# University of Liverpool

## Security Investigation Policy

(User Investigations and Information Access Requests)

| | |
|---|---|
| **Reference Number** | CSD-013 |
| **Title** | Security Investigation Policy |
| **Version Number** | v1.2 |
| **Document Status** | Active |
| **Document Classification** | Open |
| **Effective Date** | 22 May 2014 |
| **Review Date** | 28 March 2018 |
| **Author** | Computing Services Department (David Hill) |
| **Approved by** | Corporate Services & Facilities Committee (Nov 2012) |
| **Implemented by** | Information Security Officer |
| **Monitoring of compliance** | Faculty Information Security Managers (Local)<br>CSD Information Security (Central) |
| **Comments** | **This document should be read in conjunction with the Information Security Incident Response Policy**<br>• **22/05/2014 - Annual Review/Update v1.0 – v1.1**<br>• **31/07/2015 – Annual Review/Update v1.1 – v1.2**<br>• **29/07/2016 – Annual Review**<br>• **28/03/2017 – Annual Review** |

# Security Investigation Policy

## Table of Contents

## 1. Introduction

Information is a vital asset to any organisation, and this is especially so in the University which is a knowledge-driven organisation. Virtually all of our activities create information assets in one form or another. The Information Security Policy and its associated policies are concerned with managing the information assets owned by the University and used by staff/student(s) of the University in their official capacities.

## 2. Principles

Security Investigations allow authorised staff of the University to determine if the security of an asset (IT/Information) has occurred or to determine if the University's IT regulations have been breached. This investigation policy ensures that proper safeguards are put in place which secure the data on any device which is being investigated and also protect the individual carrying out the investigation.

- University staff/student(s), who have access to information assets, have a responsibility to handle them appropriately and in accordance with their classification.
- University information assets should be made available to all who have a legitimate need for them.
- Information Asset owners are responsible for ensuring that the University classification scheme, (which is described in the Information Security Policy) is used appropriately.

## 3. Objectives of this policy

- To define the responsibilities of individuals who instigate investigations.
- To define the principles to be used in carrying out investigations
- To co-ordinate and oversee the response to investigations in accordance with the requirements of UK legislation and University Policies.
- To minimise the potential negative impact of a security violation to the University, its customers and third parties.
- To engage, where appropriate, with the approved external authorities.
- To ensure potential threats to University core services are minimised.
- To provide clear and timely communication to all relevant parties.
- To ensure all staff responsible for investigations are appropriately trained and authorised to undertake the required actions needed for an investigation.
- To protect staff carrying out investigations from possible prosecution.
- To guarantee the integrity of any information assets which are being inspected

## 4. Action Implementation

Procedures will be put in place in order to ensure the effective use of the University Security Investigations Policy. The following principles underpin these procedures:

- University staff/student(s) must report information security violations to their line manager, Faculty security manager and/or CSD Service Desk.
- Staff/student(s) must be aware of University disciplinary procedures (Staff/Student) and UK legislation before requesting a user investigation.
- Staff/student(s) must supply and complete all relevant request forms with the appropriate evidence and authorisation before requesting CSD input.

- The integrity of information gathered, during an investigation, must be maintained throughout; information must be accurate, complete, timely and consistent with other information and events that may determine the reasoning and outcome of an Investigation.

## 5. Right to a user Investigation

The University reserves the right to investigate a University staff/student(s) and their use of University IT facilities and information assets (electronic and non-electronic) in specific circumstances such as, but not limited to:

- Members of Computing Services Department and other members of staff/student(s) discover or witness the misuse of University equipment, facilities or information assets.
- Where there is reasonable suspicion that a user or users are storing, transmitting or transferring data which violates the University's regulations and policies, contractual obligations or UK legislation.
- Where the University has been requested, or required, to monitor data by an approved external authority, as part of a criminal or civil investigation.
- To investigate or detect unauthorised use of the University's computing facilities.
- Investigation requests may be required as part of wider related investigations such as performance and productivity related requests or public disclosure requests.
- To exonerate a University staff/student(s) in the event of an allegation and to ensure no bias or intended misinterpretation occurs.

For more information on roles and responsibilities and the misuse of University facilities and information assets, please refer to the University Public Interest Disclosure (Whistle blowing Policy) http://www.liv.ac.uk/legal/policies/index.htm

## 6. Boundaries of Investigation(s)

Staff members of the Computing Services Department and other staff members of the University who are authorised to undertake investigations or are part of the disciplinary process must be aware of relevant legislation and restrictions as to what the University can access as part of an Investigation.

- Any University “owned” or “managed” information assets and equipment may be accessed as part of a User Investigation e.g. Laptops/Mobile Phones/Other media devices and equipment. This includes **any** item of equipment which is purchased from a University account.

