Electronic Communications Policy

Date Approved:	**07/01/2023**	**Approved By:**	**Managing Director**		
Next Review Due Date:	**31/01/2024**	**Manual ID Number:**	**BSA31**	**Version No:**	**2**
Author and Responsible Manager:	**Head of Centre**				
Applicable to:	**Staff**				
Publication:	**Staff SharePoint**				

Document Control

Version	Date	Author	Notes on Revisions

Contents

1. Purpose

The purpose of this policy is to address the use of electronic communications and will apply every individual who have been granted access to any IT facilities and services provided by or through BSA.

This includes, but is not limited to:

- All members of staff including temporary and agency staff
- All students
- Third parties i.e. contractors or subcontractors engaged to undertake work for BSA
- External Quality Assurers

2. Scope

This policy applies to the use of all IT facilities and services and include but are not limited to:

- All computers, irrespective of ownership when connected to BSA network or facilities from any location
- Physical or virtual computers, servers and desktops
- Mobile devices, laptops, tablets and smart devices
- Email and other electronic communications systems
- Telephones
- All data storage systems
- External cloud computing providers
- Virtual learning environments

Every employee has duty of care for equipment such as phones and computers that are provided for their use.

3. Electronic Communications and the Law

The most relevant legislation regulating electronic communications are:

- The Data Protection Act 1998 (relating to the use of personal information)
- The Data Protection Regulation (2018)
- Computer Misuse Act 1990 (which defines activities such as hacking or the deliberate introduction of viruses a criminal offence)
- Equality Act 2010

Breach of any of the above can constitute a criminal offence. Where BSA believes a criminal offence has taken place, it has a duty to inform the police. Using BSA's facilities in any way to break the law will be considered as gross misconduct under the Disciplinary Procedure.

4. Content and Usage

Internet Access is restricted through the use of web filtering software which prohibits the majority of inappropriate or offensive material. The content of emails is also monitored for policy enforcement, messages containing either words or attachments which breach the policy are automatically blocked.

You should be confident that anything which you access or send meets the following criteria:

- There is a legitimate business need (other than mundane personal use described later)
- That it is within the law and does not breach copyright
- That you have the authority to send the message (i.e. when committing BSA to a course of action)
- General advice on e-mail etiquette can be found in Appendix 3. A template for 'Out of Office' messages is supplied in Appendix 4.

5. Home Working

The rules outlined in this Policy apply to any equipment and systems provided or accessible to you when working from home.

If you work from home on an occasional basis it is important that you are contactable to BSA and your colleagues. Arrangements should be made with your line manager and communicated with colleagues.

COLLEAGUES MUST NOT REVEAL PERSONAL HOME/MOBILE TELEPHONE NUMBERS WITHOUT PRIOR PERMISSION FROM THE HOME WORKER.

6. Personal Use

Occasional and reasonable use of BSA's Electronic Communications systems is permitted providing that:

- It is in your own time i.e. outside normal working hours.
- It does not interfere with work performance or divert you from your duties.
- It is not used for furthering outside business interests or for personal monetary gain.
- The use of the Internet conforms to all other requirements in this policy.
- Usage does not adversely affect the performance of the e-mail system or academy network.

For the avoidance of doubt employees are advised to not publish anything that may bring themselves or BSA into disrepute e.g. if you have any inclination that your comment/post may be taken in the wrong way don't say it.

The only personal usage tolerated is in the following areas:

- Email
- Internet Access
- Social Networking sites, Personal blogs

Email

A minimal level of mundane personal use is tolerated. This use must be outside your working time. Be aware that emails are monitored and that personally sensitive information should not be sent. Messages should not contain anything that others may find offensive or distasteful.

Mobile Phones

Mobile phones should not be used during the workday, unless in an emergency, and should be kept in a secure place on silent or turned off during delivery sessions. Staff are permitted to use their mobile phones during break times

Internet Access

Limited personal use is tolerated outside of working time. Although every attempt is made to prevent access to unsuitable sites it is your responsibility not to access any sites containing unsuitable material. Be aware that all internet access is routinely monitored and logged and sites containing unsuitable material are prohibited at all times. The downloading of information for personal use is not permitted at any time. All internet connections should be via BSA's network.

