ICT Acceptable Use Policy (AUP)

This policy has been approved by the SMTand any amendments to it require the SMT's approval.
Approval:

December 2016

1. Introduction
1.1 This policy defines a framework by which ALRA's computer systems, assets, infrastructure and computing environment will be protected from threats whether internal, external, deliberate or accidental.

2. Key Principles
2.1 All central computer systems, environments and information contained within them will be protected against unauthorised access.
2.2 All use of the school's IT facilities will comply with the handbook usage guides.
2.3 Information kept within these systems will be managed securely, to comply with relevant data protection laws and to satisfy expectations that such assets will be managed in a professional, safe and dependable manner.
2.4 All members of the schoolare required to familiarise themselves with this policy, to adhere to it and comply with its requirements.
2.5 Heads of Department and line managers have a responsibility for ensuring the implementation of, adherence to and compliance with this policy throughout their areas of functional responsibility.

3. The Computing Environment
3.1Computing resources not owned by the schoolmay be connected to the school'snetwork. However, all such resources must comply with Guidance governing the use of computing resources.

3.2ALRAreserves the right to monitor, log, collect and analyse

the content of all transmissions on ALRA networks at any time deemed necessary for performance, fault diagnostic and IT compliance purposes.

4 Physical Security

4.1 Any computer equipment in general office environments should be secured behind locked doors or protected by user logout and or password protected screensavers whenever it is left unattended; and outside of general office hours.

4.3Any portable equipment (such as laptops, memory sticks, CDs, PDAs etc) should use a logon or power-on password wherever possible. Any unattended portable equipment should be physically secure, for example locked in an office or a desk drawer. When being transported in a vehicle they should be hidden from view. Staff should avoid storing sensitive information on portable equipment whenever possible (see data security section, at 5. below).

4.5 Staff who store confidential information on Schoolowned portable equipment must ensure that such data is thoroughly and securely cleansed from that equipment when they leave the school's employment.

5. Data Security
5.1 The schoolattaches great import to the secure management of the data it holds and generates and will hold staff accountable for any inappropriate mismanagement or loss of it.

5.2 The schoolholds a variety of sensitive data including personal information about students and staff. If you have been given access to this information, you are reminded of your responsibilities under data protection law

5.3 The schoolprovides secure and practical remote access to information and

6. Prevent
6.1 Users of ALRA ICT facilities must not: deliberately or unintentionally receive, access, create, change, store, download, upload, share, use or transmit:anyterrorist related or extremist material, or any data capable of being resolved into such material.This is a requirement ofthe University's Prevent Policies and the CounterTerrorism and Security Act 2015 as specified by guidance issued under s29 of the Act.