- “Non –managed” or “owned” information assets or equipment **cannot** be accessed electronically or by other means unless explicit written consent is given by their owner.

## 7. Types of Investigation

### Type 1 Investigation (Non-user Investigation)

Non-user investigations are those which have been determined by the CSD Service Desk and root cause analysis process as non-user specific investigations and may be associated with University wide specific events or problems. For more information on Type 1 Investigations please refer to the Information Security Incident Response Policy.

### Type 2 Investigation (User Investigation)

A user investigation is one in which the use of IT resources by a specified individual(s) is scrutinised. Those who request a user investigation must follow University internal disciplinary procedures and

have been authorised by senior members of Human Resources and the Student Administration and Support division (SAS) before requesting input from the Computing Services Department.

**Please refer to the relevant procedures for more information**

- Student Disciplinary Procedures
- Staff Disciplinary Procedures

**Examples of User Investigations include, but are not limited to:**

| Incident Determination | Investigation Type | Authorisation Needed |
|---|---|---|
| Sending of material which is designed or likely to cause offence, annoyance, inconvenience or needless anxiety to another individual.<br><br>Theft or physical loss of University information assets e.g. Laptop/Media devices.<br><br>Unauthorised access or usage of information assets.<br><br>Defamation of the University or its staff/student(s).<br><br>Apparent breach of the University's IT regulations and/or wider University Policies.<br><br>Intentions to steal, cheat, defraud, plagiarise or deface information assets and equipment owned both by the University or a third party.<br><br>UK Legislation and/or illegal activity. | **Type 2**<br><br>**Specific User Investigation** | **(UIGT)**<br><br>**User Investigation Governance Team** |

## 8. User Investigation Governance

Decisions to undertake a user investigation must be taken and managed by the **User Investigation Governance Team** to ensure that such requests are free from bias and are not malicious. Investigations can be time-consuming and the decision to undertake must be made centrally to justify the use of resources which is commensurate with the scale of the work to be undertaken. Taking such decisions centrally will also help to ensure consistency of treatment for all staff/student(s) of the University.

### User Investigation Governance Team

The Investigation Governance team consists of senior staff members of the University who are trained, qualified and authorised to sanction a user investigation – For the purposes of this policy; the UIGT Team will be associated with a post rather than an individual.

| UIGT |
|---|
| Director of Computing Services Department |
| Director of Human Resources |
| Academic Secretary/Director of Student Administration and Support Division |
| Director of Legal Risk and Compliance |
| Information Security Officer |

## 9. User Investigation Request (Roles and Responsibilities)

### Source/Requestor

The requestor must be authorised by the appropriate UIGT staff members only and must send a completed User-Investigation Request Form to the Director of Computing Services with all relevant identifiers and justification**.** Failure to supply the information requested may invalidate or delay the implementation of a requested investigation. For an initial User Investigation Request, the Director of Computing Services is the point of contact (POC) and all completed forms must be sent to him/her in the first instance.

### Director of Computing Services (CSD)

When receiving a user investigation request, the Director of Computing Services will initially review the reasoning for such an investigation. A decision will be made by the Director to accept, request more information or reject the request. In the event that the Director is unavailable, his/her deputy will fulfil this role (CSD Senior Management).

The User Investigation Governance Team (UIGT) may be contacted by the Director of Computing Services for specific user investigations that may need clarity on the legislative, regulative and disciplinary procedures that the University operates. This team will assist the Director of Computing Services to ensure that the correct justification for a user investigation is applied.

### CSD Security Investigation Team

These are senior staff that is trained, qualified and authorised to undertake the information/evidence gathering of a user investigation. Authorisation for the security investigation team to carry out an investigation must only come from the Director of Computing Services and/or his delegate.

As part of the investigation, specialist computer forensic tools may be used to assist in providing an analysis of the use of information assets and electronic systems.

***N.B In the event that the investigation relates to criminal/civil proceedings, any member of UIGT and the security investigations team may be asked to attend court as a witness or in an advisory capacity on the actions taken throughout a user investigation.***

### Collection and Preservation of Evidence

To ensure the collection and preservation of any information or evidence, the security investigation team will have a rigid set of documented procedures for the different types of investigation(s) that they must follow to ensure that the information/evidence gathered satisfies legislative and regulative good practice. This will ensure that the evidence gathered is adequately protected and admissible as part of University disciplinary procedures and in court.

Documentation which supports the investigation procedures must be classified in accordance with the Information Asset Classification Policy **(Confidential/Strictly Confidential)** and the sharing of this information must be limited on a need to know basis.

