Title	Online Safety
Associated Policies	• Safeguarding and Child Protection (TPO/HS/05) • Professional and Safe Conduct (TPO/STA/10) • Whistleblowing (TPO/STA/19) • Social Media (TPO/STA/20) • Anti-Bullying (TPO/STU/01) • Student Care and Welfare (TPO/STU/06) • Data Protection (TPO/STA/25)

REVIEWED: AUGUST 2017 NEXT REVIEW: AUGUST 2020

1. Policy Statement

1.1 The Brooke Weston Trust is committed to promote the welfare and safety of our students when using digital technologies. The Brooke Weston Trust recognises the importance of the contribution it can make to protecting and supporting students across its Academies in their use of these technologies.

1.2 This policy is designed to incorporate all aspects of child protection and safeguarding that may be affected by digital technology as well as Brooke Weston Trust's use of technology with its Academies.

1.3 The Trust will refer to the most recent government, DfE and ICO guidance and documentation with regard to Data Protection, data storage and privacy compliance.

2. How should this policy be applied?

2.1 This policy applies to all members of the Trust (all staff, students, governors, parents/carers and volunteers).

2.2 This policy applies to any individual who is given access to BWT's digitally connected systems (including email addresses and any other data source or system that is hosted/operated/controlled remotely or other by the Trust).

2.3 BWT expects all academies will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding the use of technology and the Internet both on and off the school site. This will include imposing rewards and sanctions for behaviour – as defined as regulation or student behaviour under the Education and Inspections Act 2006. The 'In Loco Parentis' duty allows the academy to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils.

2.4 The Online Safety policy covers the use of:

- School based IT systems
- School based intranet and networking
- School related external Internet, including but not exclusively, extranet, e-learning platforms, blogs, social media websites
- External access to internal school networking, such as webmail, network access, file-serving (document folders) and printing
- School IT equipment off-site, for example staff laptops, digital cameras, mobile phones, tablets
- Student and staff personal IT equipment when used in school and which makes use of school networking, file-serving or Internet facilities.
- Tablets, mobile phones, devices and laptops when used on the school site.

3. Who is responsible for carrying out this policy?

3.1 Principals should ensure that all academy staff and governors are aware of the Online Safety policy and procedure and of their responsibilities under it. It is the responsibility of the Principal to ensure that breaches of the policy are investigated and addressed.

3.2 Staff and governors are expected to adhere to the policy and procedure and ensure that they conduct themselves in a manner that will not place students or vulnerable adults at risk, bring the school into disrepute or damage their own professional reputation.

4. What are the principles behind this policy?

4.1 The definition of an online incident is:
"Any incident that occurs and involves any person (student or adult) where the use of technology (equipment and/or networks) enables or facilitates inappropriate behaviour and harm and/or distress is caused to another person or the reputation of the Academy and/or BWT. This may include the use of social media, forums, blogs, open and closed groups, digital images, messages or any other means".

4.2 The most likely areas of risk to students are:

- Exposure to illegal inappropriate or harmful material
- Subject to harmful online interactions with other users
- The individuals personal online risky behaviour that then leads to harm

4.3 The Trust has a responsibility for ensuring that the resources are available to promote the safe use of technology and to promote understanding and awareness of the risks attached to the use of digital technology.

4.4 The Trust seeks to promote the use of technology and connectivity to ensure that the students are equipped with the necessary skills and knowledge to perform to the best of their ability both during their time in their Academy and also in their future in their chosen careers and workplaces.

4.5 Staff and students must be able to use digital technology appropriately and safely and understand the risks related to their activity. Students will receive online safety education as soon as they start using digital technology and will be continually reinforced and monitored as students progress through their school life.

4.6 The Trust actively encourages a proactive approach to new and emerging technologies and threats to mitigate the risk of harm to students and staff and the trust and associated academies and their reputations. The Trust seeks to promote a cyber awareness culture that ensures all staff, students and governors take part in and continue to develop their knowledge and understanding of online behaviours and in particular, how to prevent harm through continual learning resources, research and encouragement from all teachers.

5. Who is responsible for online safety and what are their responsibilities?

5.1 School management and online safety

5.1.1 School senior management are responsible for determining, evaluating and reviewing online safety to encompass teaching and learning, use of school IT equipment and facilities by students, staff and visitors, and agreed criteria for acceptable use by students, school staff and governors of Internet capable equipment for school related purposes or in situations which will impact on the reputation of the school, and/or on school premises.

5.1.2 Regular assessment of the strengths and weaknesses of practice within the school will help determine inset provision for staff and governors and guidance provided to parents, students and local partnerships.

5.2 Online Safety Co-ordinator

5.2.1 The school has a designated online safety officer (see individual academy website for contact details) who reports to the SLT and co-ordinates online safety provision across the academy and wider school community.

5.2.2 The school online safety co-ordinator is responsible for online safety issues on a day to day basis and also liaises with relevant stakeholders including IT support, the Trust Education Welfare Officer and other Trust contacts, to ensure the safety of students.

5.2.3 The online safety co-ordinator maintains a log of submitted online safety reports and incidents.

5.2.4 The online safety co-ordinator audits and assesses inset requirements for staff, support staff and governor online safety training, and ensures that all staff are aware of their responsibilities and the academy's online safety procedures. The co-ordinator is also the first port of call for staff requiring advice on online safety matters.

