may result in disciplinary action.

Human Resources will be able to provide guidance to managers who are unsure on the review of files and other responsibilities under GDPR.

Each member of staff shall be responsible for the operational security of the information systems they use. There is a security banner in place for all users at log on which confirms their accountability and actions for misuse.

Employees must not disclose personal data outside the organisation's procedures, or use personal data held on others for their own purposes. Failure to do so may lead to disciplinary action and dismissal.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

Access to the organisation's information systems by external parties shall only be allowed where a contract that requires compliance with this information security policy is in place. Such a contracts shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

It is expected that Nottinghamshire Hospices business partners who access the organisations information retains a high-level of information security, and follow all expectations outlined within this policy.

Human Resources

The length of time we keep Human Resources records is subject to guidance from the Information Commissioner, HMRC, contractual requirements under NHS. Files will be reviewed and regularly audited that ensure records are not kept beyond the standard retention times. All records that are no longer needed will be disposed of in a secure and careful way.

4.	**Definitions** **Personal data -** as any information relating to an identified or identifiable natural person (a “data subject”). **Special category (sensitive) personal data -** Such data includes, but is not necessarily limited to, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation. **Processing** - applies to a comprehensive range of activities. It includes collection, storage and use of data, accessing and disclosing data and its final destruction.
5.	**General Data Protection Regulations** (**GDPR) 2018** The GDPR sets out the different bases for being able to process personal data and also includes a number of rights for individuals which Nottinghamshire Hospice works to. These are detailed below. **The right to be informed** Data held on individuals will be held in as transparent a way as possible. • The Hospice will always tell people (staff and volunteers, patients, donors or others) when we are capturing their data, why it is being captured, how it will be used, how long it will be stored for, who will have access to it and their right to be forgotten and ask for all necessary consent beforehand. • Data relating to volunteering and staff will be held for contract and legitimate interest, patient’s data may be subject to NHS requirements and Donor data will additionally be treated in line with the Fundraising Regulator requirements. • Staff can always see their Human Resources file and check any information held there; they have the right to correct data. In relation to references or information from third parties this information will not be disclosed without the consent of third parties. Access is restricted to an individual’s personal data, they have no rights to seek clarification, access or view personal data

relating to any individual involved with Nottinghamshire Hospice without their consent.

- The Hospice will always tell an individual if it is processing their data in any way that is not obvious, for example making it clear that some information has to be passed to the pension company, when you become eligible for pension contributions. This will be both a contractual and legitimate interest condition.
- Sensitive data that can be connected with an individual will not be routinely kept except sickness records. This information will only be processed in connection with the sickness absence policy.
- Data is collected at the point of referral or appointment to monitor the profile of the organisation for equality, diversity and strategic purposes. This information is held anonymously and not linked to personal profiles. It is collated across the organisation by the Human Resources Department and will not be identifiable in relation to the storage of information or the analysis of the information.
- Personal data (e.g. address details, emergency contacts etc.) will be collected systematically and verified during the annual appraisal process.
- Data will not be taken into account once it is out of date and will be deleted in line with the relevant internal and external requirements.
- All data will be kept secure and access will be strictly controlled.
- Unauthorised disclosure of confidential employee data will be a disciplinary offence, all employees and volunteers are required to sign a confidentiality agreement which is held on their personnel file or volunteer record.
- Requests for addresses, earnings etc. will always be refused unless part of an official enquiry from the Department of Social Security, DfEE, or Child Support Agency or other legitimate Government body, unless you have specifically authorised the release of such information (for example to a mortgage provider).
- Information provided by you in the course of your employment will not be disclosed to third parties without your written consent unless the law requires disclosure without informing you.

The right to access (Subject Access Requests (Appendix 2)**)**

The right to access gives individuals the right to obtain conformation of their personal data held by the organisation, a copy of that information and other supplementary information such as the purpose of processing and retention periods for storing personal data.

A Subject Access Request should only relate to the individual submitting the request unless they are acting in a legal capacity or on behalf of someone else and have written permission to act on behalf of that individual.

Requests for information can be submitted verbally or in writing via a variety of channels:

- Via a Subject Access Request form (Appendix 3)
- Via email info@nottshospice.org
- Via phone 0115 910 1008
- Via letter to Nottinghamshire Hospice, 384 Woodborough Road, Nottingham, NG3 4JF

A record of requests will be logged by the Senior Information Risk Officer and a response provided to the individual within 30 days of receipt. Where the request is complex or numerous, the person submitting the request will be informed within 1 month of receipt, that the timeframe for response has been extended up to 3 months.

Nottinghamshire Hospice will uphold individual's rights to access their data without imposing any charge. Where requests are manifestly unfounded or excessive a reasonable fee will be charged.

Where there is strong justification to refuse to comply with a request, a detailed explanation supporting the decision will be provided to the individual within 1 month of receipt.

The right to rectification

Data subjects are entitled to have their data corrected or rectified if it is inaccurate

	or incomplete. If data has been disclosed to or received from a third party, they will be informed of the error or correction. The details of any third parties will also be supplied to the person making the request. The process will usually be complete within one month of receiving the request, where the request is complex this may be extended up to three months. If the decision is not to rectify the data, this will be conveyed with an explanation as to why this was not completed. **The right to erasure (the right to be forgotten)** The right to erasure is in place to ensure that a person or data subject is able to request the deletion of their personal data where there is no compelling reason for its continued processing. This will apply in the following circumstances: • The data is no longer necessary in relation to the purpose for which it was originally collected or processed. • The person has withdrawn consent • The person objects to the processing and there is no overriding legitimate interest for continuing to process the data • The personal data has to be erased in order to comply with a legal obligation • The data was unlawfully processed • The data relates to a child. In some instances it will not be possible to erase date these are: • Nottinghamshire Hospice is exercising the right of freedom of expression and information • It is held in line with compliance with a legal obligation • The information is being held for public health interest • The information is part of archived data in the public interest, for scientific research, historical research or for statistical purposes • The information may be required at some point to exercise or defend a legal claim.

If the information has been passed to a third party the Hospice will inform them that the data has been erased.

The right to restrict processing

The right to restrict processing means that a request has been received not to erase data or that it has been requested to be erased and that this is currently being verified and during this period processing will be restricted.

If the data has been shared with a third party they will be informed of the restriction. If following investigation the restriction is not required, we will inform the person concerned together with the reasons why.

The reasons we may restrict the processing of data are:

- An individual has contested the accuracy of the information that is held, the Hospice will not process data until an investigation has been completed
- An individual has objected to procession of their personal data but the Hospice believes it is necessary 'in the public interest' or for the furtherance of Nottinghamshire Hospice legitimate interest. During the period of investigation the data will not be processed
- Where processing is unlawful, an individual opposes erasure and want the data to be restricted instead
- An individual's data is no longer required but they require it to pursue a legal claim.

The right to data portability

All data at Nottinghamshire Hospice is stored in standard formats. Individuals have the right to have their data passed to them in a standard format. This format may be that required by another organisation. If data is stored differently by Nottinghamshire Hospice and an individual requires it to be presented in a standard format this will be provided to them free of charge usually within one month of us receiving the request. If the request relates to complex data this may take up to three months.

An individual have the right to request data portability if:

- They have provided us with their data
- Processing is based on their consent or for the performance of a contract
- Processing is being carried out by automated means

The right to object

An individual has the right to object to the processing of their data if this is based on:

- The Hospice believes that there are legitimate interests or for the performance of a task in the public interest
- Direct marketing, including profiling
- Processing for the purpose of scientific or historical research and statistics.

An individuals objection is based on grounds relating to their particular situation at that time. On receiving their request The Hospice will stop processing immediately unless it can demonstrate compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of an individuals rights or those of the Hospice or to make or defend a legal claim.

Rights in relation to automated decision making and profiling

The Hospice will safeguard the data it holds against the risk of potentially damaging decision making takes place without human intervention.

The Hospice ensures that all data collected is stored correctly and will ensure that an individual is able to:

- Speak to and gain human intervention
- Express their point of view
- Obtain an explanation of the decision and challenge it

	Unless for the following reasons: • It is necessary for entering into or for the performance of a contract • Is authorised by law • Is based on explicit consent Profiling is a form of automated processing that is intended to evaluate or to predict: • Performance at work • The economic situation • Health • Personal preferences • Reliability • Behaviour • Location • Movements. If the Hospice profiles data it will ensure that: • The process is fair and transparent and provide individuals with clear and meaningful information about the logic used • Individuals are aware of the consequences of the processing • Mathematical or statistical procedures are in place • Measures are in place so that any inaccuracies can be corrected • It secures the data in a way that is proportional to the value and sensitivity of the data. Automated decision making will not be used if: • Concerns a child • Is based on processing special categories of data unless an individual has given explicit consent or processing is necessary to comply with the law.

Basic principles

Nottinghamshire Hospice subscribes to the following basic principles in relation to GDPR:

- Transparency
- Accountability
- Fairness
- Ensuring the rights of data subjects are safeguarded
- Security of Information

Processing principles

All processing of personal data must comply with eight principles of good practice. These say that data must be:

- Processed fairly and lawfully
- Obtained and processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Kept for no longer than necessary
- Processed in accordance with the rights of data subjects
- Protected against unauthorised use and against accidental loss
- Not transferred outside the European Economic Area Union without adequate protection.

The Hospice will always inform individuals what routine processing they might expect and ask for consent to any unusual processing.

	Processing of Human Resources records will be carried out in relation to the following purposes: • recruitment • legally required vetting • taking up references • entering into a contract of employment • ensuring supervision is carried out • ensuring annual appraisal is carried out • in relation to employment policies such as leave, sickness, disciplinary • medical information to safeguard your health • ending employment • providing references Only Line Managers, Human Resources, relevant Head of Department or the Chief Executive Officer will be involved in regularly processing staff files. Information may be disclosed in the process of carrying out Human Resources' policies to the Chief Executive Officer. In addition to the guidelines, the following rules apply: • All Human Resources records will be kept for the duration of an employee's employment and according to the Information Commissioner's guidance on keeping records. • All staff and volunteers will be informed periodically of the descriptive information held on them (not the whole file). • There will be a right to amend this information if it is inaccurate.

