**Document Control Information**

**Document Control**

|  |  |
| --- | --- |
| Policy Title | Record Retention & Destruction |
| Number | OPS61 |
| Date | 25/10/2020 |
| Version | 1.4 |
| Review due | 25/10/2023 |
| Classification | Unclassified |
| Owner | Governance & Quality Assurance |
| Author |  |
| Reviewer |  |

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description** |
| 1.0 | 10/05/2016 | Original Document |
| 1.1 | 19/04/2018 | Minor changes to formatting and language; major changes to some details and comments made for consideration. |
| 1.2 | 23/07/2018 | Minor changes to language; major changes to some detail re legislation and guidance |
| 1.3 | 06/12/2018 | Updates to layout, role titles and legislative links up-dated. |
| 1.4 | 25/09/2020 | Updated with current Iron Mountain process for archive and new Retention Schedule. Best practice for electronic document archive added |

**Document Approvals**

|  |  |
| --- | --- |
| **Approver** | **Date** |
| Head of Governance – | 23/11/2020 |
| SIRO – | 23/11/2020 |

**This page is left intentionally blank**

**Contents**

[1. Policy Statement 4](#_Toc56770970)

[2. Scope 4](#_Toc56770971)

[3. Purpose 4](#_Toc56770972)

[4. Security of Personal Data Records 4](#_Toc56770973)

[5. Roles and Responsibilities 6](#_Toc56770974)

[6. Archiving (Long term storage of) Data 7](#_Toc56770975)

[7. Retention periods 8](#_Toc56770976)

[8. Confidential Waste 13](#_Toc56770977)

[9. Related Policies 14](#_Toc56770978)

[10. Training Statement 14](#_Toc56770979)

[11. Contact Details 14](#_Toc56770980)

# Policy Statement

All records required for the protection of customers and the effective and efficient running of the organisation, should be collected, maintained and disposed of in accordance with the General Data Protection Regulation (GDPR) and the [Data Protection Act (DPA) 2018](http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted).

This policy relates to Optalis’ provider services and central office records. The policy exists to ensure that all Optalis records, whether analogue or digital, are subject to the retention requirements of this procedure. This policy should be read alongside the Data Protection Policy and is in line with good practice guidance. Care records should comply with standards set by regulators namely the Care Quality Commission, specifically relating to [Regulation 17: Good Governance.](https://www.cqc.org.uk/guidance-providers/regulations-enforcement/regulation-17-good-governance) Records must be:

* Kept securely
* Organised for ease of location for prompt responses to requests
* Retained for an appropriate period
* Securely destroyed when it is appropriate to do so

# Scope

This policy applies to all staff, contractual third parties, and agents doing work for Optalis. Every member of staff has personal responsibility to ensure they comply with this policy.

# Purpose

The purpose of this policy is to define the individual responsibility and accountability of every member of staff to ensure the appropriate security for data held for and within Optalis.

# Security of Personal Data Records

All staff have responsibility for ensuring the security of the records that they work with. Any records which contain personal data, that is, customer and staff names and addresses, **must be locked away when not in use**. All staff must be especially careful when handling sensitive personal data (also known as [special category data](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/)), such as information about any other person’s:

* Race
* Ethnic origin
* Politics
* Religion
* Trade union membership
* Genetics
* Biometrics (where used for ID purposes)
* Health
* Sex life; or
* Sexual orientation

In particular, this type of data could create more significant risks to a person’s fundamental rights and freedoms; for example, putting persons at risk of unlawful discrimination. There **must be a lawful basis** for processing each item of information you hold (e.g. name, date of birth, health, gender etc.). Furthermore, if you are processing special category data you need additional conditions for processing.

The Optalis Record of Processing Activity (RoPA) **records all the items of personal data that the organisation holds**, the category of individual the data is about (e.g. employee, customer etc.), and the reason we hold it (the lawful basis). The RoPA also includes how long we keep the information, where it is located and other information related to our personal data processing. Managers are responsible for contributing to, reviewing and updating the RoPA on an annual basis; this process is managed by the Data Protection Officer – [dpa@optalis.org](mailto:dpa@optalis.org).

