Information Sharing Policy for Security-related Data:
Version 3

October 2018

This policy will be reviewed every 12 months

This policy will be re-signed by the Principal whenever
a new post-holder takes over this role.

This provides a framework for information sharing between the University and the Police which is both legal and supports the primary objectives of reducing crime and disorder and ensuring safety and security at St. George's, Horton Halls and in and around Tooting.

1. Introduction

SGUL wishes to ensure that it has robust and systematic procedures in place for the collection of security-related information and for dealing with any perceived security threats to the institution's staff, students, visitors or premises.

Please note, this policy does not apply to Kingston University students attending SGUL as these students do not come under the jurisdiction of SGUL in relation to this policy.

This policy should be read in conjunction with SGUL's staff and student **Privacy Notices** and SGUL's **Dignity at Work and Study Policy.**

The purpose of this policy is to offer transparent institutional guidance to staff and students for the receipt of, and passing on of, information concerning security issues, both:

- within the institution itself, and,
- by the institution to the police.
- by the institution to other external agencies.

Such security concerns could include:

- antivivisection activities
- distribution of extremist religious propaganda
- harassment / intimidation / stalking / cyber abuse
- incitement to racial hatred
- theft / unauthorised possession or destruction of SGUL property.

All information received by the University will be acknowledged, documented, recorded and kept, or disposed of, securely –please see Appendix A for further details.-

Jenny Higham: Principal of SGUL has overall responsibility for this policy. However, in practice the Principal delegates authority to administer this policy on behalf of the university to **Paul Ratcliffe: Chief Operating Officer.**

The University has been advised by the Police that in the first instance a representative from Wandsworth Borough Police will always be available to deal with any security issue raised by SGUL.

2. Passing on security concerns appropriately within the institution

It is possible that from time to time staff or students at the university may notice incidents occurring at the institution which cause concern. These might include:

- Unattended bags or general items being left in or outside of the university buildings
- Staff or students behaving in a way that raises concern, such as: organising unauthorised meetings or events, threatening other members of the university, acting in an inappropriate way which could cause harm to themselves or others, or placing pressure on individuals to conform to a particular ideological viewpoint
- Unusual or unexpected behaviours from visitors or members of the public
- Individuals attempting to access a secure area without the appropriate permission or a valid security pass

Individuals may feel confused about the level of importance of what they have observed and unsure as to whether or not they need to pass on information.

However the university advises that everyone with any such concern - no matter how apparently insignificant - feels able to pass on this information. It is vital that SGUL has an authentic record of all information received which may be related to security. Such information may be passed on in person, by telephone, or by email to:

Chief Operating Officer:	**Paul Ratcliffe**
Dean of Students:	**Aileen O'Brien**
Director of Human Resources (or Deputy):	**Jenny Winters**
Academic Registrar:	**Jenny Laws**
Facilities Manager:	**Elizabeth Gilby**

The above individuals all have specific responsibility for collecting information on overall site security. As such, these staff may be aware of ongoing site security issues. A single piece of information may prove useful in 'triangulating' information, building up a whole picture or in demonstrating a pattern. (Please see Appendix A: Process for dealing with security concerns).

These colleagues have designated responsibility for assessing the importance of each piece of information and for deciding whether or not the university needs to act on the information received. -This is to ensure that the university protects its staff and students from any unwanted harassment based on unfounded assumptions resulting from shared information. -

The colleague that the incident was reported to will immediately make a written record of any security-related information they receive and will inform the Chief Operating Officer.

If a member of the university's staff or student passes on information, they will be asked to sign a disclosure stating that the university has accurately recorded the information they provided.

3. Passing on security concerns related to patients or patient care

a) Practice Placement

If while on any practice placement, a student has security concerns in relation to:

- a patient
- a patient's care

Then in keeping with General Medical Council guidelines the student should immediately inform their clinical contact directly. The clinical contact may be the student's supervising consultant or the most accessible senior doctor available.

This staff member will then assume responsibility for reporting any security concern using the practice placement provider's own internal security procedures.

b) Clinical skills session at SGUL

If while taking part in an SGUL's clinical skills laboratory session a university staff member or student has a security related concern pertaining to a patient, or a patient's care then in keeping with General Medical Council guidelines they should immediately inform the lead supervising member of staff directly.