	• Employees must inform Human Resources when their details change. • If legal advice is taken by an employer relating to a potential or actual legal claim by an employee, such personal data need not be disclosed to the employee. A former employee does not have the right to see a confidential reference made about them. However, they would be entitled to see a reference held by the person to whom it was supplied once they are in employment.
6.	**Data Protection Impact Assessment (DPIA)** A DPIA is required under the GDPR any time a new project is started that is likely to involve “a high risk” to other people’s personal information. The DPIA template should be completed by the project owner when scoping the project.
7.	**Confidentiality** Confidentiality is an important issue in all Nottinghamshire Hospice work, whether dealing with patients, colleagues, acting as a Line Manager or giving advice to other hospices. Except in the proper performance of their duties, staff are expected not to disclose confidential information belonging to Nottinghamshire Hospice to any person, company ororganisation, even after they have left Nottinghamshire Hospice. Confidentiality operates on a ‘need to know’ basis. Discussing confidential information with an appropriate colleague within the context of work for Nottinghamshire Hospice is not usually a breach of confidentiality. Discussing it with anyone else is likely to be a breach of confidentiality. If a member of staff causes anything marked confidential to become public knowledge, disciplinary action may be taken against them, including dismissal.

Confidential information

Information regarded as confidential may be written or verbal, ranging from telephone conversations to case files and membership records, employment and medical records. In some cases photographs, audio and video as well.

It includes, but is not limited to, the following:

- Details by which a person can be identified: name, address, telephone number
  etc.
- Information about individuals using the services of Nottinghamshire Hospice or a hospice.
- Information concerning the services offered or provided by Nottinghamshire Hospice including the names of people, companies or other organisations to which services are provided. Their requirements and terms on which services are provided to them. (This will cease to be confidential information if it is published in any prospectus or document available to members of the public).
- Nottinghamshire Hospice's marketing or fundraising strategies.
- Any information about any proposed re-organisation, expansion or contraction of Nottinghamshire Hospice services or any other development proposals.
- Financial information other than that available in audited accounts.
- Details of the employees of Nottinghamshire Hospice, their pay and benefits.
- Any information, which staff have been told is confidential, or which might reasonably expect to be confidential.
- Any information, which has been given to Nottinghamshire Hospice in confidence by members of other hospices, companies or organisations.
- All back up information, graphics, data, statistics, reports, computer programmes, designs and copyright information prepared for Nottinghamshire Hospice or obtained as a result of working for Nottinghamshire Hospice.

- All records, documents and other papers, including electronic records made or acquired by staff in the course of their work at Nottinghamshire Hospice are the property of Nottinghamshire Hospice and must be returned when you a member of staff leaves.

Confidentiality and security

Staff are expected to keep information regarding their work and the work of Nottinghamshire Hospice safe and secure (Appendix 4).

They are also expected to ensure that all confidential documents, papers, correspondence etc. including those held on home computer or laptop computers in transit are kept secure at all times, and are carefully secured at night, and that the published security procedures are maintained at all times. Information of this nature should not be kept in a car when staff are visiting Hospices, it should be taken inside the premises.

Staff must not remove such confidential information from Nottinghamshire Hospice premises except when this is essential to the proper performance of their duties. If they need to take information home regularly they must consult their Head of Department for detailed guidance about the protocols for doing so. If it is necessary to take information home on a one-off basis, permission must be received from the Line Manager first.

Any unauthorised conduct in this respect which causes loss or damage to Nottinghamshire Hospice or to any member of staff (past, present or future) may result in disciplinary action being taken, including dismissal.

Access to confidential information will be restricted through passwords on computer systems and lockable cabinets for files and on a “need to know” basis.

A specified individual will have overall responsibility for access to a particular set of records.

Staff will have their own passwords which must not be disclosed to anyone. Employees who are responsible for keys should not pass them to unauthorised individuals.

Disclosure of information

Journalists, researchers, companies and other interested individuals will not be given information on, or access to, any individual unless the individual concerned has given their consent.

Where information is supplied by third parties, the confidentiality code of the third party must be taken into account.

Disclosure of confidential information may occasionally be necessary, but this should not take place unless judged to be absolutely essential and in the interest of the person concerned. Decisions of this nature can only be authorised by the Chief Executive or Data Protection Officer (Director of Finance and Resources).

In these cases the bona fides of people or organisations requesting the information must be secured prior to giving any information, written or verbal.

Public interest disclosure – Whistleblowing (Whistleblowing Policy OP008**)**

Nottinghamshire Hospice is committed to ethical and equal opportunity organisational and managerial practices and will respond to failures to maintain quality standards very seriously.

This procedure is designed to ensure Nottinghamshire Hospice meet the provisions of the Public Interest Disclosure Act 1998. Broadly the provisions of the Act are to provide protection from dismissal, or a detriment short of dismissal, to employees who in good faith "blow the whistle" on certain specified activities within their organisation. The Act outlines the procedures an organisation should have in place to enable employees to make such a disclosure.

The purpose of this procedure is to outline the steps that should be taken by a worker who genuinely and in good faith believes that one of the following sets of circumstances is occurring, has occurred or may occur within Nottinghamshire Hospice.

- A criminal offence has been committed, is being committed or is likely to be committed.

- A person has failed, is failing or is likely to fail to comply with any legal obligation to which he or she is subject.
- A miscarriage of justice has occurred, is occurring or is likely to occur.
- The health and safety of any individual has been, is being or is likely to be endangered.
- The environment has been, is being or is likely to be damaged.

Information tending to show any matter falling within any one of the preceding

paragraphs has been, is being or is likely to be deliberately concealed.

However, that staff will not be protected from the consequences of making such

a disclosure if, by doing so, they commit a criminal offence.

If staff believe that an action has taken place that falls into one of the above categories, then they must notify their Line Manager immediately. If the allegation involves the Line Manager, then they should raise the matter with the Chief Executive.

If the Manager first approached fails to deal with the matter, staff should go to the next level up in the management structure as far as the Chair of Trustees. If this fails to secure effective action or in extreme circumstances the employee should report matters to an outside body. For example where it is a case of health and safety, to the Health and Safety Executive, or the Charity Commissioners.

If it is reasonably believed that the relevant failure (i.e. one of the set of circumstances listed above) relates wholly or mainly to the conduct of a person other than the employer or any other matter for which a person other than Nottinghamshire Hospice has legal responsibility, then that disclosure should be made to that other person.

The policy will apply where a disclosure is in good faith and where it is reasonably believed that the information disclosed, and any allegation contained in it are substantially true. If any disclosure is made in bad faith (for instance, in order to cause disruption within Nottinghamshire Hospice), or concerns information which are not substantially believed to be true, or indeed if the disclosure is made for

	personal gain, then such a disclosure will constitute a disciplinary offence for the purposes of Nottinghamshire Hospice' Disciplinary Policy and Procedure HR024 and may constitute gross misconduct for which summary dismissal is the sanction. **Copyright** Whilst employed by Nottinghamshire Hospice, every piece of work created by a staff member and arising out of, or as a consequence of, their employment shall be deemed to have been made on behalf of Nottinghamshire Hospice. This includes improvements, inventions, writing or designs or concepts, whether or not registered and/or registerable. It also includes any benefits that arise from work, and those benefits will belong exclusively to Nottinghamshire Hospice. Staff must tell your Line Manager if they think they are creating anything that ought to be protected by copyright so that Nottinghamshire Hospice can ensure it receives the full benefits. If requested to by Nottinghamshire Hospice, either while employed by it or afterwards, staff must provide help to substantiate any rights the Hospice may have over the work they did whilst working for the Hospice. The Hospice will pay any costs involved in providing such help.
8.	**Personnel Security** **Contracts of employment** Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a security and confidentiality clause. References for new staff shall be verified and a passport, driving license or other document shall be provided to confirm identity. Information security expectations of staff shall be included within appropriate job definitions. Whenever a staff member leaves the company, their accounts will be disabled the same day they leave.

	Information security awareness and training The aim of the training and awareness programmes are to ensure that the risks presented to information by staff errors and by bad practice are reduced. Information security awareness training shall be included in the staff induction process and shall be carried out annually for all staff. This is in the form of the GDPR training available on Blue Stream Academy. An on-going awareness programme shall be established and maintained in order to ensure that staff awareness of information security is maintained and updated as necessary. This includes regular discussions about information security at Corporate Management Team meetings. **Intellectual property rights** The organisation shall ensure that all software is properly licensed and approved as suitable by the IT contractor and the Director of Finance and Resources. Individual and Nottinghamshire Hospice intellectual property rights shall be protected at all times. Users breaching this requirement may be subject to disciplinary action.
9.	**Access Management** **Physical access** Only authorised personnel who have a valid and approved business need shall be given access to areas containing information systems or stored data. **Identity and passwords** Passwords must offer an adequate level of security to protect systems and data All passwords shall be eight characters or longer and contain at least two of the following: uppercase letters, lowercase letters and numbers All administrator-level passwords shall be changed at least every 60 days Where available, two-factor authentication shall be used to provide additional

	security. This is in place on the 365 portal for IT supplier administration access. All users shall use uniquely named user accounts Generic user accounts that are used by more than one person or service shall not be used, with the exception of the below accounts. • Maintenance assistant log on using maintenance@nottshopsice.org • Care Service Care Co-ordination info@nottshospice.org • Training laptops which have no access to the network, use hospicenow\training to log on **User access** Access to information shall be based on the principle of "least privilege" and restricted to authorised users who have a business need to access the information. Access to departmental information is controlled by access being approved on an individual basis by the line manager and/or the Director of Finance & Resources. **Administrator-level access** Administrator-level access shall only be provided to individuals with a business need who have been authorised by the Chief Executive. A list of individuals with administrator-level access shall be held by the IT contractor and Senior Management and shall be reviewed every 6 months. Administrator-level accounts shall not be used for day-to-day activity. Such accounts shall only be used for specific tasks requiring administrator privileges. This access can be requested by contacting the IT contractor and seeking approval from the Chief Executive. **Application access** Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g., systems or database administrators. Access is listed on the Information Asset Register.

Authorisation to use an application shall depend on a current license from the supplier.

Hardware access

Where indicated by a risk assessment, access to the network shall be restricted to authorised devices only

System perimeter access (firewalls)

The boundary between business systems and the Internet shall be protected by firewalls, which shall be configured to meet the threat and continuously monitored.