The lawful bases available for processing personal data under GDPR [Article 6](http://www.privacy-regulation.eu/en/article-6-lawfulness-of-processing-GDPR.htm) are:

* Processing is necessary for the performance of a contract;
* Processing is necessary for the compliance with a legal obligation;
* Processing is necessary for our legitimate interests; or
* Consent has been obtained (*take care, consent must be freely given and can be withdrawn; it is* ***not*** *a suitable basis for information that is needed under another category*)

The lawful bases for processing special category data under GDPR [Article 9](http://www.privacy-regulation.eu/en/article-9-processing-of-special-categories-of-personal-data-GDPR.htm) include:

* Consent has been obtained
* Processing is necessary for the obligations and specific rights in the field of employment and social security and social protection law
* Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
* Processing is necessary for the establishment, exercise or defence of legal claims
* Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical

diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

* Processing is necessary for reasons of public interest in the area of public health

If you believe that you may have data **without a legal basis for doing so** or need more information on conditions for processing please contact [dpa@optalis.org](mailto:dpa@optalis.org).

# Roles and Responsibilities

**The Director of Human Resources & Corporate Services**

The Director of HR is responsible for the retention of all HR records.

**The Head of Finance, Compliance and Performance Management**

The Head of Finance, Compliance and Performance Management has the responsibility for the retention of all financial (e.g. accounting, tax) and related records. Along with the Service Managers, this role is also responsible for ensuring that retained records are considered when preparing Business Continuity / Disaster Recovery Plans. The Head of Finance, Compliance and Performance Management will also support the Board, or their delegate, in ensuring appropriate retention and destruction of records.

**The Head of Governance**

The Head of Governance (along with the Service Managers), is responsible for ensuring that retained records are considered when preparing Business Continuity / Disaster Recovery Plans. The Head of Governance will also support the Board, or their delegate, in ensuring appropriate retention and destruction of records.

**Data Protection Officer (DPO)**

The DPOI is responsible to management and maintenance of the Optalis RoPA (register of processing activity) to ensure and assure the processing of data is legitimate and appropriate. The DPO (and where available delegated to the IGO) is also responsible for communicating the policy and procedures to all staff; acting as a central point of contact and directing staff to appropriate resources and contacts, and supporting where necessary.

**Service Managers**

Service Mangers and/or their agreed delegate within the service(s) is responsible for:

* Retention of statutory and regulatory records including Health & Safety records
* Business Continuity / Disaster Recovery Planning requirements with regard to

records

* Storage, and the eventual destruction, of data relating to their services
* Ensuring their staff understand the requirements of data retention and

appropriate destruction or archiving responsibilities

# Archiving (Long term storage of) Data

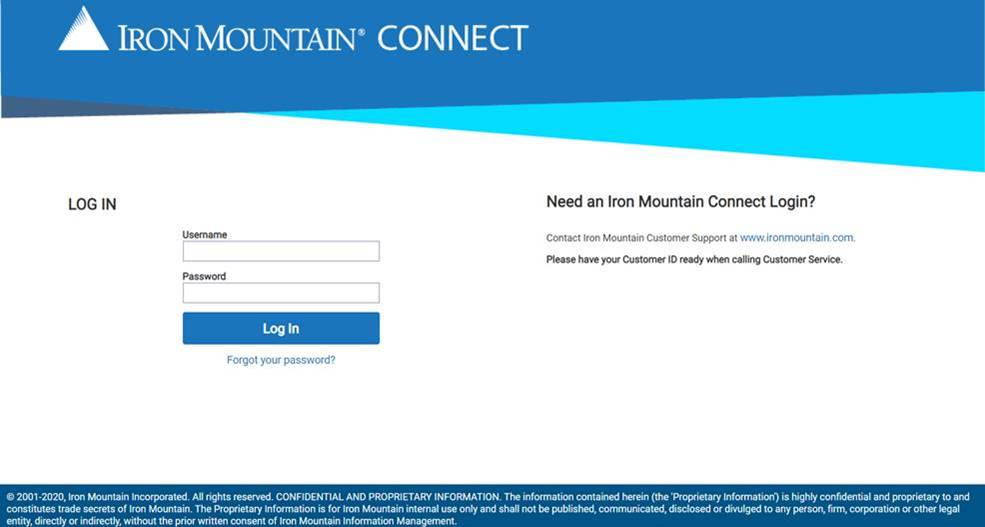
Managers committing data items to storage must ensure that each item is marked with:

* Name of record
* Type of record
* Data owner
* Information classification
* Date stored
* Retention period
* Scheduled date for destruction
* Other special information (e.g. cryptographic keys)

**Iron Mountain Archiving Process**

All staff that need to archive physical records should have an account set up with Iron Mountain who are the archive provider. If you are a new member of staff your manager should request access for you by contacting [cservices@ironmountain.co.uk](mailto:cservices@ironmountain.co.uk).

