Information Security Policy

2025

Document Control

Manager responsible: Dave Robinson, Operations and Estates Manager

Version number: 1.0

Approved by: SLT

Approval date: May 2025

Review date: May 2028

Hereford College of Arts

CONTENTS

1. Purpose

1.1 Hereford College of Arts (‘the College’) has made a large investment in its use of Information Technology (IT) across the campuses and therefore focuses on exploiting information. Next to people, information is the College’s most important asset. The information we use exists in many forms: printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Regardless of the form it takes, or means by which it is shared or stored, information should always be protected appropriately.

1.2 Information security is characterised as being concerned with guaranteeing:

1.2.1 Confidentiality (ensuring that sensitive information is accessible only to those authorised to use it).

1.2.2 Integrity (safeguarding its accuracy and completeness).

1.2.3 Availability (ensuring that authorised users always have access to information when they need it).

It must also address proper methods of disposal of information that is no longer required. Security is essential to the success of almost every academic and administrative activity. Effective security is achieved by working within a proper framework, in compliance with legislation and by adherence to the College’s approved Policy and Procedures.

2. Objective

2.1 The objectives of this Information Security Policy are to:

2.1.1 Ensure that all of the College’s computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse, and that this protection is cost-effective.

2.1.2 Ensure that all users are aware of and fully comply with this Policy statement and all associated Policies, and are aware of and work in accordance with the relevant Policies and Procedures.

2.1.3 Ensure that paper records are kept securely and managed effectively.

2.1.4 Ensure that all users are aware of and fully comply with the relevant UK and European Union legislation.

2.1.5 Create across the College an awareness that appropriate security measures must be implemented as part of the effective operation and support of information management systems.

2.1.6 Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.

2.1.7 Ensure that the College's IT Team understand their responsibilities on providing a robust infrastructure to provide the required availability to all users.

2.1.8 Ensure that information is disposed of in an appropriately secure manner when it is no longer relevant or required.

2.2 This Policy applies to all staff and students of the College and all other computer, network or information users authorised by the College or any department or employee. It relates to their use of:

2.2.1 Any College owned facilities (and those leased by or rented or on loan to the College).

2.2.2 Any centrally managed or otherwise IT systems.

2.2.3 All College owned or licensed data and programs (wherever stored).

2.2.4 All data and programs provided to the College by sponsors or external agencies (wherever stored).

2.2.5 This Policy Statement also relates to paper files and records created for the purposes of the College's business.

2.3 The College's Senior Leadership Team (SLT) has approved this Policy Statement and delegated its implementation to Heads of Departments.

2.4 Those requiring information, explanation or training about any aspects of the policy which relate to computer security should discuss their needs with the IT & Digital Resources Manager.

2.5 Questions about the creation, classification, retention and disposal of records (in all formats) should be taken to the Data Protection Officer (DPO).

2.6 The College's IT Department will in the first instance be responsible for interpretation and clarification of the Information Security Policy Statement.

3. Responsibilities for Information Security

3.1 All who make use of the College's systems and information have responsibility for protecting those assets. Individuals must, at all times, act in a responsible and professional way in this respect, and will refrain from any activity that may jeopardise security.

3.2 The Information Security Group (ISG) is responsible for defining an Information Security Policy and for ensuring it is discharged by all academic and administrative departments through the respective Head of Department.

3.3 Heads of Departments are required to implement this policy in respect of both paper and electronic systems operated by their Departments and are responsible for ensuring that staff, students and other persons authorised to use those systems are aware of and comply with it and associated codes of practice. They are required to appoint an Information Asset Owner for each system operated by them.

3.4 Heads of Department should ensure adequate oversight of security (in consultation with ISG), through departmental computing support staff or otherwise. The roles of Information Asset Owners may be shared across smaller departments whenever appropriate, but the Head of Department remains responsible for ensuring the roles are fulfilled.

3.5 Operational responsibility for records management is delegated to the Records Manager, who is responsible for the development of procedures, advice on good practice and promotion of compliance with the Records Management Policy.

3.6 The ISG advises the College's SLT on matters related to compliance with this Policy Statement, and is responsible for regularly reviewing it for completeness, effectiveness and usability.

3.7 The ISG in collaboration with the SLT, will from time to time make available supplementary procedures and codes of practice, and promote them throughout the College. Once approved by ISG and SLT these will also become College Policy and will be binding on all departments.

3.8 The ISG will arrange for analysis of security assessments received from departments and divisions, and report on these to SLT.

3.9 The ISG, in addition to its involvement in policymaking, provides relevant operational services. These include:

3.9.1 Incident response and co-ordination.

3.9.2 Dissemination of security information.

3.9.3 Training.

3.9.4 Consultancy.

3.9.5 Liaison with other external security teams and law enforcement agencies.

3.10 It is the responsibility of each individual to ensure their understanding of and compliance with this Policy and any associated procedures or codes of practice.

3.11 Staff with supervisory responsibility should make their supervised staff or students aware of best practice.

3.12 Staff and students who process or who are responsible for the processing of personal data, as defined in the College's Data Protection Policy, are additionally required to understand and comply with all obligations placed upon them under agreements with external parties, including but not limited to information security, integrity and perpetual confidentiality.