All servers, computers, laptops, mobile phones and tablets shall have a firewall enabled, if such a firewall is available and accessible to the device's operating system.

The default password on all firewalls shall be changed to a new password that complies to the password requirements in this policy, and shall be changed regularly

All firewalls shall be configured to block all incoming connections.

If a port is required to be opened for a valid business reason, the change shall be authorised following the system change control process. The port shall be closed when there is no longer a business reason for it to remain open.

Monitoring system access and use

An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed on a regular basis.

Regular audits of software will be completed by the IT provider (at least monthly)

Where software has been found to be incorrectly downloaded which does not meet Appendix 1 – Approved Applications List, this will be removed immediately by the IT provider.

The business reserves the right to monitor systems or communications activity

	where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).
10.	**Reporting a Data Breach (For the organisation not individual)** The General Data Protection Regulations 2018 requires all data breaches to be reported promptly and in a timely way. If you create or observe a breach of personal data you should inform your Line Manager and the Chief Executive immediately who will assess the situation and be responsible for reporting the breach to the Information Commissioners Office. A Data Breach Response Plan will be put in place which will include the notification of all other parties beginning with the person about whom the breach refers. Where the breach is not a risk to an individual's rights or freedoms the actions will relate primarily to an internal response. The report to the ICO will include but not be limited to: • A full explanation of the incident • Details about the number of people and records involved • The categories of personal data involved • Name of the key person within the organisation responsible for responding to the breach • Description of the likely consequences of the breach • A description of how you intend to deal with the breach Contact details for the Information Commissioners Office are: https://ico.org.uk/for-organisations/report-a-breach Telephone: 030123 1113
11.	**Data Retention and Disposal** **Data retention** As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which

that data is collected, held, and processed.

Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed) (Appendix 5).

When establishing and/or reviewing retention periods, the following shall be taken into account:

- The objectives and requirements of the Company
- The type of personal data in question
- The purpose(s) for which the data in question is collected, held, and processed
- The Company's legal basis for collecting, holding, and processing that data
- The category or categories of data subject to whom the data relates.

If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

Archiving

Paper records archived in line within the retention requirements (Appendix 6) will

	be kept on the Hospice site at Woodborough Road. These will be held in locked cabinets within a locked room and access restricted. **Data disposal** Upon the expiry of the data retention periods set out below in appendix 1 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows: • All Personal data stored electronically (including any and all backups thereof) shall be deleted • All Personal data stored in hardcopy form shall be shredded and recycled
12.	**Asset Management** **Asset ownership** Each information asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset. **Asset records and management** An accurate record of business information assets, including source, ownership, modification and disposal shall be maintained via the Nottinghamshire Hospice Device and Application List. All disposal certificates will be saved in this location; N:\Building and Transport\IT\IT equipment disposal certificates All data shall be securely wiped from all hardware before disposal. For computer drives and external disks, this should only be completed by the IT provider. **Asset handling** Nottinghamshire Hospice shall identify particularly valuable or sensitive information assets through the use of data classification.

All sensitive data will be secured with password protection before sending internally and externally.

Care Services must use SystmOne for the transfer of patient data or an nhs.email account.

Where this data is shared externally with third party suppliers, the privacy statement will be reviewed, and a data sharing contract put in place by the Director of Finance & Resources.

All staff are responsible for handling information assets in accordance with this security policy. Where possible the data classification shall be marked upon the asset itself.

All company information shall be categorised into one of the three categories in the table (Table 1) below based on the description and examples provided.

Table 1. Types of Company Information

Category	Description	Example
Public	Information which is not confidential and can be made available publicly through any channels.	• Details of products and services on the website • Published Hospice information • Social media updates • Press releases
Amber Information	Information which, if lost or made available to unauthorised persons could impact the company's effectiveness, benefit competitors or cause embarrassment to the organisation and/or its partners	• Company operating procedures and policy • Client contact details • Hospice plans and financial information • Basic employee information including personal data
Red Information	Information which, if lost or made available to unauthorised persons, could cause severe impact on the company's ability to operate or cause significant reputational damage and distress to the organisation and/or its partners. This information requires the highest levels of protection of confidentiality, integrity and availability.	• Client intellectual property • Data in e-commerce systems • Employee salary details • Any information defined as "sensitive personal data" under the Data Protection Act

Removable media

Only company provided removable media (such as USB memory sticks and recordable CDs/DVDs) shall be used to store business data and its use shall be recorded (e.g., serial number, date, issued to, returned).

Removable media of all types that contain software or data from external sources, or that has been used on external equipment, must be used on the basic Training profile, not attached to the network via Wi-Fi or ethernet cable. This can be achieved by signing in as Training on any of the designated Training laptops. This media will then be scanned using Anti-Virus software.

Where indicated by the risk assessment, systems shall be prevented from using removable media.

Users breaching these requirements may be subject to disciplinary action.

Mobile working

Where necessary, staff may use company-supplied mobile devices such as phones, tablets and laptops to meet their job role requirements

Use of mobile devices for business purposes (whether business-owned or personal devices) requires the approval of the Director of Finance & Resources.

Such devices must have anti-malware software installed (if available for the device), must have a PIN, password or other authentication configured, must be encrypted (if available for the device) and be capable of being remotely wiped. They must also comply with the software management requirements within this policy.

Users must inform the Director of Finance & Resources immediately if the device is lost or stolen and business information must then be remotely wiped from the device.

Personal devices / Bring Your Own Device (BYOD)

Where necessary, staff may use personal mobile phones to access business

	email. This usage must be authorised by the Director of Finance & Resources. The device must be registered in the asset records and must be configured to comply with the mobile working section and other relevant sections of this policy, including having the correct malware and anti-virus installed. No other personal devices are to be used to access business information **Social media** Social media may only be used for business purposes by using official business social media accounts with authorisation from the Director of Finance & Resources. Users of business social media accounts shall be appropriately trained and be aware of the risks of sharing sensitive information via social media. Business social media accounts shall be protected by strong passwords in-line with the password requirements for administrator accounts. Users shall behave responsibly while using any social media whether for business or personal use, bearing in mind that they directly or indirectly represent the company. If in doubt, consult the Director of Finance & Resources and/or the Chief Executive. **Users breaching this requirement may be subject to disciplinary action.**
13.	**Security of Records** The following organisational measures are in place within the Hospice to protect the security of personal data: • All employees and other parties working on behalf of the Hospice shall be made fully aware of both their individual responsibilities and the Hospice's responsibilities under this Policy • Only employees and other parties working on behalf of the Hospice that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Hospice • All employees and other parties working on behalf of the Hospice handling

	personal data will be appropriately trained to do so • All employees and other parties working on behalf of the Hospice handling personal data will be appropriately supervised • All employees and other parties working on behalf of the Hospice handling personal data should exercise care and caution when discussing any work relating to personal data at all times • Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed • The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed • All employees and other parties working on behalf of the Hospice handling personal data will be bound by contract to comply with this Policy • All agents, contractors, or other parties working on behalf of the Hospice handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Hospice arising out of this Policy • Where any agent, contractor or other party working on behalf of the Hospice handling personal data fails in their obligations under this Policy, that party shall indemnify and hold harmless the Hospice against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure. Nottinghamshire Hospice will take all possible steps to: • Have a back-up system and use it with rigor and discipline • Protect irreplaceable documents from fire • Ensure unauthorised users can't hack into the secure files, either within the intranet or from outside

- Check the backup process really works

All staff and volunteers must be responsible for:

- Keeping to security protocols
- Not taking irreplaceable documents out of the building
- Ensuring that old copies of data are disposed of securely
- Where appropriate sensitive documents and Human Resources' data will be shredded
- Ensuring all backup systems disks, tapes CDs etc. really are deleted when out of date

Nottinghamshire Hospice is committed to ensuring the security of data we have under our control as far as humanly possible.

This means that we will:

- Ensure people should only see data that they are authorised to see
- Prevent data getting lost, damaged or destroyed
- Ensure that 'old' copies of data are disposed of securely
- Ensure people should only see data that they are authorised to see
- The security of employees' files is the responsibility of Human Resources. They are responsible for being clear about who can access which file legitimately. They should release the relevant section of the file – e.g. supervision notes or personal details only - not the whole file - to any one person
- Line Managers will be responsible for maintaining security of data and being clear about who is entitled to see what
- Employees' files will all be kept in a locked cabinet by Human Resources

- Line Managers should not keep their own Human Resources' information in their own filing systems.
- Anyone wishing to access a file must not take the whole file but must take relevant information only. They can check data on the file, but not alter it without permission of the data subject
- Personal data must never be left out on an unattended desk
- People accessing their own files have to do so in a supervised way - i.e. not left alone with them
- If personal data is able to be brought up on screen, this should not be able to be viewed by a third party
- Personal data must never be left up on screen whilst the user walks off for however short a time period
- Personal information should only be sent via fax or email when the data will be received and held securely by the recipient. A phone call MUST be made to the recipient prior to sending such information. A written agreement must be signed by the recipient to state that the information will be stored securely and treated as confidential

Physical and environmental management

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. Physical security accreditation should be applied if necessary.

Systems shall be protected from power loss by UPS if indicated by the risk assessment.

Systems requiring particular environmental operating conditions shall be maintained within optimum requirements.

14.	**Computer and Network Management** **Operations management** Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Director of Finance & Resources and the Chief Executive. **System change control** Changes to information systems, applications or networks shall be reviewed and approved by the Director of Finance & Resources with the IT provider. **Accreditation** The organisation shall ensure that all new and modified information systems, applications and networks include security provisions. They must be correctly sized, identify the security requirements, be compatible with existing systems according to an established systems architecture (as required) and be approved by the Director of Finance & Resources before they commence operation. **Software Management** All application software, operating systems and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities. All software security updates/patches shall be installed within 7 days of their release. Only software which has a valid business reason for its use shall be installed on devices used for business purposes. See Appendix A for an approved list of Software. Users shall not install software or other active code on the devices containing business information without permission from the Director of Finance & Resources and gaining administration access by the IT provider.

For the avoidance of doubt, all unnecessary and unused application software shall be removed from any devices used for business purposes by the IT provider.

