OPS13 Data Protection Policy

Document Control Information

Document Control

Policy Title	Data Protection
Number	OPS13
Effective Date	15/04/2021
Version	4.7
Review due	31/03/2023
Classification	UNCLASSIFIED Information Governance document
Owner	Governance and QA
Author	
Reviewer	

Revision History

Version	Date	Description
1.0	31/03/2015	Original Document.
2.1	27/02/2018	Document annual review.
3.0	26/03/2018	Major revision/re-write using policy good practice from other councils and the NHS.
3.1	12/04/2018	Includes changes proposed by, and other changes relating to GDPR.
3.2	08/05/2018	Minor updates to format. Operational policy links added.
3.3	14/05/2018	Converted DPA Principles to GDPR in section 8.1
4.3	20/07/2018	Major revision/re-write using policy safe practice; ensure good governance and set expectations of compliance.
4.4	03/08/2018	Minor revisions.
4.5	30/08/2018	Minor revisions.
4.6	30/07/2020	Addition of Email Etiquette in Section 14 and updated format.
4.7	15/01/2021	Revisions to reflect UK GDPR / Brexit implications Addition of section on Anonymisation / pseudonymisation to S14 Information Security

Document Approvals

Approver	Date
Head of Finance, Compliance & Performance Management –	29/03/2021
SIRO / CEO –	06/04/2021

This page is left intentionally blank

Contents

1. Introduction

This policy explains Optalis' requirements to comply with the UK Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR) and the EU GDPR (where necessary); Together, these are referred to as the "Data Protection Legislation"; they impose legal obligations on Optalis when processing personal and sensitive personal data.

This Data Protection Policy sets out the rights of data subjects and the obligations of Optalis as a data controller under the Data Protection Legislation, laying down a number of organisational and procedural measures to help ensure compliance. Optalis is a data controller in its own right and may also be a joint controller in certain circumstances (e.g. where both Optalis and the Local Authority keep records on the same individual for related purposes).

Detail in this Data Protection Policy is extensive, aiming to reproduce key parts of the Data Protection Legislation to aid in the establishment of knowledge and understanding throughout Optalis. Despite this, however, it should be noted that training remains essential and that all individuals handling personal data within Optalis should be fully aware of the Data Protection Legislation and its principles as well as the procedures in place within Optalis.

Optalis first registered with the UK Regulator (Information Commissioner's Office – ICO) as a Data Controller in June 2011 with a registration number of **Z2720565**.

2. Scope

This policy applies to all Optalis employees, contractors, and all others who undertake and deliver work for and on behalf of Optalis.

3. Policy Statement

Optalis is registered with the UK regulator – the Information Commissioners Office and is committed to complying with the Data Protection Legislation; ensuring all staff receive the necessary training and support to enable full compliance with the Legislation. In the course of their duties, Optalis staff who process personal data must comply with the Data Protection Legislation wherever they are working. This includes:

- Remote working (at home or off-site)
- In the workplace

All Optalis staff must read and confirm that they understand this policy, related procedures, and good practice guidance. This is required to ensure data can be collected, processed, utilised, or shared appropriately and in full compliance with the Data Protection Legislation.

Optalis is committed to protecting, maintaining, and archiving accurate data information and records collected and used for processing. This covers all forms of data including, but not restricted to, verbal, written, electronic data or voice recordings. Optalis will always uphold individuals' rights under the Data Protection Legislation.

4. Policy Compliance

If any Optalis member of staff or other worker is found to have breached this policy, they may be subject to the Optalis disciplinary (or related) breach procedures.

If a criminal offence is considered to have been committed further action will be taken to assist in the prosecution of the offender(s).

Employees who disclose personal data without authorisation and without taking into consideration the Data Protection principles may face disciplinary or similar action under the Optalis HR policies.

If you do not understand the implications of the policy or how it may apply to you, seek advice from your line manager directly, or alternatively you can contact Optalis' Data Protection Officer via DPA@Optalis.org.

