



Broadway Academy Trust Policies

Our Children. Our Community. Believe it can be done!

Policy on Acceptable Use of Information and Communications Technology, the Internet and Social Media

Approved by: Deep Services, Finance, Audit and Premises Committee

Date approved: December 2025

Next review date: December 2027



Contents

	Section	Page
1	Introduction	2
2	Responsibilities	3
3	E-mail guidelines	3
4	Internet and computer guidelines	5
5	Telephones	7
6	Social media usage guidelines	7
7	Dealing with unsuitable / inappropriate activities	9
8	Responding to illegal or unacceptable use incidents	10
9	Other incidents	11
10	Academy actions and sanctions	12

This policy set out Broadway Academy's position on acceptable use of the Internet, computers within the Academy and social media which identifies the Academy

It has been produced in the light of current legislation including the following Acts:

- Copyright, Designs and Patent Act (1988)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Equality Act (2010)
- Data Protection Act (2018)

Please see the Academy's [On-line Safety Policy](#) for guidance on safeguarding and digital safety for students

1. Introduction

1.1 Purpose

This is a corporate statement of good practice to protect the Academy from casual or intentional abuse of information and communications technology including intranet (SharePoint), internet, email or social media use. Electronic communications are basic tools of day- to -day Academy life and, if abused, can create several threats and legal risks, as well as the potential costs of time to resolve and manage them. Although these tools are provided primarily for 'business' use the Academy accept that on occasion they may be used for personal use. At all times users should consider these guidelines and adhere to them.

1.2 Scope

These guidelines apply to all employees, workers, agency staff, volunteers and governors who have access to computerised equipment including e-mail or the internet on behalf of Broadway Academy.

1.3 Publicising the guidelines

All users will be notified of the Policy on Acceptable Use of Information and Communications Technology, Internet and Social Media.

New starters should not be given access to e-mail or the internet until they have seen and accepted these policies. This is the responsibility of their line manager as part of the Induction checklist issued on the new starter's arrival.

1.4 Monitoring

Broadway Academy has third party "firewall" software and systems in place to monitor all computer usage, and these will be checked and analysed on a regular basis. Certain internet sites will be blocked if they are deemed to hold inappropriate or sexually explicit material.

Although the Academy respects the privacy of every individual throughout the organisation, all external mail (both incoming and outgoing) will be checked for content and attachments to always make sure that the security and integrity of

the Academy is not impeded. The sender of any message that is intercepted will be notified immediately by e-mail response from the LEA service provider.

1.5 Disciplinary Action

Action will be taken using the Academy's Disciplinary Policy against any users who are found to breach the policies outlined in these guidelines.

Significant abuse, particularly involving access to pornographic or offensive images constitutes gross misconduct which could lead to summary dismissal.

2. Responsibilities

2.1 Governing Board

This policy and guidelines have been approved and adopted by Governing Board of Broadway Academy.

2.2 Managers and Supervisors

It is the responsibility of all managers and supervisors that the policies and guidelines are properly implemented and policed.

2.3 Trustnet

Trustnet will ensure that users are notified of their responsibilities about the use of e-mail and the Internet. Through the use of 3rd party "firewall" software, Trustnet will monitor Internet and e-mail use and the subsequent analysis of this data (in accordance with the Internet and E-mail Analysis procedure).

Appropriate security virus prevention mechanisms will be maintained and updated to meet the ongoing requirement of the Academy (in accordance with the Virus Protection procedure).

2.4 Employees

All staff, with access to computerised equipment which may or may not include access to e-mail and the Internet, will be held responsible for complying fully with the computer policies and guidelines.

3. E-mail guidelines

3.1 Personal Use

Employees are permitted to send personal e-mails on a limited basis if this does not interfere with their job responsibilities. It should be noted that any e-mail messages are not guaranteed to be private and remain the property of Broadway Academy.

3.2 Confidentiality

Messages sent and received via the Internet are regarded by the Company's Act as having the same legal status as a corporate letter. Any material that is viewed as highly confidential or valuable to the Academy should not be e-mailed externally.

The disclaimer statement will be attached to all e-mails. In no instance should the disclaimer be tampered with.

It should be remembered that the Internet does not guarantee delivery or confidentiality.

It should be noted that there are systems in place that can monitor, review and record all e-mail usage, and these will be used. Analysis of this information may be issued to managers if thought appropriate. No user should have any expectation of privacy as to his or her e-mail.