Local data storage

Data stored on the business premises shall be backed up regularly and restores tested at appropriate intervals (at least monthly).

A backup copy shall be held in a different physical location to the business premises. This is an offsite at the IT provider.

Backup copies of data shall be protected and comply with the requirements of this security policy and be afforded the same level of protection as live data.

External cloud services

Where data storage, applications or other services are provided by another business (e.g., a 'cloud provider') there must be independently audited, written confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this policy.

Protection from malicious software

The business shall use software countermeasures, including anti-malware, and management procedures to protect itself against the threat of malicious software.

All computers, servers, laptops, mobile phones and tablets shall have anti-malware software installed, where such anti-malware is available for the device's operating system.

All anti-malware software shall be set to:

- scan files and data on the device on a daily basis
- scan files on-access
- automatically check for, and install, virus definitions and updates to the software itself on a daily basis
- block access to malicious websites

	Vulnerability scanning The business shall have a yearly vulnerability scan of all external IP addresses carried out by a suitable external company The business shall act on the recommendations of the external company following the vulnerability scan in order to reduce the security risk presented by any significant vulnerabilities The results of the scan and any changes made shall be reflected in the company risk assessment and security policy as appropriate. **Penetration test** The business may choose to complete a penetration test and scan of all external IP addresses carried out by a suitable external company.
15.	**Information Security Incidents** All breaches of this policy and all other information security incidents shall be reported to the Chief Executive. If required as a result of an incident, data will be isolated to facilitate forensic examination. This decision shall be made by the Chief Executive. Information security incidents shall be recorded in the Security Incident Log as part of the Incident reporting system, an incident form completed on Vantage with identifying number and investigated by the Director of Finance & Resources and/or the Chief Executive to establish their cause and impact with a view to avoiding similar events. The risk assessment and this policy shall be updated if required to reduce the risk of a similar incident re-occurring. The incident response process will be tested annually as a minimum. **Business Continuity and Disaster Recovery Plans** The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical

	information, applications, systems and networks. **Reporting** The Information Security Officer shall keep the business informed of the information security status of the organisation by means of regular reports to senior management.
16.	**Legislation** Nottinghamshire Hospice is required to abide by certain UK, European Union and international legislation. It also may be required to comply to certain industry rules and regulations. The requirement to comply with legislation shall be devolved to employees, volunteers and agents of the Nottinghamshire Hospice, who may be held personally accountable for any breaches of information security for which they are responsible. In particular, Nottinghamshire Hospice is required to comply with: • The Data Protection Act (2018) • The Data Protection (Processing of Sensitive Personal Data) Order 2000 • The Copyright, Designs and Patents Act (1988) • The Computer Misuse Act (1990) • The Health and Safety at Work Act (1974) • Human Rights Act (1998) • Regulation of Investigatory Powers Act (2000) • Freedom of Information Act (2000) • NHS Data Security and Protection Toolkit – annual compliance review • PCI DSS Security Standards
17.	**Equality Impact Assessment (EIA)** An EIA has been completed.

Nottinghamshire Hospice Approved Applications List

Software Licence Report: ILUX Limited

Date generated: 22 Mar 2024 04:33 pm

Client: Nottinghamshire Hospice

All Software	Installed Count
64 Bit HP CIO Components Installer	8
7-Zip 23.01 (x64)	3
Action1 Connector	1
Active Protection System	1
adobe acrobat	4
Adobe Acrobat (64-bit)	36
Adobe Acrobat DC	2
Adobe Acrobat Reader	23
Adobe Acrobat Reader DC	3
Adobe After Effects 2023	1
Adobe After Effects 2024	1
Adobe AIR	1
Adobe Bridge 2021	1
Adobe Bridge 2022	1
Adobe Bridge 2023	1
Adobe Bridge 2024	1
Adobe Creative Cloud	7
Adobe Genuine Service	7
Adobe Illustrator 2024	1
Adobe InDesign 2021	2
Adobe InDesign 2023	1
Adobe InDesign 2024	1
Adobe Lightroom	1
Adobe Media Encoder 2021	2
Adobe Media Encoder 2023	2
Adobe Media Encoder 2024	1
Adobe Photoshop 2024	1
Adobe Premiere Pro 2021	2
Adobe Premiere Pro 2023	2
Adobe Premiere Pro 2024	1
Adobe Premiere Rush	1
Adobe Refresh Manager	62
Advanced IP Scanner 2.5	2
Advanced IP Scanner 2.5.1	2
Advanced Monitoring Agent	68
Agent	4
Ai Meeting Manager Service	1
Apple Mobile Device Support	1
Apple Software Update	1
Asian Language And Spelling Dictionaries Support For Adobe Acrobat Reader	2
AWS Plug-In for Veeam Backup & Replication	1
AWS Plug-in UI Extension for Veeam Backup & Replication	1
Azure Data Studio	1
Backup Manager	2
Bing Bar	1
Bing Wallpaper	1
Bonjour	2
Browser for SQL Server 2017	1

Browser for SQL Server 2019	1
Capture	1
CCleaner	1
ClaroIdeas	1
ClaroRead	1
ClaroView, ScreenRuler and ScreenMarker	1
Classic Client 6.3.12 for 64 bits	4
Classic Client 6.4.3 for 64 bits	1
Classic Client 6.5.0 for 64 bits	1
Conexant ISST Audio	1
CPUID HWMonitor 1.46	1
CreativeCloudDesktopApp	2
CreativeCloudDesktopApp_x64	3
Crystal Reports XI Runtime	1
CSY Vector 7.57 built 03/05/18	1
CSY Vector 7.59 built 03/08/21	1
CSY Vector 7.59 built 21/06/22	2
CSY Vector 7.60 built 04/07/2023	1
CutePDF Writer	1
CutePDF Writer 3.2	3
DataFlex 2017 Windows Client 19.0	26
DataFlex 2019 Client 19.1	6
DefaultPackMSI	11
Dell Command | Update	2
Dell Digital Delivery	1
Dell SupportAssist	8
Dell SupportAssist OS Recovery Plugin for Dell Update	7
Dell Touchpad	2
Dell WLAN Radio Switch Driver	1
DFUDriverSetupX64Setup	1
DisplayLink Graphics	1
DisplayLink Graphics Driver	1
Documentation Manager	1
donorflex	32
donorflex10.2	21
donorflex11.2	25
donorflex_Outlook_plugin	21
Dragon	1
DrayTek Smart VPN Client	16
Dropbox	1
Dropbox Update Helper	1
DSC/AA Factory Installer	3
Dynamic Application Loader Host Interface Service	6
Eclipse Temurin JDK with Hotspot 17.0.9+9 (x64)	1
Eclipse Temurin JRE with Hotspot 11.0.20.1+1 (x64)	1
Epson Connect Printer Setup	1
EPSON Event Manager	2
EPSON L3150 Series Printer Uninstall	1
EPSON Manuals	1
Epson Printer Connection Checker	1
Epson Scan 2	2
Epson ScanSmart	1
EPSON Software Updater	1
EPSON SX535WD Series Printer Uninstall	1
EPSON Universal Print Driver Printer Uninstall	1
EPSON XP-312 313 315 Series Printer Uninstall	1
EpsonNet Print	1
ESET Endpoint Antivirus	1

eSigner	2
eSigner 6.x Corp	3
eSigner 6.x Corp 64 bits	3
eSigner 64 bits	2
eSigner Corp	1
eSigner Corp 64 bits	1
eSigner6x Preinstall	5
ExamShield	1
ExpressBiosUpdate	4
Firebird 2.5.8.27089 (x64)	1
Firebird 2.5.9.27139 (x64)	4
Foxit PDF Editor	5
Foxit PDF Reader	1
GDR 2037 for SQL Server 2017 (KB4583456) (64-bit)	1
GDR 2042 for SQL Server 2017 (KB5014354) (64-bit)	1
GDR 2047 for SQL Server 2017 (KB5021127) (64-bit)	1
GDR 2052 for SQL Server 2017 (KB5029375) (64-bit)	1
GDR 6164 for SQL Server 2014 (KB4583463) (64-bit)	1
GDR 6169 for SQL Server 2014 (KB5014165) (64-bit)	1
GDR 6174 for SQL Server 2014 (KB5021037) (64-bit)	1
Gemalto Bluetooth Device Manager	6
GemPcCCID	3
Google Chrome	67
Google Cloud Platform Plug-In for Veeam Backup & Replication	1
Google Cloud Platform Plug-In UI extension for Veeam Backup & Replication	1
Google Drive	3
Google Update Helper	1
GoTo Opener	11
GoToAssist Customer 4.8.0.1692	1
Grammarly for Microsoft? Office Suite	1
HP 3D DriveGuard	1
HP ESU for Microsoft Windows 10	1
HP HotKey Support	1
HP MAC Address Manager	1
HP Officejet Pro 8100 Basic Device Software	3
HP Officejet Pro 8100 Help	1
HP Officejet Pro 8100 Product Improvement Study	1
HP Officejet Pro 8600 Basic Device Software	1
HP Recovery Manager	1
HP Registration Service	1
HP System Default Settings	1
HP Update	1
iCloud Outlook	1
IDGo SafeNet Minidriver 64b	2
IIS 8.0 Express	2
IIS Express Application Compatibility Database for x64	2
IIS Express Application Compatibility Database for x86	2
iMyFone LockWiper 7.5.1.5	1
Indesign	1
Integration Services	2
Intel Driver && Support Assistant	2
Intel(R) C++ Redistributables on Intel(R) 64	1
Intel(R) Chipset Device Software	13
Intel(R) Computing Improvement Program	4
Intel(R) Dynamic Platform and Thermal Framework	4
Intel(R) Icls	6
Intel(R) LMS	6
Intel(R) Management Engine Components	10

