BILBOROUGH
SIXTH FORM COLLEGE

ICT Security Policy

Amended for GDPR

Reviewed: June 2021
Reviewer: H Dennis

Introduction

Business continuity is dependent on the integrity and continued availability of the College's IT systems, including computer systems, assets, infrastructure and computing environment. This policy sets out a framework for best practice to enable the College to comply with all relevant legislation and to maintain the integrity and security of IT systems to ensure these are protected from internal and external threats due to unauthorised use, modification, disclosure or destruction, whether accidental or intentional.

Effective security is achieved by working with proper discipline, in compliance with legislation and by adherence to approved College Codes of Practice. Users are advised that Information Services reserves the right to monitor, log, and collate the content of all transmissions on networks maintained by the College or individual departments as necessary for performance, fault diagnosis and for compliance purposes in relation to the College IT Acceptable Use Policy.

1. Purpose

The purpose of this IT Security Policy and associated policies and codes of practice is to set out the responsibilities for ensuring the security of IT Systems within the College, and the procedures to be followed to safeguard the resources provided and the confidentiality and integrity of the information held therein.

The objectives of this policy are to ensure that:

- All of the College's IT hardware systems, software, programs, data, network and equipment are adequately protected against loss, misuse or abuse
- All users are aware of and comply fully with this Policy and are aware of, and work in accordance with the relevant Codes of Practice
- All users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle
- All systems and environments and the information stored within are protected against unauthorised access
- Data or information on the College's systems is managed securely and in accordance with the requirements of applicable data protection laws in a professional manner and in accordance with the College's needs and expectations
- All users understand their responsibility to report without delay any incidents that may put at risk the security of the College's IT systems and environments

2. Scope

This Policy and associated Codes of Practice applies to all staff, students and visitors to the College. This includes contractors or authorised persons accessing the systems remotely. This policy covers any system which captures stores or processes information. This includes, but is not limited to, desktop computers, laptop computers, tablets, iPads, telephones, CCTV, voicemail, financial and staff/student records systems. It covers all data storage whether on site or cloud-based (hosted).

This policy is available on the College Website, Intranet and Student Portal.

3. Policy

3.1 Responsibilities

It is the responsibility of all users as set out in section 2 to ensure their understanding of, and compliance with this Policy and the associated Codes of Practice.

All College staff are responsible for the immediate reporting of any IT security related incident to the Director of Marketing and Information or in the absence of the Director of Marketing and Information, to the Principal or another member of the Senior Leadership Team.

The Director of Marketing and Information shall take appropriate steps to inform staff, students and visitors of their obligations under this policy and any other policy referred to herein.

The College and its auditors will periodically review the adequacy of IT system controls as well as compliance with such controls.

3.2 Security of equipment and data

The College's servers and core systems are accommodated in secure accommodation with a climate-controlled environment and protected power arrangements.

The college will undertake IT vulnerability risk assessments on a regular basis (up to twice per year) to detect and manage internal and external

vulnerabilities within the IT estate using vulnerability assessment and vulnerability management protocols.

The college will engage with external support to undertake penetration testing to reduce the risk of information security breaches.

Computers in general office environments are protected by user log-out and/or password protection when left unattended and outside of normal working hours.

Desktop computers or laptops in public areas are protected by a suitable lock to prevent theft.

Personal data should be stored in centrally-held systems; the storage of personal data or sensitive data on portable devices (e.g. USB memory devices) should be avoided.

The College holds personal and sensitive data about staff and students. Staff with access to this information have responsibilities under data protection law.

Copying of (or capture of) sensitive data on to any form of portable data storage device (e.g. USB memory stick, laptop, CD, Laptop etc.) or taking such data outside of the environment in which it was intended to be used (systems environment, office environment etc.) places additional responsibility on the individual. Before doing so, the individual is required to consider the following:

Personal confidential data should not leave the college campus. In this context, "leaving" the campus means the physical removal of the data to an external and insecure location. It does not mean accessing such data remotely through the normal approved and controlled access processes.

As an additional security measure, all college staff laptops are installed with full disk encryption software.

Further guidance can be provided by the Director of Marketing and Information or by referring to the Data Protection Policy.

When a member of staff leaves the employment of the college, normal practice is for their network account to be disabled immediately after the leaving date. However, it is sometimes appropriate and necessary to retain access to the account for a period of time, depending on the nature and content of the role of the person who has left.

