BORDERS COLLEGE

Appropriate Usage of Electronic Systems Policy

November 2023

History of Changes

Version	Description of Change	Authored by	Date
1.1	Date changes and title changes	Debbie Kerr	November 2016
1.2	Date change and name change from “Electronic Systems Policy and Procedure”. Update of document to reflect range of electronic communication systems (not just email). Removal of sections relating to requirements to keep multiple copies of key data (now covered by ISLT backup). Document formatting	Conor Bradley	February 2021
1.3	Minor wording changes, dates and titles	Debbie Kerr	November 2023

Electronic Systems Policy

1 Introduction

1.1 The use of electronic systems such as e-mail, internet and other systems within the College is encouraged, as its appropriate use facilitates communication and improves efficiency. Its inappropriate use, however, may cause many problems, ranging from minor distractions to potential legal claims against both the individual and the College.

2 Scope

2.1 The purpose of this policy is to ensure the appropriate use of all electronic systems by all staff. This policy and procedure sets out the College's view on the correct use of electronic systems, and explains how this can be achieved, as well as the College's response to inappropriate use.

3 Key Principles

3.1 Authorised Use

The electronic systems are available for communication on matters directly concerned with the business of the College. Members of staff using the systems should give particular attention to the following points.

3.1.1 The Standard of Presentation

The style and content of a piece of text must be consistent with the standards that the College expects from written communications.

3.1.2 The Extent of Circulation

Individuals are often swamped with irrelevant information because the senders have not given sufficient thought to who really needs to receive the information. Information should only be sent to those members of staff for whom they are particularly relevant.

3.1.3 The Appropriateness of electronic systems communication

Staff should consider the best usage of electronic systems for communication. Hasty messages sent without proper consideration, can cause unnecessary misunderstandings with both colleagues and customers. "Flame-mails" – the sending of messages that are abusive or critical – can be a source of stress and damage work relationships. Any individual or organisation that considers electronic communications to be defamatory has the right to take legal action.

3.1.4 The Visibility of E-Mail

If the message is confidential, the user must ensure that the necessary steps are taken to protect confidentiality.

3.1.5 Personal Use

The College recognises that due to the nature of remote, home and mobile working, staff are likely to conduct some personal use of College provided electronic devices. This is acceptable providing it meets the requirements elsewhere in this document. Staff should however be aware that the College uses remote auditing and scanning tools to protect its devices and data from attack or malware. These tools will also scan any personal use of the device. Staff are also advised not to store personal data on their College device as the data cannot be recovered in the event of the device being damaged or remotely wiped by the College e.g. to protect the device in the case of a cyber-attack.

3.2 Unauthorised Use

3.2.1 E-Mail Contracts

Offers or contracts transmitted via E-mail are as legally binding on the College as those sent on paper. Contracts should therefore be sent to a member of the Executive for authorisation.

3.2.2 The College will not tolerate the use of the systems for any of the following:

- any message that could constitute bullying or harassment (e.g. on the grounds of a protected characteristic)
- online gambling
- accessing pornography
- posting confidential information about other employees, the College, its customers or suppliers. Contractual non-disclosure obligations concerning the College's confidential information still apply when using the internet and E-mail system, downloading or distributing copyright information
- downloading entertainment software or games or to play games against opponents over the internet
- downloading or distributing pirated software or data
- propagation of any virus or malware

3.3 All existing College policies apply to conduct on electronic systems, especially, but not exclusively, those that deal with intellectual property protection, privacy, misuse of College resources, harassment, equal opportunity, information and data security and confidentiality. Any unauthorised use of electronic systems may result in disciplinary action which may include dismissal.

3.4 Freedom of Information and Data Protection

Electronic systems communication is covered by both the data protection legislation and the Freedom of Information Act.

When a freedom of information (FOI) request is received asking for all correspondence on a subject, the College is required to check for data (including communications) relating to that subject. This also applies where an individual submits a Subject Access Request to the College for a copy of all the data the College holds on them. Please be aware that anything you write in an email could end up in the public domain following an FOI request or SAR. There are exemptions that allow us to refuse to publish, but these are in very limited and for specific circumstances. It is best to assume that information could be shared publicly and write your correspondence accordingly.

Information about an individual is protected under data protection legislation. This means that any electronic communications containing personal information must be sent confidentially and stored securely. An individual can request to see all correspondence relating to them, including emails, Teams messages etc.

3.5 Electronic Communications Containing Personal Information

When writing electronic communications containing personal information, care must be taken in selecting a subject title. Avoid using names and other identifying information within the subject heading. If an email message is being sent regarding an individual, then a general heading for the email should be used rather than the individual’s name and the email should be marked confidential.

Staff should take care that confidential data is not shared with other staff or students. This could be when a device is connected to a display board or projector or when working in a shared area. Staff should take appropriate measures to avoid sharing confidential data inappropriately.

Data defined as containing ‘protected characteristics’ by data protection legislation should not be conveyed by unsecured email to external email addresses. Sensitive information includes the Protected Characteristics of race, ethnicity, belief, religion, sexual orientation as well as information about trade union membership, political views, health, sex life, criminal offences. Staff transferring data such as this to external partners should contact ISLT to discuss secure routes of transfer.

3.6 Implementation of the Policy and Procedures

3.6.1 Training on use of electronic systems will be included as part of the induction of all new members of staff. Managers are required to ensure that all new members of staff have received the training prior to using the systems.

3.6.2 Regular monitoring of electronic systems use will be carried out on a random basis by the IT & Digital department. The College reserves the right to inspect any and all files stored in private areas of the College network and audit logs of user actions to ensure compliance with these guidelines. Line managers will be notified of inappropriate use of the systems.

3.6.3 All system users will be issued with a unique individual password which is confidential to the user. Access to systems using another member of staff's password without prior authorisation may result in disciplinary action, which may include dismissal.

3.6.4 Members of staff who feel that they have cause for complaint as a result of electronic system communications should raise the matter initially with their immediate line manager. If necessary, the complaint can then be raised through the grievance procedure.

4 Responsibilities

4.1 The SLT are responsible for the implementation of this policy.

4.2 The Director of People Services is responsible for the operation of this policy.

4.3 The Director of IT and Digital is responsible for the management of electronic systems.

4.4 All staff are responsible for ensuring compliance with this policy and procedure.

5 Related Documents

5.1 Discipline Policy and Procedure

5.2 Grievance Policy and Procedure

5.3 Information Security Policy

6 Review

This policy will be reviewed every 3 years.

Status:	
Policy Dated:	November 2023
Author:	Director of People Services
Review Date:	November 2026
Equality Impact Assessed:	27th September 2021