Social Networking Websites, Personal Blogs etc

Social networking websites, blogs (personal diary accounts) and other such communication methods are useful tools for:

- promoting BSA's services and the activity of the Centre
- accessing professional networks/information
- communicating with hard-to-reach groups e.g. young people, community groups etc.
- publicising events and news stories

Social networking sites are those which contain personal information

about the respective individual and where social interaction between different parties take place. These sites are very popular and whilst we cannot be prescriptive about what you do in your own time out of work, it is necessary for us to outline what we consider would be detrimental behaviour or written content on a site that could potentially lead to disciplinary action being taken against you.

This section of the Electronic Communications Policy applies to the content that you publish on the internet (e.g. your contributions to blogs, message boards and social networking or content sharing sites) even if created, updated, modified or contributed to outside of working hours or when using personal IT equipment.

Cautionary advice – Personal Use on Personal Equipment

- The Internet and its social networking sites, blogs (personal diary accounts), message boards, forums and content sharing sites are open to all to view, therefore, for your own safety and protection, caution must be exercised when using such sites.
- Anything that you publish, particularly personal information e.g. date of birth, address, photographs etc may be used by others either for illegal or nuisance purposes e.g. identity theft, spam e-mails.
- Where you identify yourself as working in a public facing role that could be deemed contentious, such information could also give rise to unwanted attention from service users.
- Any illegal activity which is posted on the Internet in an open forum, can also be viewed by the Police or other government agencies.
- Employees of BSA are ambassadors for the company and should be aware that any serious misconduct or criminal offences committed during or outside working hours which could bring BSA into disrepute may result in disciplinary action being considered.
- Personal opinions should not be stated in blogs relating to official business. If a personal blog clearly identifies that you work for BSA, and you express any idea or opinion, then you should add a disclaimer such as “these are my own personal views and not those of BSA. Please note that this does not preclude BSA from taking action in cases it considers misconduct.

Guidelines for use of social networking sites and blogs

BSA recognises that social media is now an important business tool and that tools such as Twitter are important sources of information and to create professional networks.

A small group of BSA employees will represent BSA on Twitter and Facebook. Other

employees should not create posts on social media purporting to represent official BSA opinion.
The following applies to employees who are either provided with access to social networking sites, blogs or other such communications tools for work purposes or use of such tools in an employee's personal time using BSA or personal equipment.

Employees must not:

- Reveal confidential information about BSA in online postings. This might include revealing information relating to BSA's children and young people, business plans, policies, employees, governors, contractors, financial information or internal discussions. This list is not exhaustive and you should think carefully before making any postings. Please consult your line manager if you are unclear about what might be deemed confidential.
- Criticise or embarrass BSA, its children, young people and families or employees in a public forum (including any website), whether in jest or otherwise. You should respect the reputation of BSA and the privacy and feelings of others at all times. If you have a genuine complaint to make about a colleague you should raise the matter via your line manager using the correct channels e.g. Grievance Procedure. If you have a concern or criticism about BSA and its practices you should raise this via your line manager or via the whistleblowing policy.
- Post comments that may be derogatory or defamatory towards colleagues, senior leaders, governors, children, young people and/or their families or contractors or may be deemed to be intimidatory or constitute harassment, whether in jest or otherwise. This list is not exhaustive and you should think carefully before making any postings.
- Use bad language, innuendo, discriminatory statements etc. that could potentially bring the Trust into disrepute.
- Publish film or photographs on the Internet of activity that may bring the BSA into disrepute.
- Publish photographs of children or vulnerable adults on the Internet (without prior consent) in breach of safeguarding legislation.
- "follow" members of the public using a BSA account as this could be misconstrued.

Request Process

In order for employees to establish social media accounts for work purposes they must first seek the approval of the Head of Centre who will in turn discuss the request with the Managing Director.

