IT and Information Policy

Date Approved:	**21/12/2022**	**Approved By:**	**Managing Director**		
Next Review Due Date:	**21/12/2023**	**Manual ID Number:**	**BSA019**	**Version No:**	**1**
Author and Responsible Manager:	**Head of Centre**				
Applicable to:	**Staff**				
Publication:	**Staff SharePoint**				

Document Control

Version	Date	Author	Notes on Revisions

Contents

1. Scope and Purpose of the Policy

This policy and associated code of practice applies to students, employees and third parties (users) who have been authorised to access BSA IT systems and data. The documents relate to the security and operation of:

- Data processing facilities owned, licenced, leased, rented or on-loan by BSA.
- Any data processing performed in these facilities on behalf of BSA.
- Any BSA owned, licensed, written data or software programs.
- Any data, programs or hardware provided to BSA by sponsors or external agencies.

The purpose of this policy is to ensure BSA maintains the security of its IT systems and the information they hold.

2. Policy Statement

IT systems and information provide the backbone on which BSA provides an excellent learning and working environment. This policy and associated code of practice is part of a set of risk management controls that BSA puts in place so that students and employees can rely on the availability and security of those systems.

In order to control IT security risks, ensure segregation of duties, and protect the privacy of individuals, BSA controls access to its systems. Appropriate restricted access is implemented, based upon providing the minimum access a user requires to perform their duties.

The associated code of practice describes in detail, guidelines and procedures to be followed in order to achieve the objectives of this policy, including:

- Ensuring that BSA computing facilities, data and equipment are adequately protected against loss, misuse or abuse
- Ensuring that all users are aware of their responsibilities for appropriate use and protection of any systems or data they have access to
- Ensuring that BSA IT systems are monitored for unauthorised access and that appropriate procedures are in place to minimise the risk of such attempts

ISO 27002 provides best practice recommendations on information security controls for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS). Information security is defined within the standard in the context of the C-I-A triad which is the preservation of:

- confidentiality (ensuring that information is accessible only to those authorised to have access),

- integrity (safeguarding the accuracy and completeness of information and processing methods),
- availability (ensuring that authorised users have access to information and associated assets when required).

3. Accountability

3.1 The Head of Centre is responsible for ensuring that:

- the policy is implemented, regularly reviewed and updated.
- information systems, networks and applications are available when needed
- information systems, networks and applications are able to withstand and be recovered from threats to their availability and integrity
- appropriate security measures are in place, including but not limited to: firewalls, infrastructure monitoring of servers, routers, network switches etc
- measures are in place to detect and protect IT systems, applications and networks from viruses and other malicious software
- digital communications including email and internet searches over the BSA network will be monitored and inappropriate keywords/phrases identified and reported
- all applications, systems and networks are monitored for potential security breaches. All potential security breaches must be investigated and reported
- BSA Executive are advised regarding appropriate risk management in relation to IT security
- contingency and disaster recovery plans are produced for critical applications, systems and networks
- disaster recovery simulations of critical systems are performed on a regular basis

3.2 All users are responsible for reporting known or suspected breaches of IT security

3.3 Information System / Product Owners are responsible for:

- Ensuring that access is provided to only those users who require access as a function of their role
- Ensuring that access provided by local accounts in systems is revoked when employees leave
- Ensuring that roles and privileges granted to users are appropriate to their job role and that audit logs of such roles and privileges are maintained
- Ensuring the accuracy of data held within their information systems

3.4 The Data Protection Officer is responsible for:

- Ensuring that BSA is compliant with data protections and freedom of information legislation.
- Dealing with enquiries from any source, in relation to the Data Protection Act and Freedom of Information Act.
- Advising users of BSA IT and information systems of their responsibilities under the Data Protection and Freedom of Information Acts.

4 Student Involvement

4.1 Students will be made aware of the IT and Information Security Policy and associated agreement via induction

5 Linked Policies and Procedures

This policy links into other BSA policies and procedures. These include:

- Safeguarding Policy and Procedure
- eSafety Policy
- Student Misconduct Procedure
- Mobile Device Allocation Policy and Procedure
- Social Networking Code of Practice

6. Equality Impact Assessment

Impact Assessment for the 4 strands of Equality, Safeguarding, Health and safety and Sustainability	
Initial Form to be completed with Risk Assessments or as part of a proposal or change to a policy, plan or new way of working	
Title of Activity: Author and Date: Dionne McCann Nov 2020	☐ New or ☒ Revision (**Tick as appropriate)** Expected Implementation Date: Nov 20 What is the Review Date: Every 2 Years
Equality and Diversity. Which of the characteristics may be impacted upon? And, if yes, how has this been considered? What are the risks? What are the benefits?	None, no impact
Safeguarding: Are there any aspects of this proposal which could cause a Student/member of staff/visitor to feel unsafe? If yes, how has this been considered? What are the risks? What are the benefits	☐ Yes ☒ No
Health and Safety: Have any risks been identified? If yes, how has this been considered? What are the risks? What are the benefits?	☐ Yes ☒ No
Sustainability: Are there expected benefits or impacts on sustainability issues? If yes, how have these been considered?	☐ Yes ☒ No
Evidence: What evidence do you have for your conclusions and expectations for these conclusions? How will this impact be monitored for all these considerations?	Quality is monitored through both internal and external reviews
Is this policy of a high/medium or low risk? :	☐ High ☐ Medium ☒ Low