ICT SECURITY POLICY

This policy applies to all the academies in The Lionheart Academies Trust

Version	Document History	Date
Version 1.0	Initial Document	01/10/2010
Version 1.1	Revised by Director IT	14/11/2016
Version 1.2	Draft issued for review	15/11/2016
Version 2.0	Approved by Trust Board and issued to all schools	18/11/2016

Signed by Chair of Board:_____

1. Purpose

1.1 The continued confidentiality, integrity and availability of information systems underpin the operations of the Lionheart Academies Trust. A failure to secure information systems would jeopardise the ability of the Trust to fulfil its mission of 'Academic Excellence and Holistic Development for all'. This woud also have a greater long term impact through the consequential risk of financial or reputational loss.

1.2 This ICT Security Policy provides the guiding principles and responsibilities of all members of the Trust required to safeguard its information systems. Other supporting Trust policies, procedures and guidelines will give greater detail on specific subject areas.

1.3 The IT Support Teams at each site will lead the Trust's commitment to deliver a successful implementation of this ICT Security Policy but this will only be possible if all members of the Trust community are aware of, and carry, out their own personal responsibilities

1.4 The intention of this policy is to:

i) Ensure that the information systems that the Trust manages are protected from security threats and to mitigate risks that cannot be directly countered

ii) Ensure that all members of the Trust are aware of and able to comply with relevant UK and EU legislation

iii) Ensure that all users are aware of and understand their personal responsibilities to protect the confidentiality and integrity of the systems that they access

iv) Ensure that all users are aware of and are able to comply with this policy and other supporting policies

v) Safeguard the reputation and business of the Trust by ensuring its ability to meets its legal obligations and to protect it from liability or damage through misuse of its IT facilities

vi) Ensure timely review of policy and procedure in response to feedback, legislation and other factors so as to improve ongoing security.

2. Policy

2.1 This ICT Security Policy applies to all members of Staff within the Lionheart Academies Trust ("the LAT"). For the purposes of this policy, the term "Staff" means all members of LAT staff including permanent, fixed term, and temporary staff, governors, secondees, any third party representatives, agency workers, volunteers, interns, agents and sponsors engaged with the LAT in the UK or overseas. This policy also applies to all members of staff employed by any of the LAT's subsidiary companies.

3. ICT Security Principles

3.1 The following principles form a framework for the security and management of the Trusts information and systems:

i) **Principle 1**: All individuals covered by the scope of this policy must handle information and systems appropriately in accordance all Trust policies.

ii) **Principle 2**: ICT Systems should be only available to those with a legitimate need for access.

iii) **Principle 3**: ICT Systems will be protected against unauthorised access.

iv) **Principle 4**: ICT Systems will be protected against information loss and corruption.

v) **Principle 5**: Personal data shall not be kept for longer than necessary.

vi) **Principle 6**: Breaches of policy must be reported by anyone aware of the breach in a timely manner.

4.0 Roles and Responsibilities

4.1 Individuals must adhere to the Acceptable Use Policy and follow relevant supporting procedures and guidance. An individual should only access systems and information they have a legitimate right to and not knowingly attempt to gain illegitimate access to other information. Individuals must not aid or allow access for other individuals in attempts to gain illegitimate access to data or systems. In particular individuals should adhere to the information security 'dos and don'ts' outlined in the table below:.

4.2

DO	DON'T
Do use a strong password and change it if you think it may have been compromised	Don't disclose your password to anyone
Do report any loss or suspected loss of data	Don't reuse your system password for any other account
Do be on your guard for fake emails or phone calls requesting confidential information - report anything suspicious to the IT Team	Don't open suspicious documents or links
Do ensure Trust equipment is regularly taken into your home site so that security and anti-virus updates can be applied	Don't undermine or seek to undermine the security of Trusts ICT systems
Do be mindful of risks using public Wifi or open-access computers	Don't provide someone else with access to Trust information or ICT systems
Do ensure Trust data is stored on Trust systems	Don't copy confidential information without permission
Do password protect and encrypt your personally owned devices	Don't leave your computers or phones unlocked
Do seek advice from the IT Support Team if you are unclear about any aspect of information security.	Don't use a personal email account for conducting Trust business.

4.3 The trust is responsible for ensuring that existing information systems are maintained in line with manufacturer and industry recommendations. This responsibility includes:

i) Provision and maintenance of an enterprise wide anti-virus solution

ii) Ensuring that all software and licensed products used within the Trust comply with the Copyright, Designs and Patents Act 1988, the Trust may carry out checks from time to time to ensure that only authorised software products are being used.

iii) Monitoring of electronic communications within the guidelines set down by the Regulation of Investigatory Powers Act 2000 (RIPA). The guidelines cover, but are not limited to, monitoring for criminal or unauthorised use, viruses, threats to Trust systems e.g. hacking or denial of service attacks.

iv) Provide end-user advice and guidance on understanding security risks.

5. Review

5.1 This policy will be reviewed periodically as it is deemed necessary to ensure that it remains appropriate and up to date. These reviews will be no less frequently than every two years. The policy review will be undertaken by the Director of IT for the LAT and ratified by the LAT Board.