

Policy on handling and storage of security sensitive materials

Policy owner:	Northern School of Contemporary Dance – Leadership Team
Lead contact:	ICT Manager & Prevent Spoc
Audience:	Applicants/Students/Staff for Northern School of Contemporary Dance Courses of higher education
Approving body:	Northern School of Contemporary Dance: Academic Board
Date approved:	
Policy Implementation date:	This policy takes effect from September 2022
Supersedes:	
Previous approved version(s) dates:	July 2020 / 2021
Review cycle:	Annually
Next review due date:	July 2023
Related Statutes, Ordinances, General Regulations	Validating Universities' Academic Regulations
Related Policies, Procedures and Guidance:	<ul style="list-style-type: none"> • Prevent Strategy & Policy • E Safety and Online Policy • Acceptable Use – IT Systems Policy • Data Protection Policy • Academic Freedom and Freedom of Speech Policy
UK Quality Code reference:	
OfS (Office for Students) Conditions reference:	Condition:
Equality and Diversity Considerations:	Policy should be available in accessible format for all students.
Date Equality and Diversity Assessment Completed:	
Further information:	

Table of Contents

Introduction	3
Responsibility	3
What is “security sensitive material”?	3
Scope and purpose of the policy.....	4
Policy and procedures.....	4
Disclosure before handling security sensitive materials.....	4
Rules for the safe keeping of security sensitive material	5
Discovery of or concerns about security-sensitive materials	5
Failure to follow this policy	5
Redress for actions taken under this policy	5

Introduction

1. The consultation of security-sensitive materials may be necessary for perfectly legitimate study or research consistent with the artistic activities of the school. The purpose of this policy, with reference to Prevent strategy and other relevant legislation, is to help to reduce misidentifications of information-gathering as suspect or criminal and to provide for the secure storage of security sensitive material away from personal computers or other locations which might be accessible to other staff and students.
2. Staff or students considering that it may be necessary to consult security sensitive materials should read this policy before proceeding to consult such materials.

Responsibility

3. As set out in the Prevent Strategy and Policy, the Board of Governors has overall responsibility for ensuring that NSCD discharges its Prevent duty.
4. In line with the Prevent Strategy and Policy, responsibility for the implementation of this policy rests with the school governing body, which is responsible for ensuring that appropriate policies, procedures, and networks are in place within the school to enable Prevent duty to be discharged. Management oversight for this policy rests with the school principal, who has management oversight of the implementation of Prevent duty within the school.
5. The school principal may delegate the actions identified in this policy to another member of senior staff.

What is “security sensitive material”?

6. The primary scope of this policy is the viewing, handling and storage of security-sensitive materials that can be interpreted as engaging the provisions set out in the Terrorism Act (2006). Terrorism has been defined as ‘an action that endangers or causes serious violence to a person/people; causes considerable damage to property; or seriously interferes with or disrupts an electronic system. The use or threat must be designed to influence the government or to intimidate the public and is made for the purpose of advancing a political, religious, or ideological cause.’
7. Sections 2 and 3 of chapter 11 of the Terrorism Act (2006) outlaw the dissemination of terrorist publications, including by electronic means, and give a very wide definition of ‘terrorist publication’ and ‘statements’ that could be construed as endorsing or promoting terrorism.
8. The school also has responsibilities to prevent students and staff from being drawn into terrorism.
9. In outline, security sensitive research material is likely to include, but is not limited to:
 - Military or paramilitary training manuals or procedures.
 - Documentation or media supporting extremist ideologies
 - Instructions, guidance or advice on the planning or execution of terrorist acts.
 - Instructions, guidance or advice relating to the acquisition or use of a radioactive device or radioactive material.
 - Material supporting, inciting, or condoning acts of terrorism
 - Material intended to radicalise or proselytise individuals into adopting an extremist viewpoint.
 - Material intended to recruit or otherwise enlist members or followers to banned organisations.
 - Instructions, guidance, or advice (including the acquisition of components) on the subjects of:

Policy on handling and storage of security sensitive materials

- o bomb making;
- o the manufacture of improvised explosive devices (IEDs);
- o the creation of chemical weapons or toxic agents.

Scope and purpose of the policy

10. This policy identifies security-sensitive information as a candidate for safe handling and storage and the steps to be taken where such information is identified. It is not a mechanism for the approval or regulation of research. However, the school may require handling and storage of security-sensitive material to be discontinued where conditions set under this policy are not met, or where it is determined that there is no good reason for the materials to be handled or stored.

11. Staff or students intending to consult, handle or store other kinds of information which they consider may be security sensitive in other ways, for example security-sensitive information relating to military equipment or IT encryption, should also follow the procedure for disclosure set out in the policy.

12. The scope of this policy includes both downloading material that is security sensitive and visiting security-sensitive websites.

13. In the application of this policy, the principal shall have regard for the following:

- The Terrorism Act (2000)
- The Terrorism Act (2006)
- The Counterterrorism and Security Act (2015)
- Prevent Duty, including the UK Government Prevent Strategy (2011) and NSCD's Prevent Strategy and Policy
- The duties set out in the Equality Act (2010)
- The exercise of Freedom of Speech, as set out in the school's Academic Freedom and Freedom of Speech Policy
- The exercise of Academic Freedom, as set out in the Articles of the school.

Policy and procedures

Disclosure before handling security sensitive materials

14. From time-to-time staff or students may, during studies or research (including artistic research) conducted in association with the school, identify a need to consult security sensitive materials.

15. Where study or research might necessitate access to such materials, staff and students are expected to declare this to the school principal. The principal will take steps to explore with the student or member of staff the proposed activity and, as appropriate, may set conditions for the handling and safe keeping of the materials. Conditions may include a requirement to use an approved secure storage facility and oversight of the use of an approved secure storage facility by school management. A school may require handling and storage of security-sensitive material, or plans to use such materials, to be discontinued where conditions set out in this policy are not set, or where it is determined that there is no good reason for the materials to be handled or stored.

Policy on handling and storage of security sensitive materials

Rules for the safe keeping of security sensitive material

16. Conditions set by the school for the safe-keeping of security-sensitive materials must be complied with.
17. Security-sensitive research material must not be stored on a personal computer, USB device or external hard drive.
18. Security-sensitive research material must not be transmitted to a third party or exchanged.

Discovery of or concerns about security-sensitive materials

19. Staff or students who discover security-sensitive materials on school property or school IT systems or who are concerned about unauthorised viewing or handling of such materials should raise their concerns in confidence with the school principal.

Failure to follow this policy

20. Failure to follow this policy may result in disciplinary action under the relevant school policy against the staff or student concerned.

Redress for actions taken under this policy

21. Staff and students are encouraged to raise concerns about actions taken under this policy informally with the principal or their delegate in the first instance.
22. Concerns about actions taken under this policy by the principal or their delegate may be raised formally under the staff grievance or student complaints policies of the school.