When you need to archive records you should be able to **log your request** and **book the boxes and labels** through the [**IM Connect portal**](http://www.ironmountainconnect.com) with the **ID** they provided and your **password**:



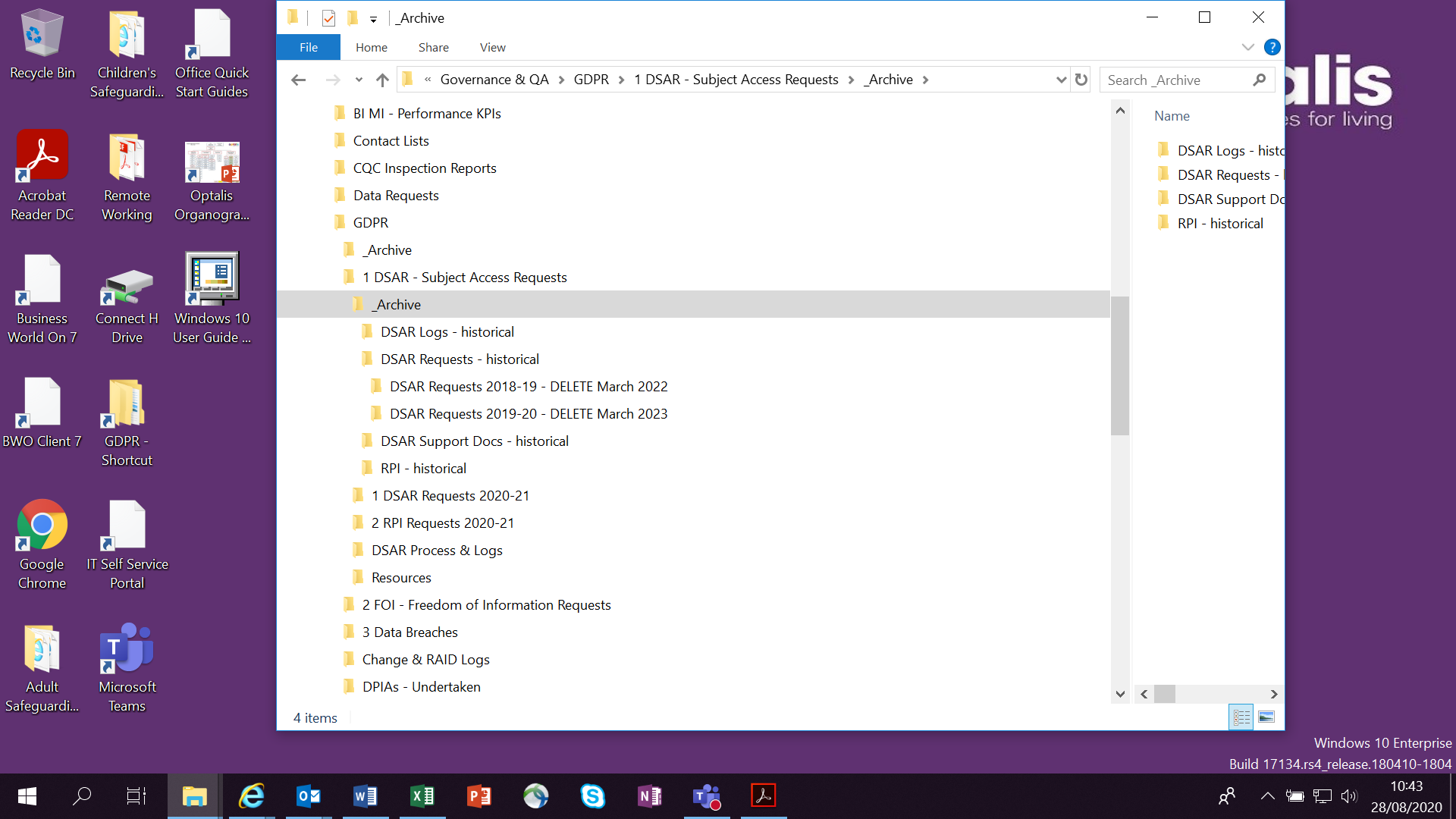
[www.ironmountainconnect.com](https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.ironmountainconnect.com%2F&data=02%7C01%7CDPA%40Optalis.org%7C3e1880fe202c475b22ac08d83ab5b27d%7C996ee15c0b3e4a6f8e65120a9a51821a%7C0%7C0%7C637323899352760409&sdata=hjIJG6l4M8uFCnOCk9btkUS9cmBXbjWv6sd0ioEQCfY%3D&reserved=0)

If you have any problems accessing this or need support, you can contact the team directly via [cservices@ironmountain.co.uk](mailto:cservices@ironmountain.co.uk). Iron Mountain have a number of training resources – tutorials, videos, live training sessions, documents etc. for you to be able to familiarise yourself with the online process.