Intel(R) Management Engine Driver	10
Intel(R) ME UninstallLegacy	4
Intel(R) Network Connections	5
Intel(R) Network Connections 23.5.2.0	4
Intel(R) Network Connections 24.1.0.6	1
Intel(R) OEM Extension	6
Intel(R) PRO/Wireless Driver	1
Intel(R) Processor Graphics	15
Intel(R) Rapid Storage Technology	3
Intel(R) Serial IO	8
Intel(R) Trusted Connect Service Client x64	4
Intel(R) Trusted Connect Service Client x86	4
Intel(R) Trusted Connect Services Client	4
Intel(R) Wireless Bluetooth(R)	5
Intel? Driver & Support Assistant	2
Intel? Optane? Pinning Explorer Extensions	17
Intel? PROSet/Wireless Software	2
Intel? PROSet/Wireless WiFi Software	2
Intel? Software Installer	1
iTunes	1
Jabra Direct	1
Java 8 Update 351 (64-bit)	1
Java 8 Update 381 (64-bit)	1
Java Auto Updater	2
KONICA MINOLTA C759_C658_C368_C287_C3851Series	2
KONICA MINOLTA Universal V4 PCL	3
Lansweeper	2
Lenovo Active Protection System	1
Lenovo Calliope USB Keyboard	1
Lenovo Essential Wireless Keyboard	1
Lenovo Smart Appearance Components	2
Lenovo System Update	8
Lenovo USB Audio	1
Lenovo Vantage Service	30
Lenovo Welcome	2
LHITS Tools	1
Magic Bullet Suite	1
MatchWare MindView 7.0	1
Maxon Cinema 4D 2023	1
Maxon Cinema 4D 2024	1
Maxx Audio Installer (x64)	4
MediaEncoder	2
Microsoft .NET Core Host - 3.1.32 (x64)	1
Microsoft .NET Core Host FX Resolver - 3.1.32 (x64)	1
Microsoft .NET Core Runtime - 3.1.32 (x64)	1
Microsoft .NET Host - 6.0.20 (x64)	1
Microsoft .NET Host - 6.0.21 (x64)	1
Microsoft .NET Host - 6.0.27 (x64)	1
Microsoft .NET Host - 6.0.28 (x64)	4
Microsoft .NET Host FX Resolver - 6.0.20 (x64)	1
Microsoft .NET Host FX Resolver - 6.0.21 (x64)	1
Microsoft .NET Host FX Resolver - 6.0.26 (x64)	1
Microsoft .NET Host FX Resolver - 6.0.27 (x64)	1
Microsoft .NET Host FX Resolver - 6.0.28 (x64)	5
Microsoft .NET Runtime - 6.0.20 (x64)	1
Microsoft .NET Runtime - 6.0.21 (x64)	1
Microsoft .NET Runtime - 6.0.26 (x64)	1
Microsoft .NET Runtime - 6.0.27 (x64)	1

Microsoft .NET Runtime - 6.0.28 (x64)	5
Microsoft 365 - en-us	11
Microsoft 365 Apps for business - en-gb	2
Microsoft 365 Apps for business - en-us	59
Microsoft 365 Apps for enterprise - en-us	5
Microsoft Analysis Services OLE DB Provider	2
Microsoft ASP.NET Core 3.1.32 - Shared Framework (x64)	1
Microsoft ASP.NET Core 3.1.32 Shared Framework (x64)	1
Microsoft Azure Plug-In for Veeam Backup & Replication	1
Microsoft Azure Plug-in UI Extension for Veeam Backup & Replication	1
Microsoft Bing Service	1
Microsoft Edge	65
Microsoft Edge Update	66
Microsoft Edge WebView2 Runtime	66
Microsoft Help Viewer 2.3	2
Microsoft ODBC Driver 11 for SQL Server	28
Microsoft ODBC Driver 13 for SQL Server	1
Microsoft ODBC Driver 17 for SQL Server	3
Microsoft Office Access MUI (English) 2010	2
Microsoft Office Access Setup Metadata MUI (English) 2010	2
Microsoft Office Excel MUI (English) 2010	2
Microsoft Office Groove MUI (English) 2010	2
Microsoft Office InfoPath MUI (English) 2010	2
Microsoft Office Office 64-bit Components 2010	2
Microsoft Office OneNote MUI (English) 2010	2
Microsoft Office Outlook MUI (English) 2010	2
Microsoft Office PowerPoint MUI (English) 2010	2
Microsoft Office Professional Plus 2010	3
Microsoft Office Proof (English) 2010	2
Microsoft Office Proof (French) 2010	2
Microsoft Office Proof (Spanish) 2010	2
Microsoft Office Proofing (English) 2010	2
Microsoft Office Publisher MUI (English) 2010	2
Microsoft Office Shared 64-bit MUI (English) 2010	2
Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2010	2
Microsoft Office Shared MUI (English) 2010	2
Microsoft Office Shared Setup Metadata MUI (English) 2010	2
Microsoft Office Word MUI (English) 2010	2
Microsoft OLE DB Driver for SQL Server	2
Microsoft OneDrive	61
Microsoft OneNote - en-us	8
Microsoft Report Viewer 2015 Runtime	1
Microsoft Search in Bing	10
Microsoft Silverlight	9
Microsoft SQL Server 2008 Setup Support Files	1
Microsoft SQL Server 2012 (64-bit)	1
Microsoft SQL Server 2012 Native Client	2
Microsoft SQL Server 2012 RsFx Driver	1
Microsoft SQL Server 2012 Setup (English)	1
Microsoft SQL Server 2012 Transact-SQL ScriptDom	1
Microsoft SQL Server 2014 Express LocalDB	2
Microsoft SQL Server 2014 Management Objects (x64)	1
Microsoft SQL Server 2014 Transact-SQL ScriptDom	1
Microsoft SQL Server 2017 (64-bit)	1
Microsoft SQL Server 2017 RsFx Driver	1
Microsoft SQL Server 2017 Setup (English)	1
Microsoft SQL Server 2017 T-SQL Language Service	1
Microsoft SQL Server 2019 (64-bit)	1

Microsoft SQL Server 2019 RsFx Driver	1
Microsoft SQL Server 2019 Setup (English)	1
Microsoft SQL Server 2019 T-SQL Language Service	1
Microsoft SQL Server Management Studio - 18.6	1
Microsoft SQL Server Management Studio - 19.1	1
Microsoft System CLR Types for SQL Server 2014 (x64)	1
Microsoft Teams Meeting Add-in for Microsoft Office	49
Microsoft Update Health Tools	63
Microsoft VC++ redistributables repacked.	10
Microsoft Visual C++ 2005 Redistributable	13
Microsoft Visual C++ 2005 Redistributable (x64)	1
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729	1
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	5
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	5
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	20
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	26
Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.61030	10
Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.61030	10
Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030	10
Microsoft Visual C++ 2012 x64 Minimum Runtime - 11.0.61030	10
Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030	10
Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030	10
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.21005	3
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501	4
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.40664	8
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.21005	3
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501	11
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.40649	46
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.40664	8
Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005	7
Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.40664	8
Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005	7
Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.40664	8
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005	14
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.40649	46
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.40664	8
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005	14
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.40649	46
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.40664	8
Microsoft Visual C++ 2015 Redistributable (x64) - 14.0.23026	2
Microsoft Visual C++ 2015 Redistributable (x64) - 14.0.24215	2
Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.23026	1
Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.24212	3
Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.24215	2
Microsoft Visual C++ 2015 x64 Additional Runtime - 14.0.23026	2
Microsoft Visual C++ 2015 x64 Additional Runtime - 14.0.24215	2
Microsoft Visual C++ 2015 x64 Minimum Runtime - 14.0.23026	2
Microsoft Visual C++ 2015 x64 Minimum Runtime - 14.0.24215	2
Microsoft Visual C++ 2015 x86 Additional Runtime - 14.0.23026	1
Microsoft Visual C++ 2015 x86 Additional Runtime - 14.0.24212	3
Microsoft Visual C++ 2015 x86 Additional Runtime - 14.0.24215	2
Microsoft Visual C++ 2015 x86 Minimum Runtime - 14.0.23026	1
Microsoft Visual C++ 2015 x86 Minimum Runtime - 14.0.24212	3
Microsoft Visual C++ 2015 x86 Minimum Runtime - 14.0.24215	2
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.21.27702	1
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.23.27820	3
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.26.28720	4
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.27.29112	2