5. Roles and Responsibilities

The Data Protection Officer (DPO)

Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with Data Protection Legislation requirements. Most importantly, the DPO will make independent decisions about when it is necessary to report a data breach to the ICO.

Under the UK GDPR the Data Protection Officer is a mandatory role under Article 37 for certain organisations that collect or process UK/EU citizens' personal data. Optalis as an organisation is classed as a public body (being wholly owned by local authorities); therefore, the appointment of a DPO is mandatory.

DPOs are responsible for ensuring that the company and its employees are educated on important compliance requirements, ensuring staff involved in data processing are trained, and conducting regular security audits.

DPOs must be "appointed for all public authorities, and where the core activities of the controller or the processor involve 'regular and systematic monitoring of data subjects on a large scale' or where the entity conducts large-scale processing of 'special categories of personal data,'" like that which details race or ethnicity or religious beliefs. As outlined in the UK GDPR Article 39, the DPO's responsibilities include, but are not limited to, the following:

- Educating the company and employees on important compliance requirements
- Training staff involved in data processing
- Conducting audits to ensure compliance and address potential issues proactively
- Serving as the point of contact between the company and GDPR Supervisory Authorities (i.e. the ICO in the UK, and the appropriate EU Authority if applicable)
- Monitoring performance and providing advice on the impact of data protection efforts
- Maintaining comprehensive records of all data processing activities conducted by the company, including the purpose of all processing activities, which must be made public on request
- Interfacing with data subjects to inform them about how their data is being used, their rights to have their personal data erased, and what measures the company has put in place to protect their personal information

The Regulation also specifies the DPO's expertise should align with Optalis' data processing operations and the level of data protection required for the personal data processed by data controllers and data processors.

DPOs may be a staff member or outsourced. Related organisations may utilise the same individual to oversee data protection collectively, as long as it is possible for all data protection activities to be managed by the same individual. The DPO must be easily accessible by anyone from any of the related organisations whenever needed.

The Senior Information Risk Officer (SIRO)

The SIRO's responsibilities are to lead a culture of good information management, own the overall information risk policy and procedures, and advise the Optalis Board on information risk. The SIRO should work closely with the DPO and with the Caldicott Guardian to ensure a complete understanding of risks. The SIRO's responsibilities can be summarised as:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers
- Owning the overall information risk policy and risk assessment processes for Optalis and ensuring they are implemented consistently by Information Asset Owners (IAOs)
- Advising the Chief Executive or relevant accounting officer on the information risk aspects of his/her statement on internal controls
- Owning the information incident management framework for Optalis
- Optalis are required to ensure their appointed SIRO possesses the necessary knowledge and skills to undertake their role effectively and to provide periodic, evidenced statements of information assurance to their organisation's accounting officer for the annual *Statement of Internal Control*
- Associating tasks with appropriate management levels
- Avoiding unnecessary impacts on day-to-day business

- Ensuring that all the necessary activities are discharged in an efficient, effective, accountable, and visible manner

The Caldicott Guardian

The Caldicott Guardian (CG) is a member of the corporate management team with professional care experience and an understanding of how care information is processed and shared between Optalis and its partnerships. The CG works closely with the SIRO and DPO on data protection and Caldicott matters:

- Ensuring Optalis managers and staff protect the confidentiality of personal information and share information with partners in compliance with the Caldicott Principles and the Optalis Code of Conduct (within the HR Library)
- Acting as the Optalis 'conscience' on the ethical and lawful use of personal information
- Agreeing, monitoring and reviewing detailed information sharing protocols governing the Optalis sharing of service user confidential information with partners, e.g., NHS and care home services, and other partners
- Overseeing care processes by documenting data flows and process flows
- Ensuring managers and staff receive support to enable them to be made aware of their Caldicott responsibilities through policies, procedures, and training
- Providing routine reports to senior management regarding information sharing issues; and maintaining a log of all requests for assistance received and responses/advice given

