Goldsmiths
UNIVERSITY OF LONDON

Password Policy

Contents

Ownership	Chief Information Officer
Policy Contact	Information Security Manager
Approval	Information Security Steering Group
Protective Marking	Public
Policy Unique ID	POL0002
Last review date	June 2023
Next review date	June 2026

1 Introduction

1.1 A password policy is a set of rules designed to enhance information security by requiring strong passwords through using complex and longer passwords.

1.2 Information security threats are increasing, and Goldsmiths is under constant attack. Complex and long passwords are an important security control in reducing the risk of a successful attack.

1.3 Resetting your password periodically is enforced, as it is best practice to assist protecting users that are unaware their accounts have been compromised.

2 Scope

2.1 This policy applies to all accounts providing access to Goldsmiths' data and services.

3 Policy Statements

3.1 Password must not contain username, first name or last name.

3.2 Password must be between 12 and 100 characters long.

3.3 Password must be different from previously used ones.

3.4 Password for your Campus ID must not be utilised in any personal or other IT system.

3.5 Password must contain characters from the four primary categories, including:

- Uppercase letters
- Lowercase letters
- Numbers
- special characters e.g.! $ # % @ + (Note do not use " < > ' & £)

3.6 Passwords must be reset immediately after becoming aware of active involvement in a security incident.

3.7 Passwords must not be shared with anyone.

3.8 Passwords should not be written down in any format that anyone else can interpret.

3.9 If a password needs to be stored electronically it must be encrypted according to a standard of AES 256 with a password that meets this policy.

3.10 Student account passwords should be reset every 5 years and one month (i.e. 61 months).

3.11 All account passwords used for IT administration or accessing privileged accounts should be reset every 180 days.

3.12 All other account passwords should be reset at least every 365 days.

4 Sanctions

4.1 Non-compliant Goldsmiths user accounts may have their access to Goldsmiths data and services disabled until the user changes their password to be compliant with the policy.

5 Monitoring

5.1 Goldsmiths may periodically test users' password compliance with this policy.

6 Exceptions

6.1 Any IT system unable to support the policy must be reported to the Information Security Manager to record, investigate and advise on alternative controls.

7 Definitions

AES 256: Advanced Encryption Standard algorithm with 256 bit key length.

8 Related documents

- Information Security Policy
- Email policy
- IT Services Regulations for Students

9 Related requirements

- Goldsmiths' auditor reports
- Information commissioner's office - GDPR guidance

10 Revision history

Version	Date	Details	Author	Approved
1.0	01/08/16	Submitted to SMT	David Swayne	Approved
1.1	07/03/19	Submitted to ISSG	Peter Hircock	Not approved
1.1	20/06/19	Re-submitted to ISSG	Peter Hircock	Approved
1.1	11/11/19	Submitted to E&IC	Peter Hircock	Noted
1.2	09/06/21	Re-draft submitted to ISSG	Peter Hircock	Approved
1.3	21/06/23	Submitted to ISSG	Peter Hircock	Approved