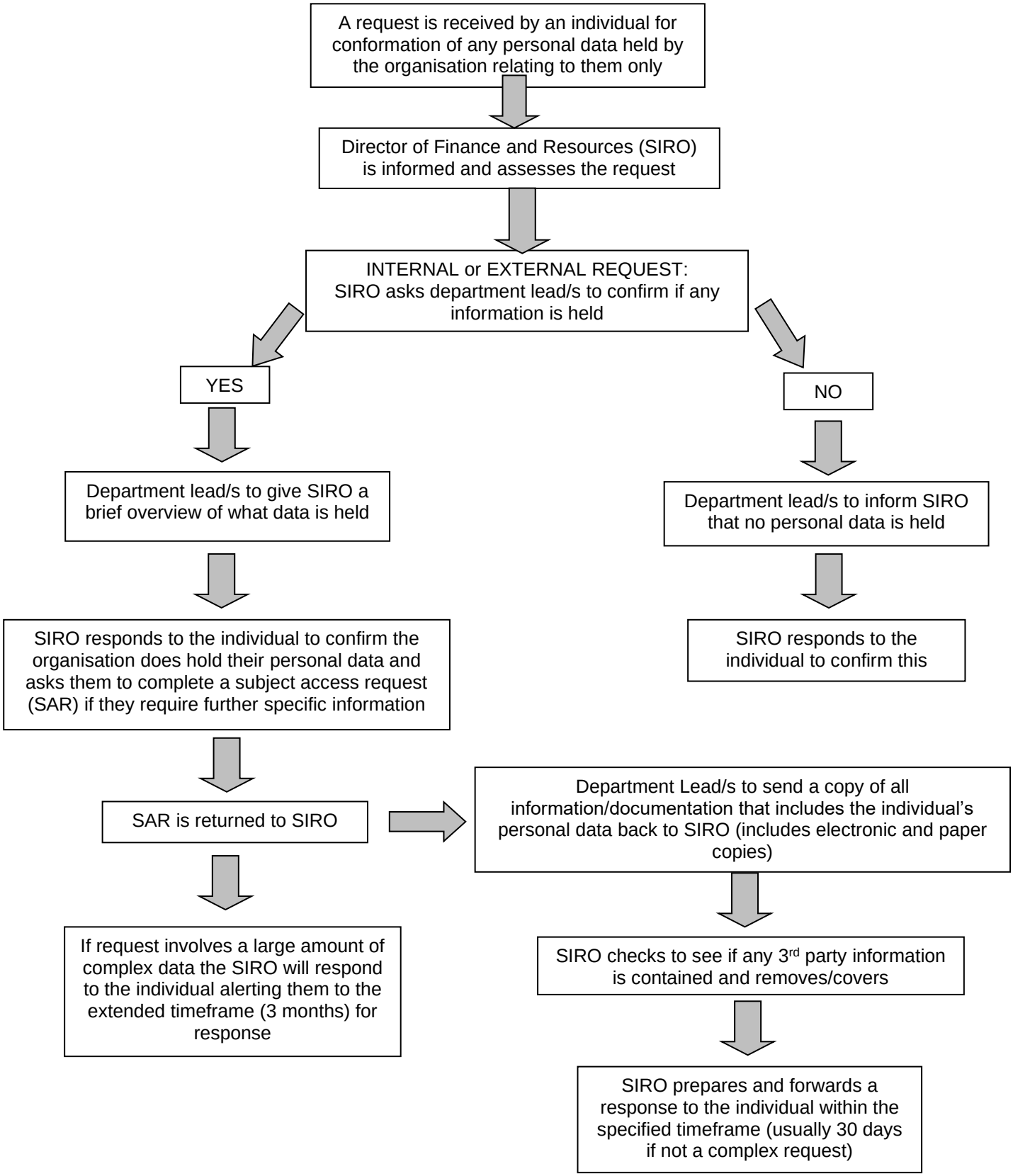
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702	1
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.23.27820	2
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.29.30133	2
Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.32.31326	6
Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.32.31332	7
Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.32.31326	6
Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.32.31332	10
Microsoft Visual C++ 2017 Redistributable (x64) - 14.10.25017	4
Microsoft Visual C++ 2017 Redistributable (x86) - 14.10.25017	4
Microsoft Visual C++ 2017 x64 Additional Runtime - 14.10.25017	4
Microsoft Visual C++ 2017 x64 Minimum Runtime - 14.10.25017	4
Microsoft Visual C++ 2017 x86 Additional Runtime - 14.10.25017	4
Microsoft Visual C++ 2017 x86 Minimum Runtime - 14.10.25017	4
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.21.27702	1
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.23.27820	3
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.26.28720	4
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.27.29112	2
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.21.27702	1
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.23.27820	3
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.26.28720	4
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.27.29112	2
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702	1
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.23.27820	2
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.29.30133	2
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702	1
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.23.27820	2
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.29.30133	2
Microsoft Visual C++ 2022 X64 Additional Runtime - 14.32.31326	6
Microsoft Visual C++ 2022 X64 Additional Runtime - 14.32.31332	7
Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31326	6
Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31332	7
Microsoft Visual C++ 2022 X86 Additional Runtime - 14.32.31326	6
Microsoft Visual C++ 2022 X86 Additional Runtime - 14.32.31332	10
Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.32.31326	6
Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.32.31332	10
Microsoft Visual Studio 2010 Tools for Office Runtime (x64)	16
Microsoft Visual Studio Tools for Applications 2017	1
Microsoft Visual Studio Tools for Applications 2017 x64 Hosting Support	1
Microsoft Visual Studio Tools for Applications 2017 x86 Hosting Support	1
Microsoft Visual Studio Tools for Applications 2019	1
Microsoft Visual Studio Tools for Applications 2019 x64 Hosting Support	1
Microsoft Visual Studio Tools for Applications 2019 x86 Hosting Support	1
Microsoft VSS Writer for SQL Server 2017	1
Microsoft VSS Writer for SQL Server 2019	1
Microsoft Windows 10 Pro	39
Microsoft Windows 11 Pro	26
Microsoft Windows Desktop Runtime - 6.0.27 (x64)	1
Microsoft Windows Desktop Runtime - 6.0.28 (x64)	1
Microsoft Windows Server 2016 Standard	3
MindView 7.0	1
Mozilla Firefox (x64 en-GB)	2
Mozilla Firefox (x64 en-US)	10
Mozilla Firefox 72.0.1 (x64 en-GB)	1
Mozilla Firefox 78.5.0 ESR (x86 en-US)	1
Mozilla Firefox ESR (x64 en-US)	2
Mozilla Firefox ESR (x86 en-US)	2
Mozilla Maintenance Service	15
MSI to redistribute MS VS2005 CRT libraries	5

MyEpson Portal	1
NirSoft BlueScreenView	2
Nmap 7.92	1
Npcap	1
NVIDIA Ansel	2
NVIDIA Control Panel 461.40	2
NVIDIA Display Container	2
NVIDIA Display Container LS	2
NVIDIA Display MessageBus	2
NVIDIA Display Session Container	2
NVIDIA Display Watchdog Plugin	2
NVIDIA Graphics Driver 461.40	2
NVIDIA Install Application	2
NVIDIA Optimus Update 38.0.2.0	1
NVIDIA Update 38.0.2.0	1
NVIDIA Update Core	1
Office 16 Click-to-Run Extensibility Component	62
Office 16 Click-to-Run Extensibility Component 64-bit Registration	2
Office 16 Click-to-Run Licensing Component	62
Office 16 Click-to-Run Localization Component	31
OneStop Collection Agent	1
OptaneDowngradeGuard	1
Payroll for Windows	1
PC-PinPad	3
Post_Update_Msi_Installer	6
PreloadHDAudioBus	1
PremierePro	2
PreReq	1
PrintProjects	1
PuTTY release 0.78 (64-bit)	1
Qualcomm 11ac Wireless LAN&Bluetooth Installer	3
Qualcomm Atheros Bluetooth Installer (64)	3
Qualcomm Atheros Setup	3
Realtek Audio COM Components	1
Realtek Audio Driver	7
Realtek Card Reader	7
Realtek Ethernet Controller All-In-One Windows Driver	1
Realtek Ethernet Controller Driver	4
Realtek High Definition Audio Driver	9
Realtek USB Audio	1
REALTEK Wireless LAN and Bluetooth Driver	1
RstDowngradeGuard	1
Sage (UK) Ltd. Sage 50cloud Payroll	1
Sage 50 Accounts	8
Sage 50 Accounts Data Access Components	8
Sage 50 Accounts Lockstep	5
Sage 50 Accounts ODBC 64 bit	7
Sage 50 Accounts Report Pack	6
Sage 50 HR v4.0	2
Sage 50 Payroll	3
Sage 50cloud Accounts	2
Sage 50cloud Accounts Data Access Components	2
Sage 50cloud Accounts ODBC 32 bit	1
Sage 50cloud Accounts ODBC 64 bit	2
Sage 50cloud Accounts Report Pack	1
Sage 50cloud Payroll	6
Sage Migration Tool	6
Scan2Text	1

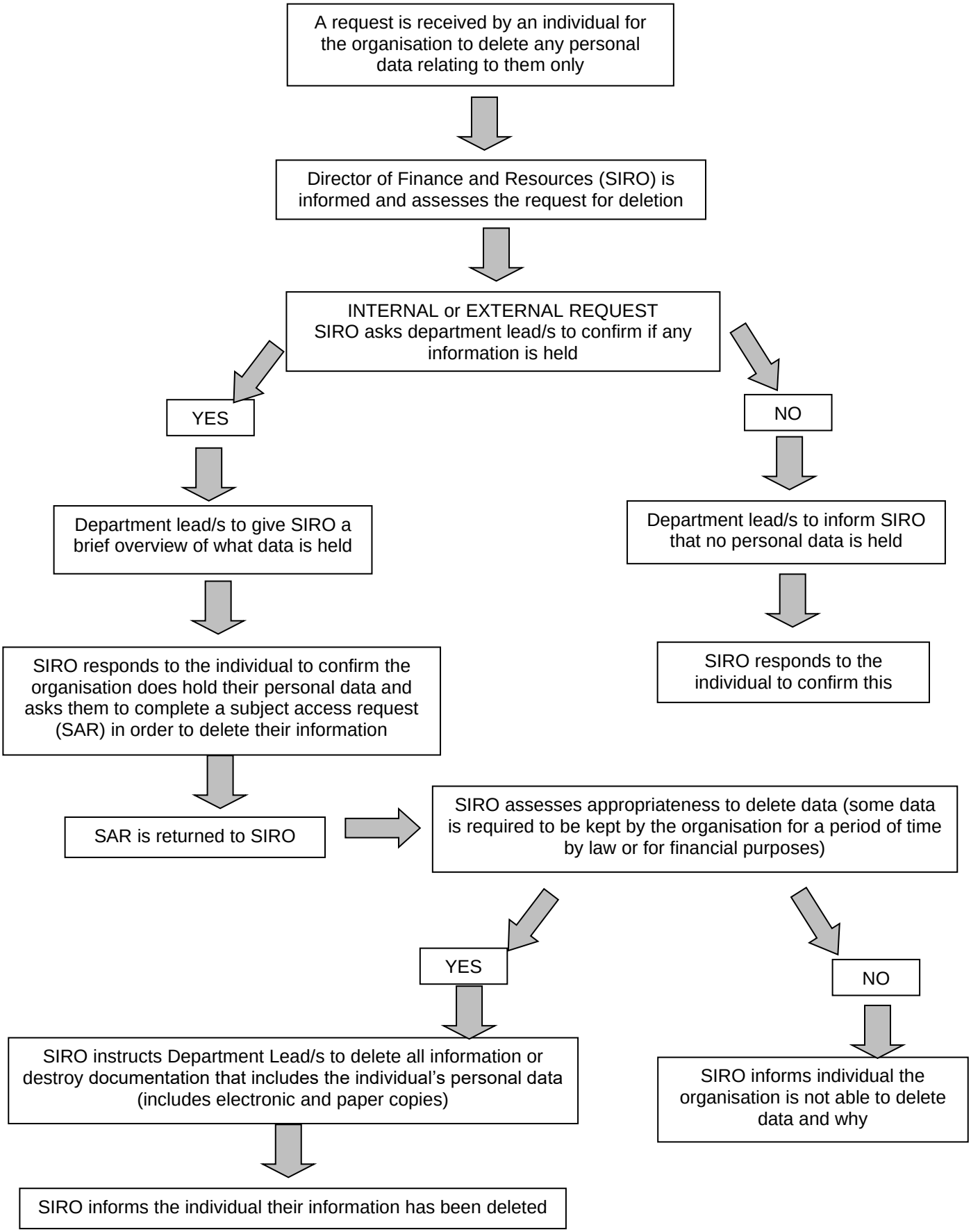
SCFileSecureAES	4
ScriptRunner Bootstrap Installer	67
ScriptRunner.Installer 2.50.1.3	53
ScriptRunner.Installer 2.92.0.7	56
ScriptRunner.Installer 2.94.0.2	6
Sentinel Agent	65
Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition	2
Service Pack 3 for SQL Server 2014 (KB4022619) (64-bit)	1
Service Pack 4 for SQL Server 2012 (KB4018073) (64-bit)	1
Skype version 8.57	1
SmartControlCenter	1
Sophos Connect	36
Splashtop Streamer	1
SQL Server 2012 Common Files	1
SQL Server 2012 Database Engine Services	1
SQL Server 2012 Database Engine Shared	1
SQL Server 2017 Batch Parser	1
SQL Server 2017 Common Files	1
SQL Server 2017 Connection Info	1
SQL Server 2017 Database Engine Services	1
SQL Server 2017 Database Engine Shared	1
SQL Server 2017 DMF	1
SQL Server 2017 Shared Management Objects	1
SQL Server 2017 Shared Management Objects Extensions	1
SQL Server 2017 SQL Diagnostics	1
SQL Server 2017 XEvent	1
SQL Server 2019 Batch Parser	1
SQL Server 2019 Common Files	1
SQL Server 2019 Connection Info	1
SQL Server 2019 Database Engine Services	1
SQL Server 2019 Database Engine Shared	1
SQL Server 2019 DMF	1
SQL Server 2019 Shared Management Objects	1
SQL Server 2019 Shared Management Objects Extensions	1
SQL Server 2019 SQL Diagnostics	1
SQL Server 2019 XEvent	1
Sql Server Customer Experience Improvement Program	1
SQL Server Management Studio	2
SQL Server Management Studio for Analysis Services	1
SQL Server Management Studio for Reporting Services	1
SQL Server Management Studio Language Pack - English	1
SSMS Post Install Tasks	2
ST Microelectronics 3 Axis Digital Accelerometer Solution	3
Suite MSIs for WebSigner Barclays	4
Surface Book 2 Update 20.012.21576.0 (64 bit)	1
SwannView Link version 2.2.2.8	1
Synaptics Pointing Device Driver	1
Synaptics WBF FP Reader	1
Teams Machine-Wide Installer	53
TeamViewer Host	2
Tenable Nessus (x64)	1
ThinkPad Thunderbolt 3 Dock	1
ThinkPad Thunderbolt 3 Dock and USB-C Dock	1
Thinkpad USB Ethernet Adapter Driver	10
ThinkPad USB-C Dock USB Audio	1
Thunderbolt? Software	1
TomTom HOME	1
TomTom MyDrive Connect 4.2.7.3966	1