3.3 Etiquette

Broadway expects emails to be courteous and for people to check them before sending them out. Ensure that the grammar is reasonable. At all times users should use appropriate etiquette when drafting e-mails, e.g. e-mails should not be written in capitals as this can be perceived as 'shouting'. Guidance on "netiquette" is provided by lots of helpful websites, e.g. the BBC maintain the following site should you want to know more:

<https://www.bbc.co.uk/blogs/webwise/netiquette>

3.4 Dissemination of Information

In cases where information of a general nature is circulated via e-mail or on an electronic notice board, database or web site, it is the responsibility of a relevant manager or supervisor to ensure that members of staff have access to information.

When sending information of a personal nature via any means, every effort should be made to ensure it goes to the right person, and they are indeed authorised to receive it. Appropriate encryption of any data should be applied when using IT system. Please read our Data protection policy which does comply with current GDPR regulations or email our team on GDPR@broadway-academy.co.uk should you have any questions.

3.5 Inappropriate behaviour

Users should not send messages that contain any unsuitable material or defamatory statements about other individuals or organisations.

Messages should not contain material or language that could be viewed as offensive to others or as contravening the Academy's Equality Policy.

3.6 Canvassing, lobbying, advocacy or endorsement

Material, which could be construed as canvassing, lobbying, advocacy or endorsement should not be sent by e-mail, particularly if this is commercially- or politically- based, and more particularly if this it expresses a personal, rather than an Academy, view. If in doubt, consult your line manager.

3.7 Virus Protection

To prevent the risk of potential viruses, users should not open any unsolicited e-mail attachments or independently load any software, including screensavers, onto their computers. If a user does inadvertently open a message or attachment that contains a virus or clicks a link on what may be a phishing email, they need to contact the Academy's network manager immediately and close the message and attachment. It should not be accessed again without approval.

3.8 Security

E-mail is an effective way of communicating confidential information. This is only the case, however, if data is encrypted and passwords are secure. To maintain security, it is good practice for users to change their passwords regularly as outlined in our Data Protection Policy. Please read section 4.8 below.

E-mail programmes should not be left running or unattended in any circumstances where this may lead to unauthorised access. The system should be closed and re-opened on return. In no instances should a user login using a colleague's password unless permission has been given by someone authorised to give such permission.

3.9 Housekeeping

Good housekeeping practices should be adopted so that files are archived to a separate file as described in our data protection policy. Files containing personal data should be deleted in line with the data retention guidelines set out in the Academy's Data Protection policy (section 4.5 and the appendix on data retention periods).

4. Internet and computer guidelines

4.1 Rules for use

Users should not download, stream or view any material that is not directly related to their job responsibility subject to 4.2 below. This especially relates to images, videos games etc. The network manager must be notified before any software is downloaded for use: all downloaded software needs to be properly licensed and registered. Any such software automatically becomes the property of the Academy. There are systems in place to monitor all computer usage including any software downloads.

4.2 Personal use of the Internet

Employees are permitted to access the internet for personal use on a limited basis with the approval of their line management if this does not interfere with their job responsibilities. This should be in the employee's own time, i.e. before or after contracted time, or with the permission of line management.

It should be noted that there are systems in place that monitor and record all computer and Internet usage. No user should have any expectation of privacy as to his or her computer usage. Analysis of this information may be issued to managers if thought appropriate.

4.3 Respecting copyright

Employees with Internet access must comply with all copyright laws of all countries relevant to Education Services. Users must not intentionally download any material that holds a copyright notice and must not infringe any copyright. This also relates to downloading and copying unlicensed software.

4.4 Security

Systems are in place to protect the Academy's information systems. However, users must also be aware of the potential risks associated with accessing the

Internet. Employees are reminded that newsgroups are public forums where information about the Academy should not be revealed. Also, see section 4.2 above.

Users are also reminded that unauthorised usage could include accessing e-mail or the Internet via a computer other than your own, including another member of staff's computer. Unpermitted access is not permissible.

4.5 Virus protection

Although virus protection software is installed on all networked computers, users should be aware of the potential hazards associated with computer viruses. Any files that are downloaded will be scanned for viruses before being accessed. If you have any concerns about viruses on the Internet or think you may have accessed material that contains a virus, please contact the network manager.