This staff member will then assume responsibility for reporting any security concern using the SGUL's site's own internal security procedures. This includes reporting the matter immediately to one of the following staff:

Chief Operating Officer:	**Paul Ratcliffe**
Dean of Students:	**Aileen O'Brien**
Director of Human Resources (or Deputy):	**Jenny Winters**
Academic Registrar:	**Jenny Laws**
Facilities Manager:	**Elizabeth Gilby**

Please see Appendix B.

4. Acknowledgment of information received

Any security-related information received by the university will be acknowledged in writing to the individual who made the disclosure by one of the staff members named in this policy as having designated responsibility for site security. The university will state that it may not always be possible to disclose how it plans to act upon the information received.

5. Possible action resulting from information received

Resulting action from information received could include:

- No action as concern is assessed to be low risk
- Internal procedures are enacted
- Security procedures are reviewed
- Support is offered to individual staff and students
- Contacting the police -if it appears the law has been broken, or a serious security risk is identified.-

6. Decision to share information received within the institution

In order to preserve confidentiality and security the decision to share security-related information within the institution may only be made by:

Chief Operating Officer:	**Paul Ratcliffe**
Dean of Students:	**Aileen O'Brien**
Director of Human Resources (or Deputy):	**Jenny Winters**
Academic Registrar:	**Jenny Laws**
Facilities Manager:	**Elizabeth Gilby**

All decisions to disclose any such information internally will be documented in a shared log (see Appendix C) and will include:

- the reasons for deciding to disclose the information
- who the information will be disclosed to
- any planned action.

7. Decision to pass information between St George's University of London and St George's NHS Healthcare Trust

As St George's University of London and St George's Healthcare Trust both share the same physical site, from time to time, and while remaining within the guidelines of data protection law, both institutions may swap information related to site security concerns as appropriate.

8. Protection of confidential personal data

Under UK Data Protection Legislation the university has a duty of care to protect its staff and students' confidential personal data, such as:

- names, addresses, telephone numbers and email details
- membership of particular teams, departments or societies
- computer use data

Additionally under **Article 8** of the **Human Rights Act 1998**, all individuals at the university have 'the right to privacy'.

The university takes very seriously its duties to comply with the law.

9. The decision to pass on information to the police

UK Data Protection Legislation includes exemptions that allow an organisation to choose to disclose data (without being in breach of the Law) if it is persuaded that doing so is both necessary and proportionate for:
a) the purpose of safeguarding national security or
b) the prevention or detection of crime, the apprehension or prosecution of offenders, or
the assessment or collection of any tax or duty (Please see Appendix C).

The decision to release data may only be made by the following role holders:

The Chief Operating Officer and the Director of Human Resources (or deputies)
<u>in the case of staff records:</u>

The Chief Operating Officer and the Academic Registrar
<u>in the case of student records:</u>

The Chief Operating Officer and the Student Union Chief Operating Officer
<u>in the case of Student Union records where the personal data originated from the University:</u>

<u>However in all cases the university will only release such data if:</u>

- there is a perceived security threat and;
- postholders are in receipt of a valid application in writing from the police, requesting the lawful release of specific confidential personal data.

In **<u>all</u>** cases the police must complete a form and send it to the organisation which may hold the information.

The university will only respond to written police requests to release such data, in the interests of national security, or for the purposes of preventing or detecting crime.

Generally this information will only be disclosed to the police officer named in this Information Sharing Policy (see Introduction). While the University is aware that requests for security related information may not always come from police local to the university premises, nevertheless any requests for information will follow the strict procedure as outlined in this policy.
Again all decisions to disclose such information to the police will be documented in the shared log and will include.

- the reasons for deciding to disclose the information
- who the information will be disclosed to

- any planned action.

10. The level of information to be shared

Untrammelled access to personal data by the police will only be provided by the university on the production of a search warrant.

However the decision to reveal the contents of any individual's mail box **will be taken by the Principal alone (or designated Deputy in her absence).**

11. Support offered to students

Students will have the ability to access support from the usual places – the Student Union, their Personal Tutor and the Counselling services.

12. The coordination of information

For all such requests the colleague who authorises the disclosure will be responsible for coordinating the institution's proper response to a request. In order to provide an audit trail that colleague will also confirm the decision to disclose information to the police in writing to the Data Protection Officer.

13. Passing on student information between institutions

Student information kept on a student record system or student files can only be accessed **by staff from the institution at which the student is currently studying.**

Information held at other institutions may not be requested or used in support of any investigation or for any other purposes unless offered by the student in support of an application of a place on a programme of study or employment.