Information Asset Owners (IAO)

An Information Asset Owner (IAO) is a senior member of staff who is the nominated owner for one or more groups of identified information assets. IAOs will work closely with the SIRO to ensure there are clear and complete asset ownership records. Also, they should have a clear understanding of responsibilities and asset ownership, especially where information assets are shared by multiple services. IAOs will support the SIRO by:

- Identifying, documenting, and monitoring what information assets are held, and for what purpose
- How information is created, amended or added to
- Define who has access to each asset and why
- Understand and address risks to assets
- Provide regular reports and asset registers to the SIRO

6. Risks

Optalis recognises that there are risks associated with the capture and processing of personal information to conduct its business. This policy aims to mitigate risks, including improper collection and use of personal data, unauthorised sharing/disclosure of personal data; inadequate protection of stored personal data; inaccurate retention of personal data that is no longer required; the inaccurate input of personal data.

Non-compliance with this policy could hold significant risk to operational efficacy and may result in financial penalties imposed by the Information Commissioner, damage to Optalis' reputation, and to loss of trust by the public and our service users/clients.

Under the Data Protection Legislation the maximum fine for a serious violation of the Law becomes the sterling equivalent of €20 million or 4% of worldwide turnover, whichever is the higher. In addition, the DPA 2018 brings criminal offences up to date, e.g. a new offence of altering records to prevent disclosure following a subject access request.

7. The GDPR/Data Protection Principles and Lawful Basis

In the course of their duties all Optalis employees; including contractors and volunteers, processing any personal data must comply with the data protection principles listed below. This includes working at home, workplace or off-site. Article 5 of the UK GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- Documented - the (data) controller shall be responsible for, and be able to demonstrate, compliance with the principles

Data Controllers must have a valid lawful basis before they process personal data. These are the different lawful bases:

- Consent
- Contract
- Vital interests to protect life
- Legitimate Interests
- Public task
- Legal Obligation

8. Definitions

General Data Protection Regulation (the GDPR): The original legislation is the EU Regulation (2016/679) by which the European Parliament, the Council of the European Union and the European Commission strengthened and unified data protection for all individuals within the European Union (EU). The UK Government have absorbed the new Regulation into the UK Data Protection Act 2018 (DPA) and, following the UK exit from the EU, also into the UK GDPR. The Information Commissioner has issued guidance documents on the different aspects of the legislation.

Purpose: The DPA says that: "Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes". What this means is that information gathered for one purpose cannot be used for another without the agreement of the individual concerned.

Processing: Processing means obtaining, recording, or storing personal data or carrying out any activity such as collecting, recording, amending, storing, destroying, rearranging, and extracting information by any means. Basically, if you are doing anything with data you are processing it.

Personal data: Information about a living individual which can easily identify them and other information, which is in, or likely to come into, the data controller's possession. It also relates to someone who can be directly or indirectly identified by reference to an identifier (e.g., NI Number, Paris ID)

Any of the following, and many more, could identify a person and constitute personal data: name; address; customer number; National Insurance Number or other reference number; biometric data (e.g. fingerprints); DNA; IP addresses; Internet cookies; images of individuals; signatures.

Special Category Data means personal data relating to -

- Racial or ethnic origin of the data subject
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- If a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Genetic data - inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample
- Biometric data - interactive technology such as mobile phones equipped with a fingerprint reader
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission by that person of any offence*
- Proceedings for any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings*

*Although personal data relating to criminal convictions and offences are not included under Article 9, similar extra safeguards apply to its processing (see Article 10).

Data Protection Officer (DPO): A mandatory role for Optalis. Provides specialist support and advice on data protection and GDPR obligations. Decides when it is necessary to report a data breach to the ICO, and acts as the point of contact with the ICO.

