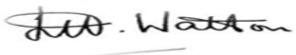
Information Security and Assurance Policy

Approved by Governors: November 2016

Chair of Governors signature: 

1. Aim

1.1. Information is an important strategic asset of significant value to the Trust and needs to be protected from threats that could potentially disrupt business continuity.

1.2. The availability, confidentiality and integrity of the Trust's information and related information systems are essential to the success of its operation and administrative activities. It is also an important part of how we ensure we protect personal data and comply with our statutory obligations under the Data Protection Act 1998 which is overseen by the Information Commissioner (www.ico.org.uk)

1.3. This policy aims to develop a positive culture of information security throughout the Trust and to bring together the current sources of policy, procedure, guidelines and information security related regulations, making it easier for staff (wherever they are based) and members of the Trust to understand their responsibilities.

2. Objectives

The main objectives of this policy and its related documents are:

2.1. To ensure that all of the Trust's computing facilities, network and equipment are adequately protected against loss, misuse or abuse.

2.2. To ensure that all users* are aware of and fully comply with this policy statement and all associated policies.

2.3. To ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.

2.4. To ensure that the Trust's requirements for information and information systems will be met.

*Users includes pupils, students, staff members and Trustees.

3. Principles

The following principles govern the Trust's information security approach:

3.1. The Trust is committed to appropriately secure its information and related information systems in compliance with related information security legislation and good practice standards.

3.2. Information will be used only for legitimate business operation purposes, will be protected against unauthorised access and integrity attacks and will be available when needed.

3.3 Business continuity plans for mission critical activities will be produced, maintained and tested.

3.4. The Trust believes that information security is the responsibility of all users. Every person handling information or using the Trust's information systems is expected to observe and comply with all Trust policies and procedures, and to take into account the agreed guidelines.

3.5. User access rights will at all times be based on a person's role and need rather than their status. Access rights will be reviewed at regular intervals and revoked if necessary.

3.6. The Trust will constantly review and seek to improve its information security status.

3.7. The Trust will seek to build and maintain a culture of information security awareness amongst its users. This will be achieved by promoting user education rather than technology enforcement, and only where necessary impose solutions or systems to enforce best practice.

3.8. The Trust will promote computer security awareness by publishing a suite of ICT policies and user guides and by alerting its users on major computer security risks or vulnerabilities.

3.9 All breaches of information security, actual or suspected, will be reported to and investigated by the Trust.

4. Supporting Documents

- Information Strategy
- Data Protection Policy
- Data Security Breach Policy
- Records Management Policy
- Archiving Policy
- Publication Scheme
- ICM Plan
- Risk Management Policy & Register
- NET ICT policies and procedures