This means that while SGUL and Kingston University share the Faculty of Health and Social Care Sciences (a unique joint faculty across the two higher education institutions); SGUL does **not** have access to any personal data related to Kingston University students. Therefore the institution is unable to pass on any data related to Kingston University students.

14. Disclosure of information to third parties

Only under certain circumstances will SGUL authorise the police to disclose information to third parties. For instance, if the police information is to be disclosed to the Serious Fraud Office, the Information Commissioner, the Crown Prosecution Services, the UK Border Agency or Her Majesty's Revenue and Customs.

However, in all such cases it is entirely the responsibility of the police to ensure that such information is properly handled once it passes from their hands to another person or organisation.

15. Associated responsibilities of the colleagues

Occasionally the university may receive a police request for information during holiday time or when the university is shut. At such times, appropriate staff and/or Student Union Executive Officers may be away from the university premises.

However at all times, relevant individuals will be assigned designated responsibility for protecting and accessing staff, student and Student Union records should a police request for information on security grounds be received.

16. Bullying and harassment

This policy should be read in conjunction with the **Dignity at Work and Study Policy**. If it is established that a member of the university (staff or student) has knowingly provided false information and raised a mischievous or malicious accusation against another person, they will be the subject of disciplinary action. The deliberately false defamation of another person's character is unacceptable to the University.

17. Reasonable notice of this policy to members of SGUL

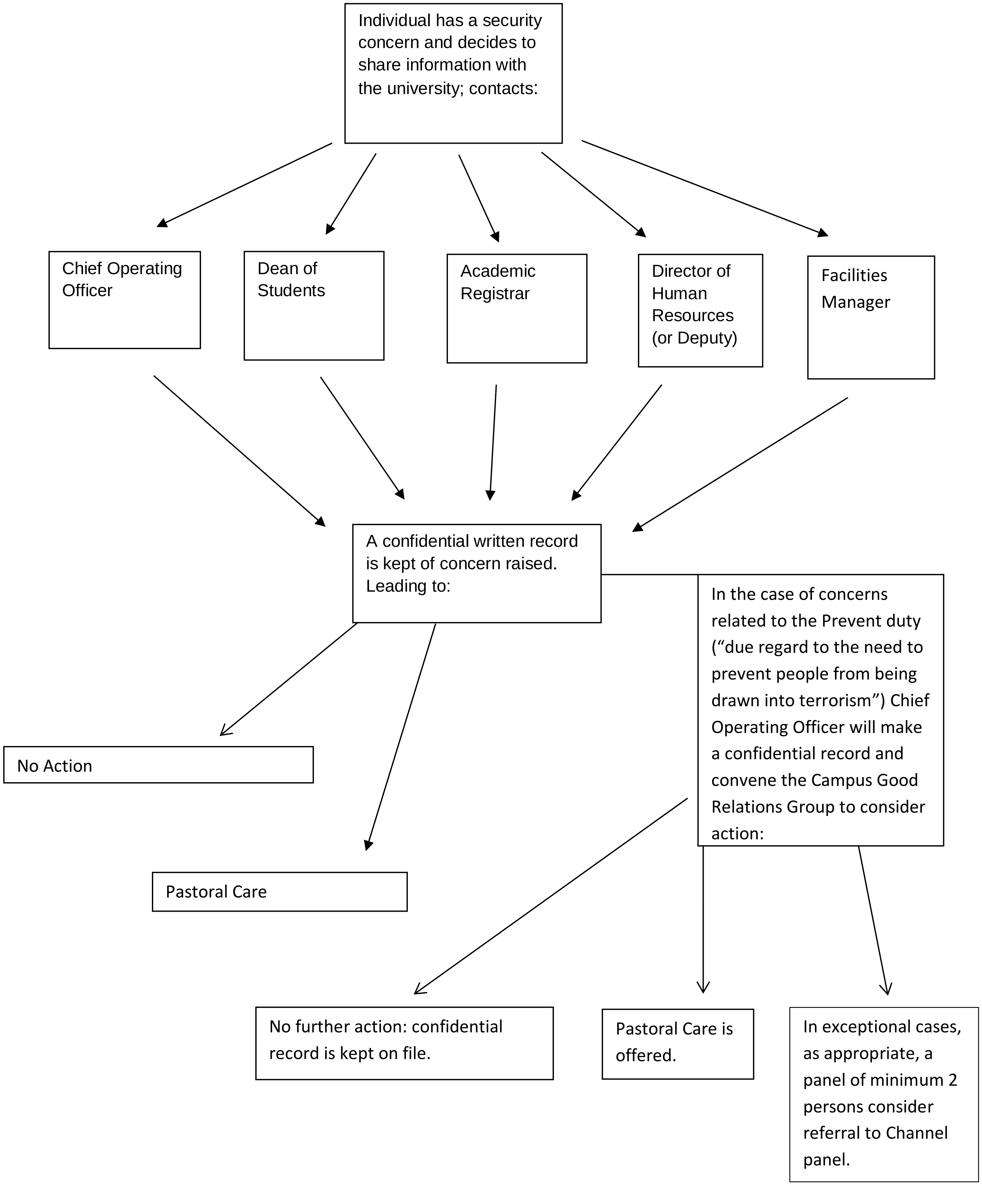
SGUL is aware that the law requires that persons are given "reasonable notice" that information concerning them may in certain circumstances be shared with the police.