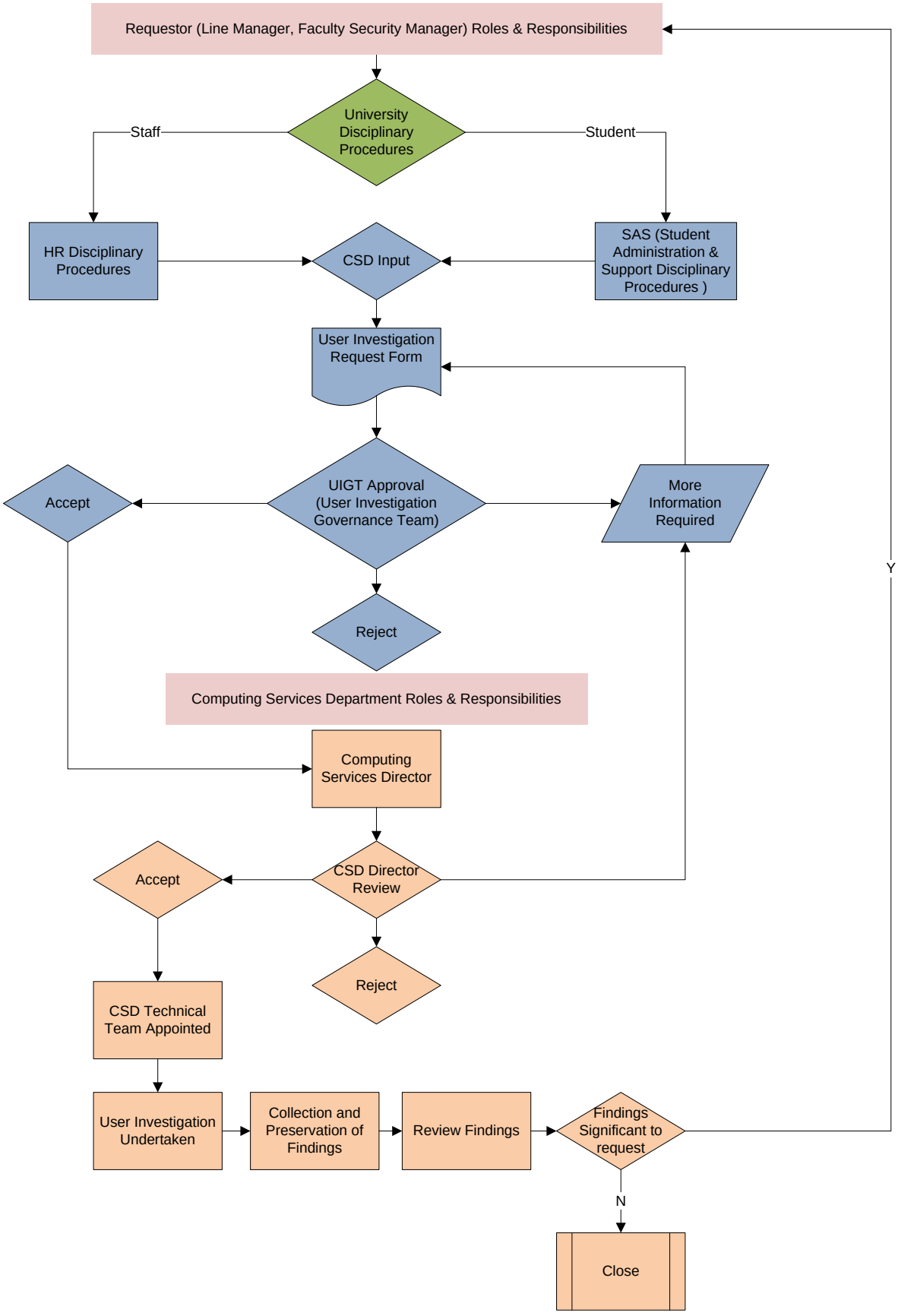
### Findings

All user investigation findings must be factual and present an accurate reflection of the initial investigation request. The findings will be reviewed to ensure they are of relevant and significant use towards the initial investigation request. If required, the findings will be sent to the Director of Computing Services only.

Due to legal ramification, any user Investigation findings must be explicitly interpreted by the security investigation team and the Director of Computing Services. The investigation findings are the ownership of the Director of Computing Services and he/she reserves the right to withhold any findings which are not pertinent to the initial investigation request.

The Director of Computing Services will co-ordinate and consult with the requestor (UIGT) of the user investigation. The consultation will advise the requestor of the findings and if they are relevant to the original request and the overall disciplinary procedures that are over seen by the Chief Operating Officer.

## 10. User Investigation Request Process



## 11. External Investigation Requests

The University may from time to time receive external requests from approved authorities and requests for information or permission to investigate a particular staff/student of the University. The University will assist with the approved authorities as required by legislation and/or law. For all approved authorities, user investigation requests must be directed immediately to the Director of Computing Services.

