# Data Security and Protection Toolkit policy

## 1. Objectives

1.1 To raise awareness and competency within Xander Recruitment Group around the requirements of the Data Security and Protection Toolki:

- To ensure that those with role-specific duties are aware of how this affects their role
- To ensure that, where required, those with specific roles and requirements receive appropriate training
- To ensure that all staff receive induction and ongoing training with regards to Data Security and Cyber Protection
- To ensure safe, secure data sharing with the NHS

**1.2** To ensure that there is a clear Data Security and Protection Toolkit 'roadmap' for Xander Recruitment Group, using:

- Guidance and templates for meeting the required ten standards
- Template for audit and spot checks
- A checklist for those working from home to ensure compliance

## 2. Policy

**2.1** The Data Security and Protection Toolkit is an online self-assessment tool that Xander Recruitment Group and all social care providers must use if they have access to NHS patient data and systems.

As a result of this requirement, Xander Recruitment Group recognises the importance of data security and cyber protection and is committed to maintaining systems that support confidentiality and the wider understanding of how data must be managed.

There are two stages on the pathway:

- Approaching Standards
- Standards Met

**2.2** The Data Security and Protection Toolkit allows Xander Recruitment Group to measure its performance against the National Data Guardian's 10 Data Security Standards. The standards are organised under 3 leadership obligations which are:

**People**

Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles

- **Standard 1:**
    - All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes

- **Standard 2:**
    - All staff understand their responsibilities under the National Data Guardian's Data Security Standards including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches

- Standard 3:
    - All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Test

Process

Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses

- **Standard 4:**
    - Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access data to personal confidential data on IT systems can be attributed to individuals

- **Standard 5:**
    - Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security

- **Standard 6:**
    - Cyber attacks against services are identified and resisted and care CERT security advice is responded to. Action is taken immediately following a data breach, also known as a near miss, with a report to senior management within 12 hours of detection

- **Standard 7:**
    - A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management

Technology

Ensure technology is secure and up to date

- **Standard 8:**
    - No unsupported operating systems, software or internet browsers are used within the IT estate

- **Standard 9:**
    - A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This reviewed at least annually

- **Standard 10:**
    - IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards

**2.3** Xander Recruitment Group does provide care through the NHS Standard Contract and so our compliance is in line with the new Data Security and Protection (DSP) toolkit.

This ensures that we demonstrate best practice and ensure compliance with the 10 Data Security Standards:

**2.4** The Care Quality Commission includes a focus on the use of technology and sharing information for the benefit of the care to the individual.

Whilst the CQC prompts do not specifically reference the Data Security and Protection Toolkit (DSPT), they detail that providers should operate within a framework that demonstrates robust arrangements around the security, availability, sharing and integrity of confidential data, records and data management standards.

In November 2021, CQC introduced additional prompts that included information governance/use of technology, they include:

- Effective
    - How is technology and equipment used to enhance the delivery of effective care and treatment to support people's independence

- Responsive
    - How is technology used to support people to receive care and support quickly? Is the technology easy to use?

- Well-Led
    - Are information technology systems used effectively to monitor and improve quality of care?
- Well-Led
    - Does the service share appropriate information and assessments with other relevant agencies for the benefit of people who use the service

**4.5** It has been recognised that social care services such as Xander Recruitment group can be very different to health services, and this has been reflected in the revised approach to the Data Security and Protection Toolkit (DSPT) for social care.

The requirements for Social Care have been broken down in to four key areas within the DSPT.

- Staffing and Roles
- Policies and Procedures
- Data Security
- IT Systems and devices

# Data Security and Protection Toolkit policy

Each category will have a subset of requirements that, once completed, will enable Xander Recruitment Group to achieve “Standards Met” status.

**4.6** This policy and wider data security management are supported by a range of data protection policies in place.

This Data Security and Protection Toolkit (DSPT) policy will support Xander Recruitment group in understanding responsibilities with regard to data management and security. Completion of the Toolkit will support, compliance with data protection requirements and add to Xander Recruitment Group assurances regarding:

- Confidentiality
- Data Protection
- Cyber Security
- Information Governance
- Staff Training

**Alex Stockley - Managing Director – XANDER RECRUITMENT GROUP LIMITED**

**Date: March 2024**