Data controller: A natural or legal person, public authority agency or other body which, alone or jointly with others determines the purposes for which and the way in which any personal data are, or are to be, processed. Optalis is the Data Controller and may be joint controller with local authorities.

Data processor: A person or organisation who deals with personal data, as instructed by a controller, for specific purposes and services offered to the controller that involve personal data processing.

Data subject: A living individual who is the subject of personal information (data).

Data protection principles: Six principles that underpin the data protection legislation.

Privacy notice: The oral or written statement that individuals are given when information about them is collected. A more accessible description is “how we use your information”. In general terms, a privacy notice should define the purpose or purposes for which you intend to process the information; and any extra information you need to give individuals in the circumstances to enable you to process the information fairly.

Data Protection (Privacy) Impact Assessment: A data protection impact assessment (DPIA) is a process to help identify and minimise data protection risks of a project, certain listed types of processing, or any other processing that is likely to result in a high risk to individuals’ interests. It is also good practice to do a DPIA for any major projects which process personal data. See OPS13a DPIA Procedure and related templates.

9. Service users and their rights

Optalis holds a large amount of personal and sensitive data. Loss or damage of this data could have serious implications for the individual whose data has been breached as well as pose a reputational and operational impact to Optalis. Everyone working on behalf of Optalis has a responsibility to safeguard data appropriately. The Optalis commitment is to ensure that:

- Information provided to Optalis is maintained accurately and kept up to date
- Personal data is stored securely, disposed of safely, and appropriately secured when in transit
- Optalis will only use the information for the purpose it was gathered
- Every member of staff is informed and can both confirm and articulate a full understanding of their responsibilities under the Data Protection Legislation
- Optalis provides training and support to staff, Board members, contractors, agency workers and volunteers
- Every member of staff understands that they must keep information secure, e.g., passwords or access codes must not be shared
- All contracts with third parties will include an agreement to abide by the Data Protection principles and provide sufficient assurances in respect of any personal data the contractor may hold on our behalf
- Managers and staff are aware that they must provide a secure environment for handling personal information when working at home or in locations away from their normal workplace

10. Individual Rights

Individuals have legal rights in relation to the personal data held about them. These include **the right to**:

- Be informed, and know why/how their data is being processed
- Have access to their personal data
- Rectify inaccuracies
- In certain circumstances, the right to have their information erased, to restrict processing, and to object to processing; the right to object to direct marketing is absolute
- Data portability (request information they have provided in a useful electronic format)
- Have human intervention when automated decision-making or profiling is used

- Make a complaint to the Information Commissioner for investigation
- Seek compensation for damage or distress arising from any breach of the Data Protection Legislation

11. Data Subject Access Requests (DSARs)

Individuals have a legal right to request a copy of the information held about them. These elements are covered in the Privacy Notice; these include:

- To be informed as to whether any personal data is being processed
- To be given a description of the personal data
- To be informed of the reasons the data is being processed
- To be informed as to whether and with whom the data will be shared
- To be provided with a copy of data and details of the source data; where available

Requests can be made verbally through:

- Social media
- By a third party
- In person
- In writing
- Via email

The **requests should be formalised as quickly as possible through the Information Governance Team** by using the email address subjectaccessrequest@optalis.org.

12. Information Sharing

In general, information will normally only be shared for legally justified reasons or with the consent of the data subject. **However, where a vulnerable adult is at risk of harm, or where there is wider crime prevention or public safety implications or such action would prejudice any subsequent investigation, information may need to be shared without consent**. This information should be shared on a 'need to know' basis only.