Any user investigation findings may be referred to approved authorities and partners. In the event this is required, CSD will communicate with the relevant stakeholders e.g. University's Security Services and/or the University's Police Officer in the first instance.

## 12. Information Access Requests (Non-Investigative)

Information access requests (IAR) are **non-investigative** and dependent on the request, will only be considered if there is an operational need.

CSD may be requested to provide specific information from University assets (managed and owned) such as IT Systems and media devices which include:

- PCs
- Mailboxes
- M Drive/Departmental drives
- Telephones (Landline/Mobile phones)

### Usage Reports (Compliance and Monitoring)

As part of the University's Compliance and Monitoring activities, authorised staff may request CSD to provide usage reports for specific University assets. Usage reports include:

- Telephone (Landline/Mobile)
- Printer(s)
- Internet
- VITAL

Information access request(s) (IAR) must be sought via an IA Request Form which must be completed with all the relevant information prior to submission. Failure to supply the information requested may delay or invalidate the request.

### Authorised Request

CSD will only be notified of IA request(s) that have been reviewed and authorised by your department/faculty approver prior to CSD receiving the completed form. CSD will not undertake any data gathering until the relevant area approval has been completed. In the event a request is rejected the requestor will be notified via email.

**Authorisation Matrix (Table 1)**

<table>
<tr><th colspan="5">Requestor and Authorisation Matrix</th></tr>
<tr><th colspan="2">Professional Services Staff</th><th colspan="3">Academic Staff</th></tr>
<tr><th rowspan="2">Requestor</th><th rowspan="2">*Authorisation</th><th rowspan="2">Requestor</th><th colspan="2">*Authorisation</th></tr>
<tr><th>Staff</th><th>Student</th></tr>
<tr><td>Staff/Senior Staff</td><td>Professional/Operational Services Director</td><td>Academic/Senior Academic</td><td rowspan="4">Faculty Operational Services Director(s)<br><br>Faculty Corporate Services Officer(s)</td><td rowspan="4">Faculty Corporate Services Officer(s)<br><br>Faculty Student Experience Manager</td></tr>
<tr><td rowspan="3">Professional/Operational Services Director</td><td>Director of Legal Risk and Compliance</td><td rowspan="2">Head of Department</td></tr>
<tr><td>Director of Human Resources</td></tr>
<tr><td>Director of Computing Services</td><td>School/Institute Manager</td></tr>
<tr><td colspan="5">*Requests are automatically sent to the appropriate staff/student authoriser(s) upon submission. CSD will not undertake any data gathering until the IAR has been reviewed and authorised.</td></tr>
</table>

***N.B. Information provided and stipulated in the original (Information Access Request(s) must only be used for the purposes stated in the request. In the event that information provided is used for purposes other than advised, the requestor may be in breach of wider University Policies and they themselves may face disciplinary actions.***

### 13. FOI (Freedom on Information) Requests

Any information that may be requested by an unapproved authority, third party or member of the public under the freedom of information act should be referred to the University Legal, Risk and Compliance department.

### 14. Legal obligations and University policies

This policy is aimed at all staff/student(s) of the University who have a responsibility for the usage, management and ownership of information assets. This policy is part of the University Information Security Management System (ISMS) and should be read in conjunction with the **Information Security Policy** and its sub policies and relevant UK legislation(s). Further relevant policies and legislation(s) are listed in **Appendix A**.

### 15. Compliance and Monitoring

All staff/student(s) of the University are directly responsible and liable for the information they handle. University staff are bound by the terms of their employment with the University to abide by its IT regulations. Students' registration with the University also binds them to abide by the University's IT regulations.

Authorised staff of the University may monitor the use and management of information assets to ensure effective use and to detect unauthorised use of information assets.

## Appendix A – University ISMS Reference

- Regulations for the Use of IT Facilities at the University of Liverpool
- JANET Acceptable Use policy
- Information Security Policy
- Workspace and IT Equipment Security Policy
- Information Security Incident Response Policy
- Information Asset Classification Policy
- Information Security Review Policy
- IT Procurement and Third Party Security Policy
- IT Asset Disposal Policy
- Procurement Policy
- Data Protection Policy
- Freedom of Information Policy
- Copyright Policy
- Card Payment Policy
- Records Management Policy
- Records Retention Policy
- Risk Management Policy
- Student/HR Disciplinary Procedures

Relevant legislation includes:

- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act 1988
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Data Retention Investigatory Powers Act 2014
- Counter Terrorism and Security Act 2015 (Prevent)
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Police and Justice Act 2006
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002

Relevant Regulation includes:

- PCI-DSS (Payment Card Industry Data Security Standards)