4.6 Inappropriate websites and material

Under no circumstances should a user access a web site or other material that contains sexually explicit or offensive material. This includes pictures, movies, text or sound files. If you find yourself connected to such a site inadvertently, you should disconnect from that site immediately and notify the network manager IT Director.

Because individuals may consider a wide variety of material offensive, users should not use an Academy computer to open, store, view, print or redistribute any material that is not directly related to the user's role or the Academy's activities without prior permission of their line manager. For a definition of offensive, refer to the list at section 7.1.

4.7 Personal use of Computer Equipment

Computers are provided throughout the Academy for staff and pupils to use for Broadway Academy work. They may be used for personal use on a limited basis with the approval of their line management if this does not interfere with their job responsibilities. This should be in the employee's own time, i.e. before or after contracted hours or with the permission of line management.

It should be noted that there are systems in place that can monitor and record all computer usage, and these will be used. No user should have any expectation of privacy as to his or her computer usage. Analysis of this information may be issued to managers if thought appropriate.

4.8 Personal data transfer into or out of the Academy

Staff must ensure that they:

- Always take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media **the data must be encrypted and password protected.**

4.9 Bring your own device

Staff have the opportunity to use their personal electronic devices for work purposes when authorised in writing, in advance, by the staff member and ICT Director. These devices should only access internet resources whilst on site and no access to our wider network infrastructure will be granted. While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of company devices. Staff should also accept that the Academy will not be held responsible for any lost or damage to personal owned technology brought onto the site. (See Appendix 1 Staff BYOD Forms).

4.10 Use of AI

The integration of AI tools in the classroom is permitted to augment traditional teaching methods, facilitate personalised learning experiences, and support educators in creating engaging and effective lessons.

However, staff must adhere to all relevant data protection and privacy regulations when using AI tools, ensuring the secure handling of student or staff data.

Any attempt to manipulate or disrupt the normal functioning of the school network via AI or compromise the integrity of school data is strictly prohibited.

5. Telephones

5.1 Telephones (both mobile and land lines) are provided throughout the Academy for staff to use for Broadway Academy work. The Academy does permit personal use on a limited basis with the approval of their line management if this does not interfere with their job responsibilities. This should be in the employee's own time, i.e. before or after contracted time, or with the permission of line management.

5.2 It should be noted that there are systems in place that monitor and record all telephone usage. No user should have any expectation of privacy as to his or her telephone usage. Analysis of this information may be issued to managers if thought appropriate.

5.3 The Academy will not be held responsible for any lost or damage to personal mobile phone technology brought onto the site.

6. Social Media usage guidelines

6.1 Broadway Academy has a duty of care to provide a safe learning environment for students and staff and could be held responsible, directly or indirectly, for the actions of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race, disability, sexual orientation, religion or age or who defame a third party may render the Academy liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

6.2 The Academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the Academy:

- ensuring that personal information is not published
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk

6.3 Broadway Academy uses social media as part of its communication and public engagement strategy. The Academy also recognises that most staff will utilise social media in some form

6.4 Social media use on behalf of the Academy

Academy staff should ensure that, when using social media on behalf of the Academy:

- no unauthorised reference is made in social media to students, parents / carers or Academy staff
- they do not engage in online discussion on personal matters relating to members of the Academy community
- personal opinions are not attributed to the Academy

6.5 Personal social media use

Academy staff should ensure that, when using personal social media:

- in all cases, where a personal account is used which associates itself with the Academy or impacts on the Academy, it must be made clear that the member of staff is not communicating on behalf of the Academy with an appropriate disclaimer. Such personal communications are within the scope of this policy
- identifiable references are not made in social media to students, parents / carers or Academy staff they do not engage in online discussion on personal matters relating to members of the Academy community
- they do not accept or make contact or 'friend' requests from students
- security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information

6.6 The Academy permits reasonable and appropriate access to private social media sites, where it is permitted by our filtered broadband provider, in line with the provisions for personal internet and email usage i.e. in the employee's own time, before or after contracted hours or when on a break, or with the permission of line management. However, where excessive personal use of social media in the Academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

6.7 Personal communications which do not refer to or impact upon the Academy and are made in employee's own time are outside the scope of this policy

6.8 Monitoring public social media

As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the Academy. The Academy will respond to social media comments made by others according to a defined policy or process

6.9 The Academy's use of social media for professional purposes will be checked regularly by the IT Director and Online Safety Group to ensure compliance with the Academy policies.