In such circumstances, access to the network account will be disabled to the leaver upon leaving the employment of the college, but access retained for a

period of 3 months, with the need to maintain accessed reviewed termly thereafter.

Administrator account access is reviewed on a quarterly basis to ensure that only those staff entitled to have administrator access have administrator accounts.

3.3 Breaches of Security

Security of the network systems and data is paramount. During the course of their normal duties, IT Support staff may take action or make recommendations consistent with maintaining the security of College IT Systems.

The Director of Marketing and Information acting as Data Protection Officer has the authority to take whatever action is deemed necessary to protect the College against breaches of IT security. As far as is reasonably possible, any such action will be taken after consultation with the Principal or other members of the Senior Leadership Team

Any breach of security of the College's IT System could lead to loss of personal data and could be an infringement of the General Data Protection Regulation, leading to civil or criminal proceedings. It is vital, therefore, that users of College IT Systems comply not only with this policy, but also with the College's Data Protection Policy. Any user suspecting a breach or threat to IT security should inform the Director of Marketing and Information who will determine what action should be taken. In the event of a suspected or actual breach of security, the Director of Marketing and Information may make inaccessible or remove any unsafe user or login names, data and/or programs on the system from the network, computer systems and any associated equipment, pending further investigation.

Loss or theft of Confidential Information

Incidents of loss or theft of confidential information must be reported to the Director of Marketing and Information. The Director of Marketing and Information (in their role as Data Protection Officer) will follow the College's Data Security breach Management Procedure to investigate and record the circumstances of the loss or breach and if appropriate, will submit a report to the Office of the Information Commissioner.

A security breach could arise from a range of circumstances, for example the loss of password information or the loss or theft of confidential data. Such events could result in:

- Risks to system or data integrity
- Risks to the availability of systems and/or data
- Risks to the reputation of the College
- The disclosure of confidential information to an unauthorised person

Use of Email

Users should be aware that email is not a secure medium and should consider how emails might be used by other parties. In particular, users should be aware of the scope for email content to be taken out of context and it how quickly and easily large quantities of information can be distributed by email.

3.4 Compliance with Legislation

The College, and all users of its systems, have an obligation to abide by all UK legislation and relevant legislation of the European Community. Of particular importance in this respect are the following:

- Regulation of Investigatory Powers Act 2000 (RIPA), together with Regulations issued pursuant to that Act, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
- The General Data Protection Act 2018
- The Human Rights Act 1998
- The Copyright, Designs & Patents Act 1988
- The Computer Misuse Act 1990
- Freedom of Information Act 2000

4. Policy Awareness and Disciplinary Procedures

This policy is available on the College website and intranet.

All users covered in section 3.1 will be made aware of the location of this policy.

Failure of an individual to comply with this policy and the associated policies and procedures referenced within it, may lead to the instigation of the relevant disciplinary procedures. In certain circumstances, this may lead to legal action.

5. Associated Documents

Related Regulations, Policies, Processes and Codes of Conduct

- IT Systems Acceptable Use Policy
- Disciplinary Policy – Staff

- Code of Conduct for System Administrators
- Data Protection Policy
- CCTV policy

JANET Acceptable Use Policy -
http://www.ja.net/documents/publications/policy/aup.pdf

Regulations

Regulation of Investigatory Powers Act 2000 –
http://www.legislation.gov.uk/ukpga/2000/23/contents

Data Protection Act 1998 –
http://www.legislation.gov.uk/ukpga/1998/29/contents

Human Rights Act 1998 –
http://www.legislation.gov.uk/ukpga/1998/42/contents

Copyright, Designs & Patents Act 1988 –
http://www.legislation.gov.uk/ukpga/1988/48/contents

The Computer Misuse Act 1990 –
http://www.legislation.gov.uk/ukpga/1990/18/contents

Freedom of Information Act 2000 –
http://www.legislation.gov.uk/ukpga/2000/36/contents

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 –
http://www.legislation.gov.uk/uksi/2000/2699/contents

6. Status

This policy does not form part of a formal contract of employment with the College, but it is a condition of employment that employees abide by this, and other College policies that have been approved by the College Corporation. Likewise, the policy is an integral part of the Student Disciplinary Procedure.

7. Review

This policy and associated procedures will be reviewed at least every year or more often if there is a significant change in legislation or a new information system introduced.