ITSERT Terms of Reference

Version Number 1.4

Effective from 01 February 2019

Author: Senior Information Security Officer

Information Governance, Quality Enhancement Office

1.0 Membership

Core roles

- Associate Director Digital Strategy Office (Chair)
- Information Governance Officer
- Information Security Officer
- Digital IT Operations Managers
- Digital IT Head of Service Delivery
- Digital IT Head of Applications
- Digital IT IT Security Manager (Plus Analyst)

Plus support resources as necessary

2.0 Frequency

Monthly as well as ad hoc meetings to respond to specific IT security incidents or investigation requests.

3.0 Responsibilities

3.1 These ITSERT Terms of Reference relate to ICT Acceptable Use Policy breaches, IT security and data loss incidents and associated investigation requests, as well as general ICT security analysis, activity, web filtering and vulnerability reporting. It is a subsidiary / supporting document to the ICT Acceptable Use Policy

3.2 The target audience for this document is members of Digital IT, QEO Information Governance and other staff who carry out system administrator functions with access to system logfiles.

3.3 This document does not currently constitute a Security Incident Response Plan. Major Security Incident Response Plans will be developed as an essential component of the University Cyber Security Strategy and will correspond with the University Emergency Planning approach.

3.4 The ITSERT will act as gatekeeper to ensure that the response to Policy breach or IT security incident and any subsequent investigation is co-ordinated, accountable and justified and that it is not a disproportionate invasion of privacy or overuse of Digital IT resources. All use of ICT facilities is logged and may be subject to monitoring. Monitoring is proportionate to the assessed risk to University ICT infrastructure and information systems. Monitoring may take place, to facilitate, academic and pastoral care by ensuring that students not using electronic systems vital for study are identified and encouraged to do so and thereby not fall behind or drop out. Monitoring is carried out in compliance with applicable obligations under the General Data Protection Regulation, Data Protection Act 2018 and the

Regulation of Investigatory Powers Act 2000 (and associated Telecommunications Regulations) for the purposes of:

- Preventing or detecting criminal activities
- Investigating or detecting unauthorised use of the University's ICT facilities
- Ascertaining compliance with regulatory or self-regulatory practices, procedures and standards
- Ensuring effective system operation.

3.5 Records of all ICT activity (including access to University ICT activities when using personally owned computers or mobile devices) are retained in accordance with the University Records Retention Schedule.

3.6 Where investigations relating to named individual's accounts / individual's use of ICT facilities are deemed necessary, an IT Account Investigation Request Form (see Related Documentation) must be completed and subject to appropriate discussion and approvals to proceed i.e. no form means no investigation. In the event of security vulnerability reports or infringement notices, routine investigation of network activity logs will be carried out without recourse to the IT Account Investigation Request form.

3.7 The ITSERT will:

a. Use a systematic approach to the storage, handling and analysis of ICT activity logfiles and digital evidence. Taking an image to investigate and avoiding where possible amendments to the original - access to digital evidence, whether viewing or otherwise accessing can alter date stamps and render the evidence inadmissible and will be considered as a disciplinary offence.

b. Investigate and present findings in a clear and understandable manner that are reliable and rigorous enough to be admissible in a formal dispute or legal process (such as disciplinary, misconduct allegations, or police requests).

c. Take appropriate action to protect the University network (in accordance with the ICT Acceptable Use Policy) by: blocking; disabling or enabling IT accounts; network connections; disconnecting or where relevant removing computer equipment from the network.

d. Not carry out forensic analysis of University IT equipment. The ITSERT will arrange for forensic analysis (where appropriate to the investigation and available budget) to be carried out by suitable and approved forensics company (with up to date accreditation, skills and experience).

e. Ensure that ICT activity logfiles and investigations are treated with the strictest confidence, stored securely and shared only with those who need to be involved in the investigation or outcome reports.

3.8 If, during an investigation any information warrants escalation to the relevant law enforcement agency (or statutory body), the ITSERT will undertake this action and

advise the CIO, Associate Director Digital Strategy Office (ITSERT Chair) and Director of Legal & Compliance before referring the matter to law enforcement.

Document Control Information				
Owner Associate Director Digital Strategy Office		**Reason for Development** Revised Terms of Reference which specify remit of the ITSERT in supporting IT investigations as referred to in the ICT AUP		
Equality Assessment		**Submitted Jan 2019**		
Revision History (published versions)				
Date	**Author**	**Summary of Changes**	**Version**	**Authorisation (Board & Date)**
Jan 2019	C Price	Updated to reflect organisational changes and to incorporate section on monitoring ICT activity.	V1.4	DIT Associate Director Digital Strategy: 30/01/2019
May 2015	C. Price	Update of organisational structures and published separately to the ICT AUP (4.1.) within University Policy pages	V1.3	CIO: 18/11/2015 Director LPG: 09/12/2015 ITMG: 30/09/2015 (same time as AUP V4.1 approval)
Dec 2013	C.Price	Updated to reflect organisational changes. First published as part of ICT AUP.	V1.2	CIO & University Secretary: 17/12/2013
March 2008	C. Price & M. Hilditch	New document to specify remi of ITSERT approved by Director Information Services Division	V1.0	Director ISD and ISD SMT: 02/05/2008
Review Due		2 years by January 2021		
Document Location		University Policy & Procedure pages (IT section) University Policy pages: http://www.salford.ac.uk/policies		