TreeSize Free V4.7.1 (64 bit)	1
Ubiquiti UniFi (remove only)	1
UpdateAssistant	2
update_server	1
UXP WebView Support	2
Veeam Agent for Linux Redistributable	1
Veeam Agent for Mac Redistributable	1
Veeam Agent for Microsoft Windows Redistributable	1
Veeam Agent for Unix Redistributable	1
Veeam Backup & Replication	1
Veeam Backup & Replication Console	1
Veeam Backup & Replication Server	1
Veeam Backup Catalog	1
Veeam Backup Transport	1
Veeam Backup vPowerNFS	1
Veeam Distribution Service	1
Veeam Explorer for Microsoft Active Directory	1
Veeam Explorer for Microsoft Exchange	1
Veeam Explorer for Microsoft SharePoint	1
Veeam Explorer for Microsoft SQL Server	1
Veeam Explorer for Microsoft Teams	1
Veeam Explorer for Oracle	1
Veeam Installer Service	1
Veeam Mount Service	1
ViceVersa Pro 3.0 64-bit (Build 3003)	1
Visual DataFlex 2012 Client Engine 17.1	20
Visual Studio 2017 Isolated Shell for SSMS	2
VLC Media Player	2
VMware Remote Console	1
VMware Tools	3
VNC Server 6.6.0	1
VNC Viewer 6.20.529	1
Vulkan Run Time Libraries 1.0.61.0	1
Vulkan Run Time Libraries 1.0.65.1	3
Web Signer Bundle 64 bits Barclays with Classic Client middleware & eSigner	2
Web Signer Extension 64 bits for Barclays	6
Wildix Collaboration	10
Wildix Collaboration 2.6.5	2
Wildix Integration Service	3
Windows 10 Update Assistant	26
Windows Internet Explorer	68
Windows PC Health Check	2
Windows Setup Remediations (x64) (KB4023057)	3
Zoom (64-bit)	27
Zoom Outlook Plugin	4
Zoom(64bit)	5

Subject Access Request Process



Requests to Delete Data



Nottinghamshire Hospice
adding life to days

Subject Access Request Form

You have a right to access the information which Nottinghamshire Hospice holds about you.

You can use this form to ask for a copy of personal data that we hold about you or on behalf of someone else if you are legally allowed to act on their behalf, in line with data protection legislation.

To request information please complete this form and return it with identification to:

Nottinghamshire Hospice
384 Woodborough Road
Nottingham
NG3 4JF

Or via email info@nottshospice.org

Provided we have sufficient information and proof of identity to locate the information sought, a response will be provided within 30 days of receipt. Where a request is complex or numerous, the person submitting the request will be informed within 1 month of receipt that the timeframe for response has been extended up to 3 months.

Please make sure you complete all relevant sections in block capitals and black ink to ensure that details are clear.

Section 1: Details of the person this request is about (the 'Subject')

Forename(s)		Title	
Surname		D.O.B	
Maiden/Former/Other name			
Contact Number(s)			
Email Address			
Current Address			
Previous Address (for period covered by request if necessary)			

Section 2: Written authority to act on behalf of the person you are making the request for

This section should only be completed if you are making a request on behalf of someone else. We need to know what gives you the authority to act on their behalf, so please state your relationship with them e.g. a parent, solicitor, or holder of power of attorney.

Full Name	
Relationship with the subject	
Contact Number(s)	
Email Address	
Address	

Section 3: Personal Data Sought:

Please use the space below to describe the information sought. Be clear about the information you require and give us as much detail as possible, as this will help us to respond promptly to your request. Please include relevant dates and times, descriptions of circumstances or times you were in contact with the Hospice, and how.

Section 4: Proof of Identity

Please do not send any original documents only printed or electronic copies.

Applying for yourself
If you are applying for yourself, we need to see:

1. One document confirming your name, from Group A, below

    - Full driving licence
    - Passport
    - Birth certificate
    - Marriage or civil partnership certificate

2. One document confirming your address, from Group B, below

    - Utility bill
    - Bank statement
    - Credit card statement
    - Benefit book
    - Pension book

Applying on behalf of someone else
If you are applying on behalf of someone else, we need to see:

1. One document confirming your name and one document confirming the name of the person you are applying on behalf of, from Group A, below

    - Full driving licence
    - Passport
    - Birth certificate
    - Marriage or civil partnership certificate

2. One document confirming your address and one document confirming the address of the person you are applying on behalf of from Group B, below

    - Utility bill
    - Bank statement
    - Credit card statement
    - Benefit book
    - Pension book

3. Proof that you have the authority to access the records, from Group C, below

    - Health and Welfare Lasting Power of Attorney
    - Court of Protection Order appointing you as a personal deputy for the personal welfare of the Subject
    - Signed declaration from the subject

Section 5: where you would like the copies of your information to be sent

We prefer to send your information via email as this is a secure method. However if you would like to get your information by post, please note that information will be sent via special delivery and will need a signature upon receipt.

Please select one option to tell us where you would like your information sent:

☐ I am the Data Subject and would like my information sent to my email address given in Section 1.

☐ I am the Data Subject and would like my information posted to my home address given in Section 1.

☐ I am the Data Subject and would be happy to collect my information in person from Nottinghamshire Hospice.

☐ I am acting on behalf of the Data Subject and would like the information sent to the email address given in Section 2.

☐ I am acting on behalf of the Data Subject and would like the information posted to the address given in Section 2.

☐ I am acting on behalf of the Data Subject and would be happy to collect the information in person from Nottinghamshire Hospice.

Section 6: Declaration

I confirm that the information I have supplied in this application is correct, and I am the person whom it relates to, or I am acting on behalf of the Data Subject and have enclosed the relevant proof of authority.

Knowingly or recklessly obtaining or disclosing personal data is an offence under data protection legislation. By signing this form, you are giving agreement that your personal data (or that of the person you are acting on behalf of) can be shared within Nottinghamshire Hospice in order that we may process your request.

Data Subject:

Signature: …… Date: …….

Print Name: ……..

Person making a request on behalf of the data subject:

Signature: …… Date: ……

Print Name: ……..

Protecting Security of Data

- All emails containing personal data must be password protected
- All emails containing personal data must be marked “confidential”
- Personal data may only be transmitted over secure networks
- Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it
- Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using a ‘signed for’ delivery or courier service; and should be marked “confidential”
- No personal data may be shared informally and if access is required to any personal data, such access should be formally requested
- All electronic copies of data stored on physical media should be stored securely and password protected
- No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation
- Personal data must be handled with care at all times and should not be left unattended or on view
- Computers used to view personal data must always be locked before being left unattended
- No personal data should be stored on any work mobile device, without the formal written approval of the Senior Risk Information Officer and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary
- Personal data may only be transferred to devices personally belonging to employees, agents, contractors, or other parties working on behalf of the Company where the

party in question has agreed to comply fully with the Company's Data Protection Policy and the GDPR

- All personal data stored electronically should be backed up daily with backups stored offsite. All backups should be password protected
- All passwords used to protect personal data should be changed regularly and must be secure
- Passwords should not be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT support staff do not have access to passwords
- All software should be kept up to date. Security-related updates should be installed as soon as reasonably possible after becoming available
- No software may be installed on any Company-owned computer or device without approval.
- Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Fundraising Manager to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

Appendix 5

Payment Card Industry Data Security Standard (PCI DSS)

PCI Security Standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data – with requirements for software developers and manufacturers of applications and devices used in those transactions.

