Brook Learning Trust
Digital Communications Policy

At Brook Learning Trust we bring together our unique academies in our belief in the power of education to change lives and communities. It is our steadfast purpose to challenge and defy the barriers that constrain the educational progress of any child. We set high aims for aspiration and secure collective responsibility for all our children's achievements. Our work is underpinned by the values of Integrity, Respect, Courage, Optimism, Excellence and Accountability.

1 Scope of the Policy

This policy applies to all members of the Brook Learning Trust community (including trustees, academy councillors, staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of Trust information systems, both internally and externally. It should be read in conjunction with the Trust information systems: acceptable use policy.

Trust staff will inform parents/carers of any incidents of inappropriate e-safety behaviour that are discovered, whether these take place on or off Trust premises and during or out of school hours.

Trust personnel will monitor the impact of this policy and the associated Information Systems: Acceptable Use Policy by means of:

- Logs of reported incidents
- Logs of internet and network activity (including websites visited)
- Information from students, parents/carers and staff

2 Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of Trust staff and students.

2.1 Trustees / Academy Councillors

- Trustees are responsible for ratifying this and the information systems acceptable use policy
- Academy Councillors are responsible for ratifying the relevant academy safeguarding policy
- One or more Councillors have responsibility for monitoring safeguarding in the relevant academy and will make a minimum of three visits to schools per year to meet with the Designated Safeguarding Lead (DSL).
- Safeguarding Councillors' reports are submitted to the Trust Audit & Risk Committee which meets three times a year and reports any concerns to the Board.

2.2 Principal and Members of the Senior Leadership Team (SLT)

- The Principal has a duty of care for ensuring the safety (including e-safety) of all members of the academy community, though the day to day responsibility for e-safety will be delegated
- The Principal and/or SLT will ask the HR Manager to invoke the Staff Disciplinary Procedure in the event of a serious e-safety allegation being made against a member of staff
- The Principal will ensure that academy staff receive appropriate training in e-safety and related matters
- The Principal will ensure that staff with responsibility for e-safety are supported to undertake their roles; their performance will be monitored

- The Principal will ensure that e-safety is intrinsic to all areas of the curriculum and academy activities

2.3 Academy Staff tasked with monitoring e-Safety

- Will take responsibility for all aspects of e-safety
- Will review and ensure compliance with academy e-safety related policies and procedures
- Will ensure that all staff are adequately trained
- Will liaise as necessary with the Network Manager and ICT support staff
- Will ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety breach
- Will receive and log reports of e-safety incidents
- Will report regularly to the Principal and to safeguarding Councillors

2.4 Network Manager/ICT Support Staff

- Will undertake regular monitoring of the information systems: both hardware and software
- Will ensure that Trust information systems comply with statutory e-safety technical requirements and adopt best practice
- Will ensure that the Trust technological and electronic infrastructures are secure and not open to misuse or malicious attack
- Will ensure that users of Trust information systems may only access the networks and devices by way of protected and regularly changed passwords
- Will monitor the application, and oversee updates, of the Internet filtering policy (more than one person will be involved with this)
- Will ensure that their CPD is kept up to date

2.5 Teaching and Support Staff

- Are expected to be aware of e-safety related Trust and academy policies
- Must read, understand and sign the Acceptable Use Policy Agreement before they are granted access to the information systems
- Will report any suspected misuse of the information systems to the Principal
- Will conduct all digital communications with students/parents/carers and others in a professional manner
- Will only communicate with parents/carers and students via Trust information systems
- Must ensure that students understand and abide by the terms of this and the information systems: acceptable use policy
- Will instruct students in research skills, the avoidance of plagiarism and an awareness of copyright
- Will oversee the use of all digital devices and systems on Trust premises and ensure compliance with all relevant policies

2.6 Designated Safeguarding Leads (DSLs)

- Will be trained in their roles to protect students and staff from breaches of e-safety
- Will ensure that staff and students:
  - Refrain from sharing personal data and/or digital images
  - Are denied access to inappropriate websites and digital material from Trust information systems
  - Understand the danger of establishing online contact with strangers via social networking or similar platform

- Are aware of the dangers of grooming
- Feel able to report incidents of cyber-bullying and/or breaches of e-safety

2.7 Students

- Must understand the terms of this policy and the information systems: acceptable use policy (including use of personal mobile phones and tablets)
- Will be instructed in research skills, the need to avoid plagiarism and the importance of complying with copyright regulations
- Will know the procedures for reporting incidents of abuse, misuse of the information system or access to inappropriate material
- Will be instructed in the importance of adopting good e-safety practices in and out of school

2.8 Parents / Carers

Parents/carers play a crucial role in ensuring that their children understand the need to access online material and information with care and in an appropriate way. Each academy will assist parents to understand e-safety related issues and parents will sign the Information Systems Acceptable Use policy before their child is granted access to the Trust system.