7. Dealing with unsuitable / inappropriate activities

7.1 Some computer activity e.g. accessing child abuse images or distributing racist material is illegal and is banned from the Academy and other technical systems. Other activities (e.g. cyber-bullying) are illegal and could lead to criminal prosecution. There are also a range of activities which may be legal, but which are inappropriate in an Academy context, either because of the age of the users or the nature of those activities.

Broadway Academy defines the activities below as inappropriate for staff users. Staff and others should not engage in these activities in / or outside the Academy when using Academy equipment or systems.

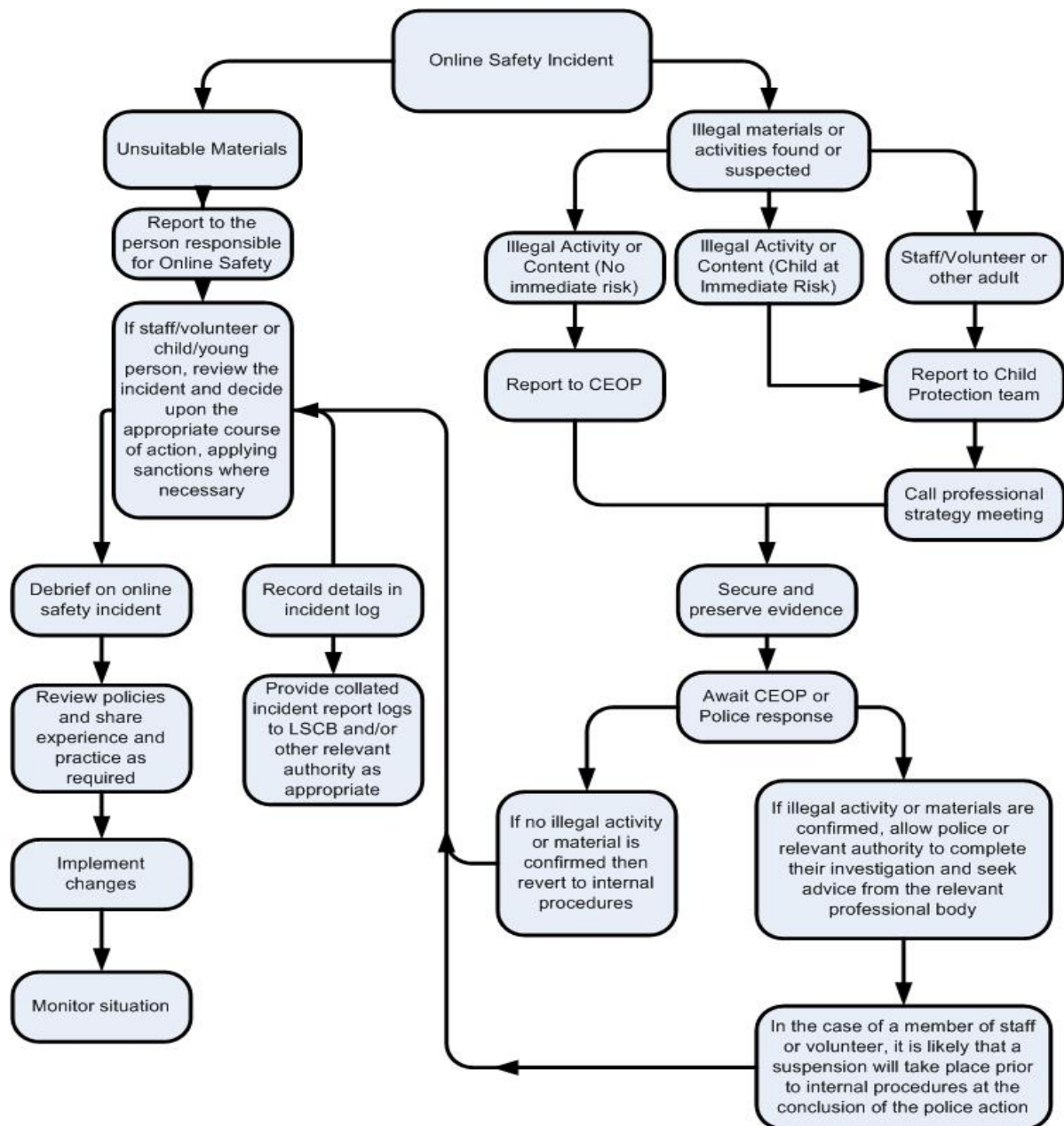
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978
- grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003
- possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008
- criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986
- pornography
- promotion of any kind of discrimination
- threatening behaviour, including promotion of physical violence or mental harm
- promotion of extremism or terrorism
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the Academy or brings the Academy into disrepute
- creating or propagating computer viruses or other harmful files
- unfair usage (downloading / uploading large files that hinders others in their use of the internet)