The Council is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB, MasterCard and Visa Inc.

There are a broad range of consequences associated with breaching the regulations, including a suspension of the ability to accept credit cards, liability for fraud charges, credit card replacement costs, and mandatory forensic examination.

Security of POI (Point of Interaction) Devises

Nottinghamshire Hospice should ensure POI devises are used in accordance with the solution providers guidance/instruction manual.

- POI devise surfaces should be periodically inspected to detect tampering and unauthorised substitution.
- Identification should be requested, before any third party is granted access to modify or troubleshoot devices.

Training

Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes:

- Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.
- Procedures to ensure devices are not installed, replaced, or returned without verification.
- Being aware of suspicious behaviour around devices.
- Reporting suspicious behaviour and indications of device tampering or substitution to appropriate personnel.

Emergency Contact

The Retail Operations Manager should be contacted in the event of an emergency relating to POI devices.

Shop/Location	Model	MID	Serial Number
41 Mansfield Road, Blidworth, Mansfield. NG21 0RB	Verifone P400 Plus	2102003664	807-458-759
45 Main Street, Burton Joyce, Nottingham. NG14 5DX	Verifone P400 Plus	2102003670	807-458-691
900 Woodborough Road, Mapperley, Nottingham. NG3 5QR	Verifone P400 Plus	2102003665	807-458-489
Unit 2, Main Street, Radcliffe on Trent, Nottingham. NG12 2FH	Verifone P400 Plus	2102003673	807-458-633
10 High Street, Ruddington, Nottingham. NG11 6EH	Verifone P400 Plus	2102003681	807-458-731
583 Mansfield Road, Sherwood, Nottingham. NG5 2JN	Verifone P400 Plus	2102003669	807-458-782
6 Gordon Road, West Bridgford, Nottingham. NG2 5LN	Verifone P400 Plus	2102003682	807-458-692
174 Bramcote Lane, Wollaton, Nottingham. NG8 2QP	Verifone P400 Plus	2102003660	807-458-762
Fundraising Team, Nottinghamshire Hospice, 384 Woodborough Road, Nottingham NG3 4JF	Ingenico Tetra Move 5000 Engage v400	2102003665	23081731316129400000000

Data Categories and Retention Periods

Appendix 6

Data Category	Type of Data	Retention Trigger	Retain For	Action	Retention Source
Regulatory	Audit Reports	Case closed	6 years	Review	Business Need
Regulatory	Breach Report	Case closed	2 years	Destroy	Business Need
Internal Regulatory Activities	Information created in relation to new policies, guidelines and research	Last Action	6 years	Review	Business Need
Stakeholder Engagement	Engagement with significant stakeholders	Last Action	6 years	Review	Business Need
Corporate Governance	Unsuccessful Trustee Recruitment Information	Creation	6 months	Destroy	Business Need
Corporate Governance	Trustee contact details, skills/application forms, election and term information	Resignation	7 years	Destroy	Business Need
Corporate Governance	Ambassadors contact details	Resignation	3 years	Destroy	Business Need
Corporate Governance	Memorandum of Understanding	End of Understanding	6 years	Destroy	Business Need
Corporate Governance	Committees and group minutes	Minutes agreed	6 years	Review	Business Need
Corporate Governance	Organisation wide corporate plans, policies, business continuity, risk management and strategies	Superseded	3 years	Review	Business Need
Corporate Governance	Corporate roles and responsibilities	Superseded	6 years	Review	Business Need
Corporate Governance	Non-clinical Complaints	Closure	1 year	Destroy	Business Need

Data Category	Type of Data	Retention Trigger	Retain For	Action	Retention Source
Corporate Governance	Non-clinical Incidents and Accidents	Closure	7 years	Destroy	Business Need
Corporate Functions	Health and Safety Inspections, Property Management and Asset records	Last Action	6 years	Review	The National Archives Retention Scheduling: Departmental Accounts, H&S at work Act 1974 and supporting regulations, Limitation Act 1980
Corporate Functions	Documents relating to IT systems integral to their running and long term use	End of system life	3 years	Review	Business Need
Corporate Functions	Records and Information Management	Last Action	3 years	Review	Business Need
Corporate Functions	It Infrastructure	Last Action	3 years	Review	Business Need
Corporate Functions	Information Security	Last Action	6 years	Review	Business Need
Corporate Functions	Information Requests	Case Closed	2 years	Destroy	Business Need
Corporate Functions	Projects and Corporate Programmes	Last Action	3 years	Review	Business Need
Corporate Functions	CCTV	Last Action	1 month	Destroy	ICO CCTV Policy
Corporate Functions	Reception sign in book	End of Year	2 years	Destroy	Business Need
Finance	Financial Information	End of Financial Year	7 years	Destroy	The National Archives Retention Scheduling: Employee Personal Records and CIPD
Finance	Payroll Capita Reports	End of Financial Year	7 years	Destroy	HM Treasury guidelines, National audit office, Companies Act 2006
Finance	Employee contact, bank, tax and pension details	End of Employment	7 years	Destroy	Business Need

Data Category	Type of Data	Retention Trigger	Retain For	Action	Retention Source
Human Resources	Employee files and Personal Development Records	End of Employment	7 years	Destroy	The National Archives Retention Scheduling: Employee Personal Records and CIPD
Human Resources	Disciplinary and Grievance, Examination and Testing, Accident and Ill Health	Last Action	7 years	Destroy	Limitation Act 1980
Human Resources	Job Descriptions and T&Cs	Last Action	7 years	Destroy	Limitation Act 1980
Human Resources	Training Material	Superseded	7 years	Destroy	Limitation Act 1980
Human Resources	Political Declarations	Superseded or end of employment	7 years	Destroy	The National Archives Retention Scheduling: Employee Personal Records and CIPD
Human Resources	Industrial Relations	Last Action	7 years	Destroy	Limitation Act 1980
Human Resources	Payroll sheets	End of Financial Year	7 years	Destroy	HM Treasury guidelines, National audit office, Companies Act 2006
Human Resources	Maternity, Paternity, Adoption and Sick Leave	End of Financial Year after return	7 years	Destroy	Statutory Sick Pay Regulations 1982, Statutory Maternity pay Regulations 1986, Statutory Paternity pay and Adoption pay Regulations 2002
Human Resources	Successful Recruitment Candidate Information	End of employment	7 years	Destroy	The National Archives Retention Scheduling: Employee Personal Records and CIPD
Human Resources	Unsuccessful Recruitment Candidate Information	Last Action	6 months	Destroy	Limitation Act 1980
Human Resources	Staff pension, pay history and termination reasons	From DOB	100 years	Destroy	The National Archives Retention Scheduling: Employee Personal Records

Data Category	Type of Data	Retention Trigger	Retain For	Action	Retention Source
Human Resources	Health Surveillance	Last Action	40 years	Destroy	Health and Safety at Work Act
Human Resources	Third Party emergency contact details provided by the staff member	End of Employment	Immediate	Destroy	Business Need
Human Resources	DBS Certificates	Creation	6 months	Retain top part of certificate only	Business Need
Human Resources	Medical Referrals	End of Employment	7 years	Destroy	Business Need
Legal	Policy Legal and Legal Advice	Last Action	6 years	Review	Limitation Act 1980
Legal	Contracts	End of Contract	6 years	Review	The National Archives Retention Scheduling: Contractual Records
Legal	Unsuccessful Tenders	Last Action	400 Days	Review	The National Archives Retention Scheduling: Contractual Records
Legal	Building Contracts and Leases	End of Contract	12 years	Review	Limitation Act 1980
Volunteering	Unsuccessful Volunteer Recruitment Information	Creation	6 months	Destroy	Business Need
Volunteering	Successful Volunteer Recruitment Information	End of volunteering	3 years	Destroy	Business Need
Volunteering	DBS Certificates	Creation	6 months	Retain top part of certificate only	Business Need
Volunteering	Volunteer files, contact details and development records	End of volunteering	3 years	Destroy	Business Need
Retail	Customer contact and addresses, payment history /purchase history for refunds or voids	Transaction	3 years	Destroy	Business Need

Data Category	Type of Data	Retention Trigger	Retain For	Action	Retention Source
Retail & Fundraising	Gift Aid donor declaration forms and contact information	The most recent donation that gift aid was claimed on	7 years	Destroy	Business Need
Fundraising	Donor contact details	Last Action	3 years	Destroy	Business Need
Fundraising	Donor Bank details on leaflets and envelopes	Last Action	Instant	Destroy	Business Need
Marketing and Comms	Event and Challenge attendees contact details	Last Action	3 years	Destroy	Business Need
Marketing and Comms	E-newsletter subscribers via mailchimp	Until user unsubscribes	Instant	Destroy	Business Need
Corporate Communications and Marketing	Market research reports, press releases, campaigns and projects, informer and image banks	Last Action	6 years	Review	Business Need
Corporate Communications and Marketing	Staff Events and Briefings, Public Engagement and Political Monitoring	Last Action	3 years	Review	Business Need
Corporate Communications and Marketing	Requests for Publications	Creation	4 weeks	Destroy	Business Need
Bereavement and Carer Support	Client files, contact details and personal information	Death/Discharge	7 years	Destroy	Business Need
Clinical	Patient files, contact details and personal information	Death/Discharge	10 years	Destroy	Business Need
Clinical	Clinical Incidents and Accidents	Closure	10 years	Destroy	Business Need
Clinical	Clinical Complaints	Closure	10 years	Destroy	Business Need

Data Category	Type of Data	Retention Trigger	Retain For	Action	Retention Source
Communication Activities	Staff Mailboxes and Outlook	End of Employment	2 years	Delete	Business Need
Communication Activities	Physical Correspondents	Once Scanned	6 months	Destroy	Business Need
Organisation Wide	Internal Audits	Creation	3 years	Destroy	Business Need
Organisation Wide	Templates, Procedures, Team Information and Team Meetings	Last Action	3 years	Review	Business Need
Organisation Wide	Department Logs and Registers	Last Action	12 months	Review	Business Need
Organisation Wide	Team Administration	Creation	3 years	Review	Business Need
Organisation Wide	Management Information	End of Financial Year	6 years	Review	Business Need
Organisation Wide	Mobile device information for visitor Wi-Fi use	Creation	90 days	Destroy	Business Need