When completing the section referring to **Purchase Order numbers**, this can contain the delegate’s (person submitting) name, enabling the processing screens to continue to completion.

**Electronic Data Archiving Process**

Where data is stored electronically, the relevant Directors or equivalent Managers should authorise / co-ordinate the disposal of the data. This could be made easier by reviewing the folders (within Archive folders) themselves, ensuring that the folder in question e.g. a staff file, would carry the retention date / timeframe within the title – advising of the period. An example of this structure is shown below for the Data Subject Access Request (DSAR) files within the Governance & QA Team.



Within the DSAR Archive folder the other folders are marked ‘historical’ to denote they contain old versions and old records that are no longer in use but may be needed for reference purposes. Within the ‘DSAR Requests – historical’ folder are two folders that have deletion dates in line with the period specified in the Retention Schedule. These folders **will be deleted at the appropriate time** during the regular records management process.

# Retention periods

Optalis retains a large number of records and the required retention periods, by record type, are listed in detail in the **Optalis Retention Schedule**. The Schedule can be accessed on the Optalis intranet.

The following tables give retention periods for key records only. For other records please see the full Optalis Retention Schedule. Where relevant, retention periods are aligned with the Records Management Code of Practice for Health and Social Care 2016 published by NHS Digital / Information Governance Alliance and referenced by the CQC within the [Codes of Practice for Handling Information in Health and Care](https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care).

|  |  |
| --- | --- |
| **1. Customer Information** |  |
| **Document** | **Retention period** |
| Accident book records and accident reports | 3 years from last accident or investigation into accident (or if a young person is involved, until that person reaches the age of 21) |
| Carer’s assessment | 6 years after cessation of service |
| Complaints | 6 years after customer dies or moves on, or 6 years from completion of investigation if later |
| Adult social care record (customer file) | 8 years from last contact |
| DOLS (with Adult social care record) | 8 years from last contact |
| Liberty safeguards | 8 years from last contact |
| Needs assessment | 8 years after cessation of service |
| Outcome of safeguarding investigations | 6 years |
| Register of compliance failures | 6 years |

|  |  |
| --- | --- |
| **2. Residential & Homecare** |  |
| **Document** | **Retention period** |
| Allegations of abuse, neglect or other harm | 6 years after last entry |
| Customer File (adult Social Care Records) | 8 years from last contact |
| Details of physical restraint | 6 years after last entry |
| Notification of death, illness or accident | 6 years |
| Residential Care Homes Regulations, records kept under Schedule 3 | 6 years from date of last entry |
| Residential Care Homes Regulations, records kept under Schedule 4:  Copy of statement of aims and objectives of the home  Daily register  Special arrangements  Medical and Dental provision  Handling and Administration of Medicines  Scale of charges  Official inspections  For employment records, please see HR section | 6 years from date of last entry |
| Staff Rotas | 6 years from close of financial year |

|  |  |
| --- | --- |
| **3. HR: Personnel Procedures** |  |
| **Document** | **Retention period** |
| Application forms of non-shortlisted candidates | 1 year |
| DBS clearance documentation | Date of clearance + up to a maximum of six months |
| Parental leave information | 3 years after the end of the tax year in which the leave period ends |
| Short lists, interview notes and related application forms | 1 year |
| Staff Record | Whilst current then 6 years from leaving / decease or until 75th birthday (see Notes in Optalis Retention Schedule) |
| Staff Record Summary | 75th Birthday |
| Staff training records | Records of significant training must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member’s role. The IGA recommends:   * Clinical training records - to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer * Statutory and mandatory training records - to be kept for ten years after training completed * Other training records - keep for six years after training completed |
| Timesheets - original record | 2 years from creation |

|  |  |
| --- | --- |
| **4. HR: Health & Safety** |  |
| **Document** | **Retention Period** |
| Accident/incident/near miss records, reports | 6 years after date of occurrence |
| Health and Safety assessments | Permanently |
| Medical records as specified by the COSHH Regulations | 40 years from the date of the last entry |
| Medical records under the Control of Asbestos at Work – containing details of employees exposed to asbestos | 40 years from the date of the last entry |
| Occupational Health reports | Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner |
| RIDDOR notification | 12 years from the date of the entry |
| Sickness records | 6 years from end of sickness. However for industrial injuries not detectable within that period e.g. asbestos, the time period may be extended. Also for employees exposed to hazardous substances |