In 2014 SCIE (Social Care Institute for Excellence) reinforced this message by publishing seven golden information sharing principles that were originally shared by HMG:

1. Remember that the Data Protection Act is **not a barrier to sharing information but provides a framework** to ensure that personal information about living persons is shared appropriately

2. **Be open and honest** with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be, shared, and seek their agreement unless it is unsafe or inappropriate to do so
3. **Seek advice if you are in any doubt**, without disclosing the identity of the person where possible
4. **Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information**. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case
5. **Consider safety and wellbeing**: base your information-sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions
6. Necessary, proportionate, relevant, accurate, timely and secure**: ensure that the information you share is necessary for the purpose for which you are sharing it**, is shared only with those people who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely
7. **Keep a record of your decision and the reasons for it** – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

13. Data Retention and Disposal

The Data Protection Legislation requires that personal data is not kept for longer than is necessary for its purpose unless it's required to be kept for longer by statute. The ICO guidance is that you must:

- Review the length of time you keep personal data
- Consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it
- Securely delete information that is no longer needed for this purpose or these purposes
- Update, archive or securely delete information if it goes out of date

You should reference OPS61 Record Retention & Destruction Policy when considering retention and disposal. Optalis also has a detailed Retention Schedule which can be accessed through the DPO – dpa@optalis.org

At the end of the retention period, personal data **should be reviewed and deleted**. It **must be disposed of appropriately**.

Information containing any personal information **must be shredded or incinerated** and electronic data **must be destroyed by reformatting or overwriting the hard drive**; a process supported and driven by Optalis ICT provider – Wokingham Borough Council, as stated within their policies.

14. Information Security - Keeping Information Secure

Staff Accountabilities

Normal email sent over the **Public Internet** is **not secure**. It has been compared to sending a postcard through the mail. Anyone who comes into contact with the email can read it and misuse the information it contains.

Care must be taken to **ensure that that data is not accidentally sent to the public domain**. Before sending e-mails always double check that the information being sent is up to date, accurate, the minimum details necessary, and it is being sent to the correct address/addresses.

Optalis staff are reminded that normal email sent over the Public Internet carries higher risks. If personal data is sent this way, **it must have additional protection**, e.g., by using password-protected attachments.

When sending emails, staff **must be considerate of the content and 'trail' of content**, ensuring that any previously visible information is appropriate, relevant and professional, e.g. not subjective, of a personal nature or in inappropriate. It is good practice to ensure that the **subject is aligned to the content**, if it is not, the recommendation is to begin a new email focussing the content to the subject – this avoids:

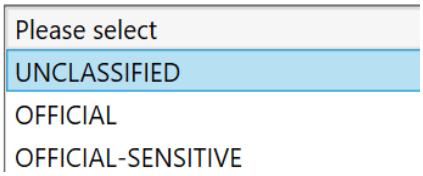
- Unnecessary sharing of information
- Reduces **potential breach** implications
- Ensures **appropriate** communication
- Focuses the content against the specific **subject**
- Reduces the **potential for disciplinary action**

Email

Wokingham Borough Council (WBC) and the Royal Borough of Windsor and Maidenhead (RBWM) have invested in high security email services. WBC and RBWM email can be used to exchange Client-based or financial information with another person or organisation who is part of the Government network. This includes:

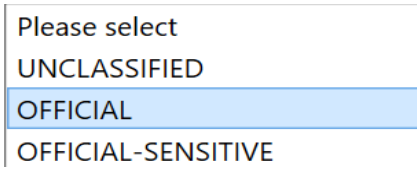
- Central government departments
- Local authorities
- NHS
- Police

"OFFICIAL" or "OFFICIAL-SENSITIVE" emails should be used to send or receive official information or sensitive information that is Client-based or financial to another person or organisation (e.g. Schools, transport providers and parents, law firms, etc.) this can be assured by selecting the appropriate choice of '**protective marking**':



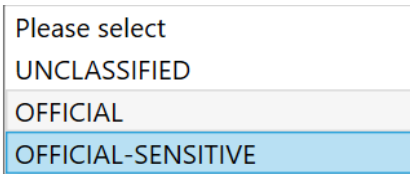
By selecting **UNCLASSIFIED**, you are confirming if the data included within this email is disclosed, lost, stolen and misused, there would be;