Therefore the university will give staff and students such reasonable notice that the institution intends to introduce and operate an information sharing policy for security related data and will in its absolute discretion share information with the police from time to time. This information will be communicated by SGUL's accessible, **'Fair Processing (or Privacy) Notice** – which advises SGUL staff and students of all the purposes for which the university processes their personal information. The university will alert individuals to its Fair Processing (or Privacy) Notice by -:

- notices placed on staff, student and student union university noticeboards,
- an email link to this upload on the Portal sent to all staff and students.

APPENDIX A:

Process for passing on security concerns appropriately within the institution



Individual has a security concern and decides to share information with the university; contacts:

Chief Operating Officer

Dean of Students

Academic Registrar

Director of Human Resources (or Deputy)

Facilities Manager

A confidential written record is kept of concern raised. Leading to:

No Action

Pastoral Care

In the case of concerns related to the Prevent duty (“due regard to the need to prevent people from being drawn into terrorism”) Chief Operating Officer will make a confidential record and convene the Campus Good Relations Group to consider action:

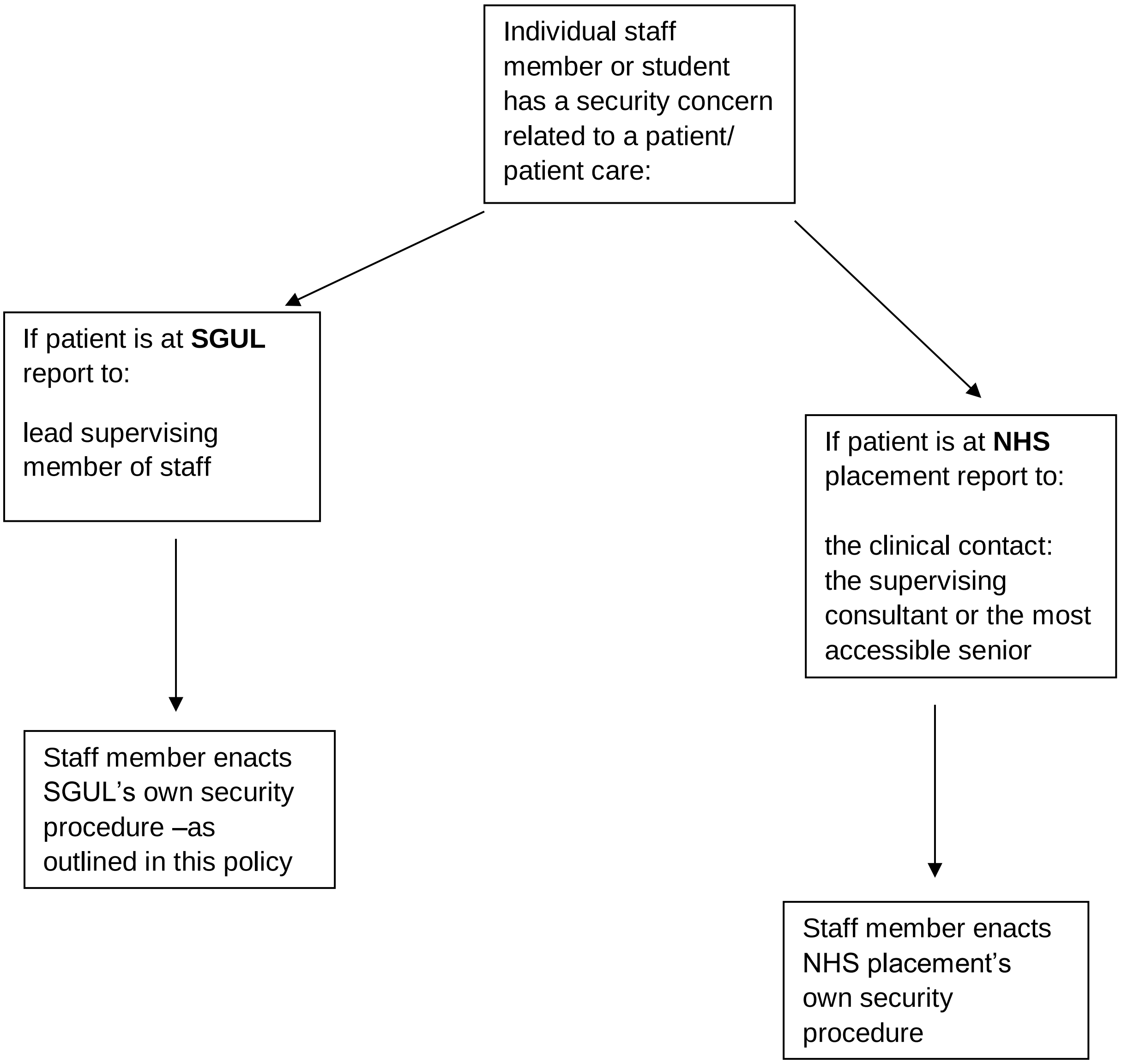
No further action: confidential record is kept on file.