|  |  |
| --- | --- |
| **5. HR: Tax & Social Security** |  |
| **Document** | **Retention Period** |
| Copies of notices to employee (e.g. P45, P60) | 6 years plus current year |
| Income tax PAYE and NI returns | 6 years |
| Payroll & Salaries | 6 years plus current year |
| Record of maternity payments | 6 years |
| Record of sickness payments | 6 years |
| Redundancy details and record of payments and refunds | 12 years from date of redundancy |

|  |  |
| --- | --- |
| **6. HR: Pension Schemes** |  |
| **Document** | **Retention Period** |
| Detailed returns of pension fund contributions | Permanently |
| Investment policies | 12 years from end of benefits payable under policy |
| Pensioner's records | 12 years after benefit ceases |

|  |  |
| --- | --- |
| **7. Data Protection** |  |
| **Document** | **Retention Period** |
| Data Breach records | 6 years from end of investigation |
| Data Subject Access Request and disclosure correspondence | 3 years from closure of DSAR or where there has been an appeal, 6 years from closure of appeal |
| Freedom of Information (FOI) request, responses and associated correspondence | 3 years from closure of FOI or where there has been an appeal, 6 years from closure of appeal |

|  |  |
| --- | --- |
| **8. Governance Documentation** |  |
| **Document** | **Retention Period** |
| Board member documents e.g. appointment letters, SLAs, bank details etc. | 6 years after board membership ceases, although some details should be destroyed when membership ceases e.g. bank details etc. |
| Business plans and supporting documentation (e.g. organisation structures, aims, objectives, funding issues) | 5 years after plan completion |
| Declarations of interest | All versions retained until 7 years has elapsed since end of employment |
| Incidents - serious | 20 years from date of incident |
| Intranet site | 6 years from creation |
| Website | 6 years from creation |

|  |  |
| --- | --- |
| **9. Insurance** |  |
| **Document** | **Retention Period** |
| Claims and related correspondence | 3 years after settlement |
| Current and former policies | Permanently |
| Employer’s liability insurance certificate | 40 Years |
| Group health policies | 12 years after cessation of benefit |

|  |  |
| --- | --- |
| **10. Finance, Accounting & Tax** |  |
| **Document** | **Retention Period** |
| Accounting records for Limited Company | 6 years |
| Capital assets | Date of purchase to at least 6 years after date sold, transferred or disposed of |
| Signed copy of report and accounts | Permanently |
| VAT records | 6 years  10 years if VAT MOSS system used |

|  |  |
| --- | --- |
| **11. Other Banking Records** |  |
| **Document** | **Retention Period** |
| Bank statements and reconciliations | 6 years |

|  |  |
| --- | --- |
| **12. Contracts & Agreements** |  |
| **Document** | **Retention Period** |
| Contracts for the supply of goods or services, including professional services | 6 years after completion (including any defects liability period) |
| Contracts under seal and/or executed as deeds (including Notices posted in the Official Journal of the European Union (OJEU)) | 12 years after completion (including any defects liability period) |
| Contracts with grant funders for service delivery | Funders often have their own requirements for document retention and this should be adhered to  In the absence of guidance from the funder we should use 6 years after completion of all returns and funder sign-off or 12 years if related to land purchase/usage |
| Documents relating to successful tender | 6 years after end of contract |

# Confidential Waste

All hard copy data **must be destroyed by shredding** (ideally with a cross-cut shredder) **and then disposed of through appropriate recycling**. For large scale disposal an approved/accredited professional company will be used; in line with the PSL (Preferred Supplier list) within each service.

# Related Policies

OPS13 Data Protection Policy

OPS37 Compliance in Records Management

OPS29 Information Security

# Training Statement

Data Protection and records management responsibilities are initially covered in the induction process. However, comprehensive training is available to train and refresh staff on all aspects of data protection which includes retention and destruction requirements. As well as broad-based E-Learning, periodic face to face training (in person or online) is available specific to Optalis’ requirements and to various job roles.

# Contact Details

Data Protection Officer

Email: [DPA@Optalis.org](mailto:DPA@Optalis.org)

Governance and Quality Assurance Team

Email: [GovQA@Optalis.org](mailto:GovQA@Optalis.org)

Trinity Court

Wokingham

Berkshire

RG41 2PY