2.9 Guests

Guests will be asked to sign the information systems: acceptable use policy before being granted access to a Trust information system.

3 Education/Training – students / pupils

Staff will reinforce the importance of e-safety which will be addressed across all areas of the curriculum and discussed in assemblies and tutorial activities. Students will be taught to apply critical judgement in respect of materials they have accessed online. They will be taught referencing conventions and will learn to be aware of copyright regulations.

4 Education/Training – parents/carers

The academies will engage with parents to ensure that all concerned have the fullest understanding of e-safety and an awareness of ways to ensure their children are safe online. Academies may provide information and awareness to parents by way of:

- Curriculum activities
- Letters, newsletters, website publications, materials on the VLE
- Parents/carers evenings/sessions
- Dedicated events/campaigns

5 Education/Training – Staff/Volunteers and Trustees/Councillors

All staff and Councillors will receive regular e-safety training to ensure their full grasp of their responsibilities, as outlined in this policy and related safeguarding-related policies.

6 Trust Information Systems

The Trust is responsible for ensuring that its information systems are as safe and secure as is reasonably possible: this requirement will apply to hardware and software. Hardware will be kept securely. Use of the systems will be in accordance with policies and procedures written to ensure responsible and safe use. Software will be covered by licences which will be administered and logged by the Network Managers.

7 Internet Access

See the BLT information systems: acceptable use policy

8 Email

See the BLT information systems: acceptable use policy

9 Bring Your Own Device (BYOD)

See the BLT information systems: acceptable use policy

10 Personal Mobile Phones and Tablets

See the BLT information systems: acceptable use policy

11 Use of digital and video images

See the BLT information systems: acceptable use policy

12 Data Protection

See BLT data protection related policies

13 Social Media - Protecting Personal and Professional Identities

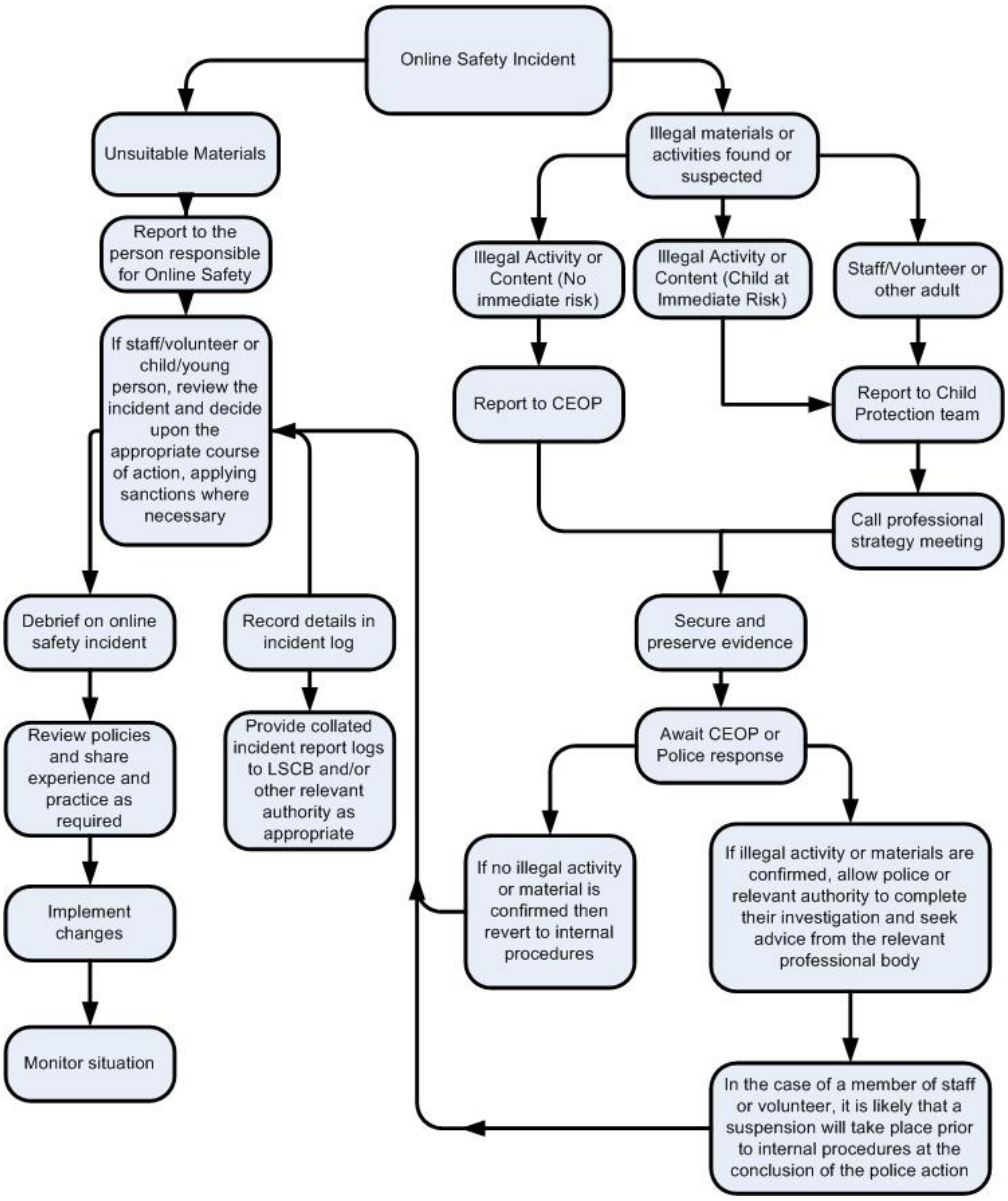
The Trust has a duty of care to provide a safe learning environment for academy pupils and a safe teaching and administrative platform for its staff. Reasonable steps to prevent harm to students and staff arising from the use of social media have been taken, to include:

- Policies written and implemented to safeguard students and staff
- Delivery of education in all matters relating to safe use of the Internet and social media platforms
- Staff instructed to refrain from:
  - Making references on social media to students, parents or other staff
  - Engaging in online discussions of personal matters relating to members of the academy community
  - Presenting personal opinions as Trust policy

Informative Table of the Status of User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Use of criminally racist material to stir up religious hatred (or hatred on the grounds of sexual orientation) contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using Trust information systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Trust					X	
Infringing copyright						X
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files						X
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)					X	
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping / commerce				X	X	
File sharing				X		
Use of social media				X		
Use of messaging apps					X	
Use of video broadcasting e.g. YouTube			X	X		

14 Guidance for dealing with Illegal Incidents

If there is any suspicion that website/s containing child abuse images have been accessed, or if there is any other suspected illegal activity, refer to the right hand side of this flowchart for responding to online safety incidents and report immediately to the police.



15 Guidance for dealing with Other Incidents

All Trust staff and academy students are expected to be responsible users of digital technologies who understand and follow Trust policy. However, should policy infringements be suspected, the following procedure has been written as a guideline:

In the event of suspicion of policy infringement, all steps in this procedure should be followed and recorded for future reference:

- More than one senior member of staff will be involved in this process
- Investigations should be conducted via a designated computer which should be used for the duration of the procedure.
- The e-safety of staff and students should be protected from the adverse results of a security breach
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for the investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Following initial investigation, staff members involved will need to judge whether or not the potential infringement has substance. If it does then appropriate action will follow and could include the following:
  - An internal response or the invoking of formal disciplinary procedures
  - Involvement of an external agency, as appropriate
  - Police involvement and/or action
    - **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. The computer must be isolated but its state not otherwise altered**
    - **Other instances to report to the Police would include:**
    - **Incidents of 'grooming' behaviour**
    - **The sending of obscene materials to a child**
    - **The accessing of adult material which breaches the Obscene Publications Act**
    - **Criminally racist material**
    - **Other criminal conduct, activity or materials**

Students / Pupils

Template for the Investigation of real and/or alleged Policy Breaches

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Designated Safeguarding Lead (DSL)	Refer to Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / Internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)									
Unauthorised use of non-educational sites during lessons									
Unauthorised use of mobile phone / digital camera / other mobile device									
Unauthorised use of social media / messaging apps / personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school / academy network by sharing username and passwords									
Attempting to access or accessing the school / academy network, using another student's / pupil's account									
Attempting to access or accessing the school / academy network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's / academy's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									

Template for the Investigation of real and/or alleged Policy Breaches

Staff	**Actions/Sanctions**							
Incidents	Refer to Line Manager	Refer to Principal	Refer to HR Manager	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)								
Inappropriate personal use of the internet / social media / personal email								
Unauthorised downloading or uploading of files								
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account								
Careless use of personal data e.g. holding or transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature								
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy								
Using proxy sites or other means to subvert the school's / academy's filtering system								
Accidentally accessing offensive or pornographic material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material								
Breaching copyright or licensing regulations								
Continued infringements of the above, following previous warnings or sanctions								

POLICY REVIEW AND RATIFICATION

Policy reviewed bi-annually and ratified by BLT Audit & Risk Committee in July

This review by the Trust Executive In consultation with Network Managers	May 2017
Summary of amendments to this iteration:	Considerable re-wording of all sections of this document to ensure that all related matters are covered comprehensively in this policy and the BLT information systems: acceptable use policy. The two documents should be read in conjunction.
Ratified by Audit & Risk Committee	May 2017
Next review	December 2018