Pastoral Care is offered.

In exceptional cases, as appropriate, a panel of minimum 2 persons consider referral to Channel panel.

APPENDIX B

Process for passing on security concerns related to patients or patient care



Individual staff member or student has a security concern related to a patient/ patient care:

If patient is at **SGUL** report to:

lead supervising member of staff

Staff member enacts SGUL's own security procedure –as outlined in this policy

If patient is at **NHS** placement report to:

the clinical contact: the supervising consultant or the most accessible senior

Staff member enacts NHS placement's own security procedure

APPENDIX C

1. Recording of information received

The accurate recording of information received

In order to preserve confidentiality, all security related data received will be recorded and stored in a shared log. All information in the log will be encrypted and securely protected.

SGUL will ensure it is provided with up to date advice on encryption technology by its Computer Services Team to prevent any information being inadvertently disclosed.

The colleagues will be able to access this log as required.

2. Acknowledgment of information received

All security-related information received by the university will be acknowledged in writing to the individual who made the disclosure.

Copies of all emails received and sent in relation to security issues will also be securely stored in the shared log.

3. Storage of information received

In order to prevent unauthorised or accidental disclosure of confidential information, it will not be permitted for individuals to store or transport this information on a lap top or a memory stick.

IT Services will advise on appropriate security and encryption technologies with respect to storing and transferring any data.

The institution will keep a permanent record of all disclosures made to all third parties, e.g. the police, benefit fraud investigation units.

However in some cases SGUL may decide that it is not appropriate to take any action. For example if an SGUL member made a report which involved suspicions about another SGUL member and the matter was subsequently investigated and no evidence of any wrongdoing was found, then in such instances SGUL will not keep a record of this report.

Otherwise information on the shared log will be permanently stored. Nevertheless, regular consideration will be given to whether data should be deleted or destroyed if it is no longer required for the original purpose it was supplied, unless:

- it was supplied in order to meet a statutory obligation
- it is required by the Metropolitan Police for a policing purpose.

4. Disposal of information received

The colleagues will jointly authorise in writing the disposal of any security related information to the Head of IT Services.

Any disposal will be done on site by staff as authorised by the Head of IT Services.

University records including data recorded in any form, such as paper files, computer files, audio- and videotapes, film and microfiche will be disposed of securely using methods which do not allow future use or reconstruction.

SGUL adheres to the British Standards on records management (15489-1) as set by the International Organization for Standardization which specifies the following principles should apply to the destruction of records:

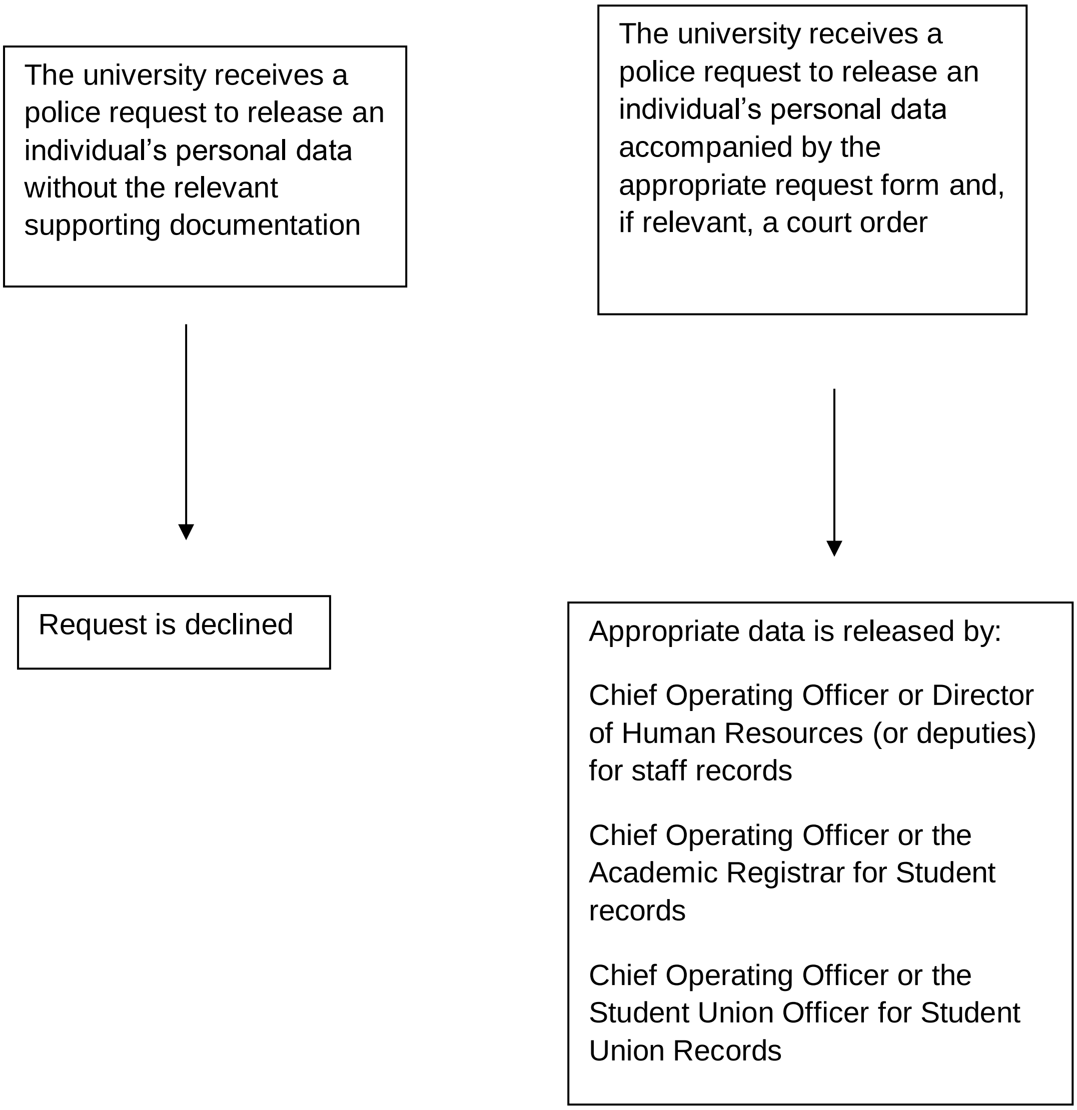
"…

- Destruction should always be authorized
- Records pertaining to pending or actual litigation or investigation should not be destroyed
- Records destruction should be carried out in a way that preserves the confidentiality of any information they contain
- All copies of records that are authorized for destruction, including security copies, preservation copies and backup copies, should be destroyed…"

A disposal record will list what records have been destroyed, when, by whom, and using what method of destruction in order to respond to potential Freedom of Information requests. Records which have been kept or archived may also be tracked. The record may consist of a simple list on paper, or be part of an electronic records management system.

APPENDIX D

Process for releasing security data to the police



The university receives a police request to release an individual's personal data without the relevant supporting documentation

Request is declined

The university receives a police request to release an individual's personal data accompanied by the appropriate request form and, if relevant, a court order

Appropriate data is released by:

Chief Operating Officer or Director of Human Resources (or deputies) for staff records

Chief Operating Officer or the Academic Registrar for Student records

Chief Operating Officer or the Student Union Officer for Student Union Records

KH November 2013
Updated RR December 2015
Updated PR/CM June 2018
Updated CM October 2018