- Little or no impact on the finances of the Authority
- No inconvenience or distress to the customer
- Little or no financial impact to the customer
- Little or no impact on the Authority's standing or reputation



By selecting **OFFICIAL**, you are confirming if the data included within this email is disclosed, lost, stolen and misused:

- Short-term inconvenience, harm or distress to an individual
- Cause financial loss or loss of earning potential, or to facilitate improper gain
- Damage to the Council's standing or reputation
- Financial impact to the Council
- Breach proper undertakings to maintain the confidence of information provided by individuals or third parties
- Breach statutory restrictions on the disclosure of information

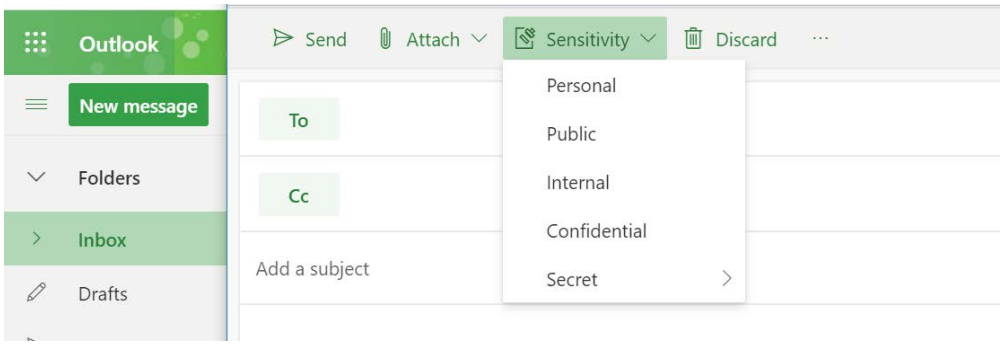


By selecting **OFFICIAL-SENSITIVE**, you are confirming if the data included within this email is disclosed, lost, stolen and misused:

- Substantial inconvenience, harm or distress to individuals
- Cause financial loss or loss of earning potential, or to facilitate improper gain or advantage
- Substantial damage to the Council's standing or reputation
- Significant Financial impact to the Council (Millions)
- Prejudice the investigation of or facilitate the commission of low-level crime, hinder detection of serious crime

Webmail

Webmail enables a different view and alternative options that do not restrict the email being sent. However, these options **must be considered with the same level of risk and accountability**, and therefore used with the same consideration:



Password Protection

Good practice standards for this important information security topic include:

- Users must take sufficient precautions to maintain the security of their passwords. Passwords must not be disclosed to or shared with anyone
- All passwords are to be treated as sensitive, confidential information
- Passwords should not be written down and left accessible, nor given to others to use under any circumstances
- Do not speak about a password in front of others, or hint at the format of a password (e.g., "my family name")
- If someone demands a password, refer them to your Manager
- If an account or password is compromised or suspected of being compromised, report the incident to IT Support immediately and ask them to block access. Also, inform your line manager or service manager

Anonymisation and pseudonymisation of data

Both physical and electronic personal data must be sufficiently protected. Anonymisation and pseudonymisation give substantial protection to personal data and should be considered wherever possible. Data protection law does not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. Fewer legal restrictions apply to anonymised data.

We cannot always make personal data totally anonymous as to carry out our functions we need to know who the data relates to. However, if the information is being used for statistical purposes you must ensure that it is anonymised through the removal of any identifiers. This includes codes such as Paris / Mosaic IDs and employee numbers as they can still be used along with other information to make the information identifiable.

Pseudonymisation is a procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. A single pseudonym for each replaced field or collection of replaced fields makes the data record less identifiable while remaining suitable for data analysis and data processing. The 'key' to the data must be kept separately.

For example, an extract is made from Paris of the health information of all customers over 70 years old. The names, dates of birth, and addresses are removed but the Paris ID is left on the extract. The extract is now pseudonymised; without the additional information associated with the ID, which is held separately on Paris, individuals cannot be identified.