4. Compliance with Legislation

4.1 The College, each member of staff, and its students have an obligation to abide by all UK legislation and the relevant legislation of the European Union. Of particular importance in this respect are:

4.1.1 The Computer Misuse Act 1990.

4.1.2 The Data Protection Act 2018.

4.1.3 The Human Rights Act 1998.

4.1.4 The Regulation of Investigatory Powers Act 2000.

4.1.5 The Terrorism Act 2006.

4.1.6 The Counter Terrorism and Security Act 2015.

4.2 This Policy satisfies the Data Protection Act's requirement for a formal statement of the College's security arrangements for personal data. The requirement for compliance devolves to all users defined in (2.2) above, who may be held personally responsible for any breach of the legislation.

4.3 Relevant legislation is referenced in supporting Polices and Guidelines. Full texts are available from The Stationery Office and at http://www.legislation.gov.uk/ukpga/1998/29/contents

5. Risk Assessment and Security Review by Departments/Divisions

5.1 Information should be suitably classified according to the guidance given in the Colleges Information Classification Standard.

5.2 Information Asset Owners should adopt a risk-based approach to assessing the value of information handled, its sensitivity and the appropriateness of security controls in place or planned. Without proper assessment of the value of information assets, and the consequences (financial, reputational and otherwise) of loss of data or disruption to service, efforts to improve security are likely to be poorly targeted and ineffective. Similarly, periodic review is necessary to take into account changes to technology, legislation, business requirements and priorities; security arrangements should be revised accordingly.

5.3 Heads of Department should establish effective contingency plans appropriate to the outcome of any risk assessment. They are also required to re-evaluate periodically the security arrangements for their information management systems - at least once every three years, and additionally in response to significant departmental changes (such as turnover of key staff, commissioning of new systems etc.) A formal report must be submitted to the ISG.

6. Breaches of Security

6.1 Any individual suspecting that the security of a computer system has been, or is likely to be, breached should inform the ISG immediately. The College's ISG will advise the College on what steps should be taken to avoid incidents or minimise their impact, and identify action plans to reduce the likelihood of recurrence.

6.2 In the event of a suspected or actual breach of security, The College's ISG may, after consultation with the relevant Head of Department, require that any unsafe systems, user/login names, data and/or programs be removed or made inaccessible.

6.3 Where a breach of security involving either computer or paper records relates to personal information, the College's DPO must be informed, as there may be an infringement of the Data Protection Act 2018 which could lead to civil or criminal proceedings. It is vital, therefore, that users of the College's information systems comply, not only with this Policy Statement, but also with the College's Data Protection Policy and associated codes of practice, details of which may be found on the College website.

6.4 All physical security breaches should be reported immediately to any member of staff or the Management Team.

6.5 The Network Team will monitor network activity, receive reports from the College's Information Security Group and other security agencies, and take action or make recommendations consistent with maintaining the security of the College's information assets.

6.6 The Principal or their deputy has the authority to take whatever action is deemed necessary to protect the College against any breaches of security.

7. Policy Awareness and Disciplinary Procedure

7.1 The Contract of Employment shall state that employees are required to comply with all the Information Technology related Policies and Procedures, including such additions or amendments as may be made by the College from time to time.

7.2 As part of the induction process, managers are reminded via the standard checklist to ensure that the online security awareness training is completed.

7.3 Students are required to comply with all Information Technology related Policies and Procedures, including such additions or amendments as may be made by the College from time to time.

7.4 Existing staff and students of the College, authorised third parties and contractors given access to the College network will be advised of the existence of this Policy Statement and the availability of the associated procedures, codes of practice and guidelines which are published on the College website.

7.5 Failure of an individual student or member of staff to comply with this Policy Statement or any of the Information Technology Polices may lead to the instigation of disciplinary procedures and, in certain circumstances, legal action may be taken. Failure of a contractor to comply could lead to the cancellation of a contract.

8. Supporting Policies, Procedures and Codes of Practice

8.1 Supporting Policies, procedures and codes of practice amplifying this Policy are published with it and are available on the College website. Staff, students, contractors and other third parties authorised to access the College network to use the systems and facilities identified in paragraph (2.2) of this policy, are required to familiarise themselves with these and to work in accordance with them.

8.2 Personal data (as defined by the Data Protection Act, 2018) must be stored securely. If such data is held on mobile devices (e.g. smartphones) or removable media, it must be strongly encrypted, in compliance with the Data Protection Policy. Other forms of sensitive business data, intellectual property, etc. should, similarly, be strongly encrypted.

8.3 The ISG will issue and keep under review guidance on what constitutes an acceptable standard of encryption.

9. Status of the Information Security Policy

9.1 This Policy does not form part of a formal contract of employment with Hereford College of Arts, but it is a condition of employment that employees will abide by the regulations and Policies made by the College including this one.

10. Summary

10.1 Hereford College of Arts is committed to providing a safe and managed environment for students, staff and visitors to any part of the campus, by embedding this Policy Statement and all other Information Technology Polices it will ensure the College complies with all aspects of relevant Regulation and Law.

10.2 Everyone working across the campus has a responsibility to follow all guidance as detailed in this Policy, should any person require clarification, guidance or advice then they should contact the Operations Manager.