Policy 56 the handling, storage and disposal of Disclosure of Information.

Data Protection and Access to Records

ONCE Healthcare Ltd processes personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This includes information collected during recruitment and ongoing compliance, such as:

- Identity verification and proof of right to work in the UK
- Qualifications, training records, and professional registration
- Disclosure and Barring Service (DBS) checks
- Health declarations and occupational health clearance
- References, contracts, and assignment history

This information is stored securely and only accessed by authorised personnel. Data may be shared with regulatory bodies (e.g., RQIA), client organisations, or auditing entities strictly for lawful purposes, such as safeguarding, placement suitability, or regulatory inspections.

Work-seekers have the right to request access to their data and can also request rectification or erasure where legally permissible. Some data must be retained for specific periods to meet our legal or contractual obligations.

Your Rights

You have the right to:

- Request access to the personal data we hold about you
- Request correction of any incomplete or inaccurate data
- Request erasure of personal data where no legal basis exists for its retention
- Restrict or object to certain types of processing
- Be informed of any data breaches that may impact your rights
- Lodge a complaint with the Information Commissioner's Office (ICO)
- Request portability of your data where applicable

All requests will be verified and responded to within statutory timeframes.

Confidentiality

All staff are bound by a duty of confidentiality. Personal information about patients, clients, or colleagues must never be shared with unauthorised individuals. This includes verbal, written, or electronic disclosure.

- Breaches of confidentiality include:
- Discussing service users with friends, family, or on social media
- Sharing care notes, photos, or medical information without consent
- Accessing records without legitimate reason
- Any breach will lead to disciplinary action, including potential removal from the agency register and referral to professional bodies such as the NMC or NISCC.

Contact

info@oncehealthcare.com

(+44)7802469064

oncehealthcare.com

Company number: NI727513

Foundry 8, City East Business Centre, 68-72 Newtownards Road BT4 1GW

oncehealthcareltd oncehealthcare ONCE Healthcare Ltd ONCE Healthcare Ltd

If you witness a breach, you must report it immediately to the Officer on Call or the Registered Manager.

Data Protection Officer

ONCE Healthcare Ltd has formally appointed **Marvi Santos** as the organisation's Data Protection Officer (DPO).

As DPO, Marvi is responsible for:

- Monitoring ONCE Healthcare Ltd's compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018
- Advising the organisation and its staff on data protection obligations
- Overseeing responses to subject access requests and liaising with the Information Commissioner's Office (ICO) where necessary
- Managing and investigating personal data breaches
- Ensuring that appropriate data protection policies and procedures are implemented and regularly reviewed

Marvi operates independently in this role and is supported by ONCE Healthcare Ltd to perform these duties without conflict of interest or undue influence.

Any queries or concerns related to data protection should be directed to:
msantos@oncehealthcare.com

Caldicott Principles

ONCE Healthcare Ltd requires all staff to follow the Caldicott Principles when handling confidential service user information during placements in care homes or other healthcare settings. These principles ensure that personal data is used appropriately, lawfully, and with respect for individual privacy.

Staff must adhere to the following eight principles:

- Justify the purpose – Every use or disclosure of confidential information must have a clear and lawful reason.
- Don't use personal data unless necessary – Only use identifiable information when absolutely essential.
- Use the minimum necessary – When using personal data, limit the amount to what is strictly required.
- Access on a need-to-know basis – Only those involved in the direct care or support of the individual should access their information.
- Understand responsibilities – All staff are responsible for maintaining confidentiality and must complete data protection training.
- Comply with the law – Personal data must be processed in accordance with UK GDPR, the Data Protection Act 2018, and RQIA requirements.

The duty to share can be as important as the duty to protect – When sharing information is necessary for safe and effective care (e.g., safeguarding), it must be done appropriately.

Be transparent – Individuals should be made aware of how their information is used and their rights to access it.

Breach of these principles will result in disciplinary action and may lead to referral to professional regulatory bodies (e.g., NMC, NISCC).

Contact

info@oncehealthcare.com
(+44)7802469064
oncehealthcare.com
Company number: NI727513

Foundry 8, City East Business Centre, 68-72 Newtownards Road BT4 1GW

oncehealthcareltd oncehealthcare ONCE Healthcare Ltd ONCE Healthcare Ltd

Office Use Only

Document History

Revision	Date	Created by	Changes made

Contact

info@oncehealthcare.com

(+44)7802469064

oncehealthcare.com

Company number: NI727513

Foundry 8, City East Business Centre, 68-72 Newtownards Road BT4 1GW

oncehealthcareltd oncehealthcare ONCE Healthcare Ltd ONCE Healthcare Ltd