Unacceptable Use

The accessing or distribution of offensive, illegal or unsuitable material is unacceptable and subject to disciplinary action and/or prosecution.

Offensive material is anything which is abusive, intimidating, malicious or insulting. The persistent abuse of power, or the belittling of someone, either in public or private, which makes them feel upset, threatened, humiliated, vulnerable or undermines their self-confidence, through the use of Information Technology is unacceptable and will be deemed to be bullying or harassment.

Employees must not engage in:

- Posting information that may tend to disparage, threaten, or harass others on the basis of gender, race, age, disability, religion or belief, sexual orientation or national origin;
- Excessive personal use of the internet and social networking sites on BSA or personal equipment during working time;
- Posting statements that are defamatory or information that is false or misleading concerning BSA or other organisations and their services/products;
- Distributing confidential or sensitive information about BSA or its children and young people that might compromise its confidentiality;
- Deliberately using email in such a way that it constitutes bullying or harassment;
- Originating or participating in email chain letters;
- Substantial personal use of email, including the transmission of large documents or programs which will add an unnecessary burden to the network;
- Sending jokes, games and other non-work related emails, in a “chatty” and informal style could lead to problems for both BSA and its employees – do not assume others share your sense of humour.
- Sending or receiving inappropriate material via e-mail (either within an email or as an attachment) such as adult material (pornography), racism / hate, drugs, terrorist and violent activities, gambling, share dealing, paedophilia etc (unless specifically for work purposes).
- Receiving, archiving, storing, distributing, editing or recording sexually explicit material or materials of a disturbing nature using the BSA’s network or computing resources.
- The use of Internet based email accounts i.e. Hotmail is prohibited unless a case for access has been approved.

The list above gives examples of the types of behaviour which constitute violation of the policy. This is not an exhaustive list and there may be other violations which are not listed here.

Misuse

Where misuse has been identified, employees need to be aware that disciplinary action will be taken. The following, although not an exhaustive listing, is an example of actions, which would warrant serious disciplinary action with possible suspension/dismissal and in certain cases potentially criminal prosecution:

- Employees accessing certain websites e.g. child pornography and terrorist sites for non-work purposes.
- Employees accessing and/or distributing materials of an unsuitable nature via e-mail or within an e-mail attachment.
- Defacement of BSA website.
- Any involvement in 'hacking', virus propagation and spamming of the BSA or any website or contravention of The Computer Misuse Act 1990.

7. Security arrangements and controls

Security incidents, including the following examples, must be reported to your line manager immediately:

- Where it is believed another person is using an employee's ID/ password. Attempts to log on as another user will result in cancellation of e-mail and Internet access and may result in disciplinary proceedings. Internet passwords should not be disclosed to anyone else. Each Internet user is totally accountable and responsible for usage on his / her account: this is also applicable where users have one "log on" password that gives access to both Internet and e-mail.
- If an employee believes another user is accessing prohibited material.
- Construction of personal / business [non-BSA] websites.
- The settings of the PC anti-virus software being amended or disabled.
- Employees engaging in 'hacking' activities into non-BSA web-sites (serious disciplinary action may result).
- If an employee accidentally accesses a prohibited site – this should be reported to the Line Manager as soon as possible after the incident and details of the incident should be logged.

Unauthorised devices e.g. i-pods, cameras, non-BSA memory sticks,

external hard drives should not be connected to BSA computers as this poses a risk to the security of BSA's network.
Any suspicious e-mails or attachments should not be opened or forwarded to others as they may contain a virus.

When using telephones, either landlines or mobile handsets, and whether for personal calls or in the course of your duties, you should take into consideration the location where you are making the call, whether or not it will distract colleagues and whether or not the nature of the telephone conversation is appropriate in front of colleagues and/or visitors to the Centre. It is also important to be courteous and take into consideration that colleagues may not want to be interrupted by your telephone conversations.

Personal mobile phones should not be used during working hours unless necessary and should be kept on silent/vibrate when in the office.

8. 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