8. Responding to illegal or unacceptable use incidents

8.1 The flowchart below sets out the process to follow in the event of illegal or unacceptable use incidents. If there is any suspicion that any computer or social media use may contain child abuse images, or if there is any other suspected illegal activity, use the right-hand side of Flowchart for responding to online safety incidents and report immediately to the police.

Flowchart for responding to illegal and unacceptable use incidents



9. Other Incidents

9.1 It is hoped that all members of the Academy community will be responsible users of digital technologies, who understand and follow Academy policy. However, there may be times when infringements of the policy take place, through careless, irresponsible or, very rarely, through deliberate misuse.

9.2 In the event of suspicion about unacceptable use, the procedure used will include the following:

- More than one senior member of staff will be involved in this process - to protect individuals if accusations are subsequently reported
- Investigations under the procedure will be conducted using a designated computer that will not be used by students and, if necessary, can be taken off site by the police should the need arise. The same computer should be used for the duration of the procedure.
- Relevant staff will have appropriate internet access to conduct the procedure and the sites and content visited will be closely monitored and recorded (to provide further protection).
- The URL of any site containing the alleged misuse will be recorded and the nature of the content causing concern described. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the Online Safety Group will need to judge whether this concern has substance or not. If it does appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Referral to national / local organisation (as relevant).
 - Police involvement and/or action

9.3 **If content being reviewed includes images of child abuse, the monitoring should be halted and referred to the police immediately. Other instances to report to the police include:**

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

9.4 It is important that all the above steps are taken as they will provide an evidence trail for the Academy and the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

10. Academy Actions and Sanctions

- 10.1 It is more likely that the Academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the Academy community are aware that incidents have been dealt with. Incidents of misuse by staff will be dealt with through normal disciplinary procedures.

Appendix 1

Broadway Academy Staff Bring Your Own Device Agreement

Definition of “Device”

For purposes of BYOD, “Device” refers to a privately owned laptop or tablet that can be used for accessing the internet, running Office 365 products and other education resources. Mobile phones, iPads, smart watches, Kindles and other personal devices are also subject to this agreement. Personal IT equipment not declared within this agreement should not be brought into or used within school.

Internet

Internet access is only allowed through the Broadway wireless network. The wireless networks provide the same filter as workstations within school. Personal internet connective devices such as but not limited to mobile phones / mobile network adapters are not permitted to be used to access outside internet sources at any time.

Security and Damages

Responsibility to keep the device secure rests with the individual owner. Broadway Academy is not liable for any device stolen or damages on any school campus. If a device is stolen or damaged, it will be handled through the administrative office similar to other personal artifacts that are impacted in similar situations. Protective cases for devices are encouraged.

B.Y.O.D. Staff Agreement

Staff members should only use an internet enabled device within school grounds if the below form has been completed. Staff are reminded all data policies including the **acceptable use and Data Protection apply to this and any other device**. We also ask staff not to engage in activities which may stream large amounts of bandwidth, such as videos, music or live TV.

Responsibility for Devices

- The technology devices staff bring to school are their responsibility.
- School personnel assume no responsibility for personal devices if they are lost, damaged, or stolen.
- Personal devices may be subject to investigation in accordance with school policy.
- Staff are to keep their devices secure at all times and not share them or loan them to others.
- Each staff member is responsible for his/her own device, including set up and maintenance. Broadway technicians will not diagnose, repair, or work on a staff member’s personal device.
- **No photos, audio recordings, or videos are permitted while on school property.**
- Staff understands that there is no access to the school file server. Files may have to be saved on the Office 365 cloud. No data should be transferred onto any personal device.
- Staff realises that printing from personal laptops will not be possible at school.
- Data usage will be monitored by Broadway Staff.

Broadway Academy BYOD Agreement

Staff Agreement Form

I understand and will abide by the BYOD Agreement.

Printed Name of Staff Member

Signature of Staff Member

Date

Printed Username of Staff

Type of device: _____

Serial Number of device: _____

Identifying marks/labels on device: _____