Pseudonymisation **must** be considered when sharing information outside the organisation as it adds an additional layer of security.

Storage of personal data

Both physical and electronic personal data must be sufficiently protected. Good practice standards include:

- All personal data must be accessible only by those authorised to do so
- Sensitive, physical data (or data held on removable devices such as CD/DVD, flash drives etc.) must be either kept in lockable filing cabinets, locked cupboards, or drawers, or in restricted access rooms
- For electronic information, access must be controlled by passwords, encryption, and access authorised levels logins
- There must be regular backups to ensure that important data cannot be lost as the result of computer hardware problems
- Computers should not be left unattended. Lock your computer if moving away from it
- Have a clear desk policy. Clear your desk every day before you leave the office, making sure personal and confidential documents are not left lying around on your desk overnight
- Cleaners could access to personal and sensitive information they are not authorised to see. Lock them away each evening before you leave

- For officers working in public areas, please ensure that screens are not in view of the public and that a suitable directional filter is applied to the screen if regularly working with sensitive or personal data (i.e. in reception areas)

Use of Fax Machines

Fax machines are rarely used nowadays and should only be used in exceptional circumstances. This is because fax machines present a higher security risk as documents can be left uncollected, or the wrong number dialled.

If you must use fax, then you should follow good practice including:

- Ensure there are appropriate levels of security in effect for the receiver fax
- Before sending any fax transmission call the recipient to confirm the fax number
- Ensure that someone will be at the fax machine to receive it (if not pin activated)
- Obtain confirmation from the intended recipient that the fax has been received

Remote Working

Care must be taken when laptops, smartphones or any other electronic devices are used to process personal data away from the Optalis' offices. The secure network should be used at all times and no information stored on local drives.

Information displayed on your screens should not be able to be viewed by members of the public, members of the family or any unauthorised person. Keep all personal information secured and protected by using secure passwords. Refer to **OPS13-2 Remote Working** (Home Working).

15. Training Statement

All staff should be asked to read the policies relating to data protection as part of their induction process. Training in data capture and how to check/correct the quality of data should be given to all staff. All staff using IT systems should be thoroughly trained in its use. Staff must complete the required training or eLearning, e.g., 'Introduction to Data Protection' and 'Information Security' through the MyLearningCloud training system.

16. Contact Details

For all Information Governance & Data Protection Queries: DPA@Optalis.org

Trinity Court
Molly Millars Lane
Wokingham, RG41 2PY

17. Related Optalis Policies

OPS10 Business Continuity Plan
OPS13a Data Protection Impact Assessment
OPS13-2 Remote Working (Home Working)
OPS13-G1 Remote Working (Home Working)
OPS16 Consent
OPS22 Good Governance
OPS29 Information Security
OPS30 Information Sharing Principles
OPS37 Compliance of Records Management
OPS61 Record Retention & Destruction
OPS68 Information Governance
OPS70 Security Incident
OPS70-F1 Security Incident Reporting Form
OPS70-F2 Security Incident Risk Assessment
OPS71 Information Asset Management
OPS72 Caldicott Guardian
HR001 Disciplinary Policy and Procedure

Wokingham Borough Council (WBC) policies:

WBC Information Security and Acceptable Use of ICT Policy
WBC Conduct Policy (email usage)
WBC Data Protection Policy

Royal Borough of Windsor and Maidenhead policies:

RBWM Security Information and Use of Technology Policy
RBWM Security Policy (use of email)
RBWM Data Protection Policy

18. References

ICO Guide - Data Protection Act 2018
Central Government - Guide to Data Protection Act 2018
ICO Guide - General Data Protection Regulations
New GDPR - Lawful Bases for Processing
ICO Consultation - Data Processing Impact Assessments
DPA 2018 - Subject Access Request Procedures

GDPR Guidance - Changes to Subject Access Request Procedures
DPA Guidance - Data Retention and Disposal