5.2.5 The online safety co-ordinator is responsible for promoting best practice in online safety within the wider school community, including providing and being a source of information for parents and partner stakeholders. This may include facilitating regular assemblies and other such activities that focus on positive messages and behaviours.

5.2.6 The online safety co-ordinator will be involved in any risk assessment of new technologies, services or software to analyse any potential risks.

5.3 Governors

5.3.1 The Safeguarding Governor and the online safety co-ordinator will liaise directly with one another with regard to report on online effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and wider school community.

5.3.2 To provide and evidence a link between the school, governors and parents.

5.3.3 To ensure that they have demonstrable experience, skills and training to be able to provide appropriate challenge and support to the school management team.

5.4 IT support staff

5.4.1 Internal IT support staff are responsible for maintaining the academy's networking, IT infrastructure and hardware. IT staff will be aware of current thinking and trends in IT security and ensure that the school system, particularly file-sharing and access to the Internet is secure. IT staff will ensure systems are not open to abuse or unauthorised external access.

5.4.2 IT support staff are responsible for:

- Defending the network and infrastructure of the academy, reviewing activity logs regularly
- Ensuring that users comply with basic access policies and that only trusted devices can connect to the academy network
- Filtering of search facilities is robust and regularly checked for penetration to ensure that the risk of students accessing material that is unsuitable is minimised.
- To keep up to date with current threats and attack trends and take steps to mitigate this and communicate with the management team and Online Safety Co-ordinator.
- To report to the management team and Online Safety Co-ordinator on any network intrusions or other threats to the network
- To ensure that any IT outsourced e.g. connectivity, maintenance, cloud based services website, email provision, filtering, anti-virus, complies with DfE guidance and Data Protection regulations.
- Promoting basic cyber security practices within the academy e.g. locking computers when away from the desk, using secure passwords, caution when using USB removable drives.

5.4.3 External contractors, website designers/hosts will be made fully aware of and agree to the Trust's Online Safety Policy.

5.5 All staff

5.5.1 Teaching and support staff are responsible for ensuring that they are aware of the current online safety policy, practices and associated procedures for reporting online safety incidents in line with academy procedures.

5.5.2 All staff will be provided with an online safety induction as part of the overall staff induction procedures. All staff will attend mandatory online safety training.

5.5.3 All staff will ensure that they have read, understood and signed the Acceptable Use Policy relevant to Internet and computer use in school (see Appendix 1).

5.5.4 All teaching staff are responsible for rigorously monitor student Internet and computer usage in line with the policy. This includes the use of personal technology, such as cameras, phones on the school site.

5.5.5 Internet usage and suggested websites should be pre-vetted and documented in lesson planning.

5.5.6 To promote and reinforce safe online practices when on and off-site, including providing advice to students on how to report incidents.

5.5.7 To report as soon as is practicable any suspected misuse of Trust/academy digitally connected systems to the Principal or Online Safety Co-ordinator.

5.6 Designated Senior Lead (DSL)

5.6.1 The DSL will be trained in specific online safety issues e.g. CEOP accredited course.

5.6.2 The DSL will be responsible for escalating online safety incidents to the relevant external parties e.g. CEOP, local Police, Local Safeguarding Children's Board, social services and parents/carers. Possible scenarios might include:

- Allegations against members of staff
- Computer crime – hacking of school systems
- Allegations or evidence of 'grooming'
- Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication.

5.6.3 The DSL is responsible for acting 'in loco parentis' and liaising with websites and social media platforms, such as Twitter and Facebook, to remove instances of illegal material or cyber bullying.

5.7 Students

5.7.1 To ensure use of school Internet and computer systems in agreement with the terms specified in the Acceptable Use Policy. Students are expected to sign the policy to indicate agreement.

5.7.2 Students are responsible for ensuring they report online safety incidents in school or with other external reporting facilities, such as CEOP or Childline.

5.7.3 To be aware of and comply with academy policies for Internet and mobile technology usage in the academy, including the use of personal items such as mobile phones.

5.7.4 To be aware that their Internet use out of school on social networking sites is covered under the Acceptable Use Policy if it impacts on the school and/or its staff and students in terms of cyber bullying, reputation or illegal activities.

5.7.5 To follow basic cyber security practices within the academy e.g. locking computers when away from the desk, using secure passwords, caution with use of USB removable drives.

5.8 Parents/carers

5.8.1 To support the academy in its promotion of good Internet behaviour and responsible use of IT equipment and mobile technologies both at school and at home.

5.8.2 To sign the academy's Acceptable Use Policy, indicating agreement regarding their child's user and also their own use with regard to parental access to school systems such as websites, forums, social media, online reporting arrangements and questionnaires.

6. Procedures

6.1 Systems

6.1.1 School computer systems will be configured to ensure the teaching and learning requirements of the school are met whilst ensuring online safety is maintained.

6.1.2 Risk assessments are completed when there is a major overhaul to the system or a new cloud-based software package is purchased, for example.

6.1.3 The system will be compliant with the academy, Trust, local authority, DfE, ICO and Data Protection guidelines with regard to online safety procedures being met.

6.1.4 Regular audits and evaluations of the IT network will be carried out, identifying where improvements can be made.

6.1.5 School IT staff will be responsible for monitoring IT use.

6.2 Filtering

6.2.1 The academy will ensure an accredited filtering system is used. Filtering reports and logs will be examined regularly.

6.2.2 Any filtering incidents are examined and action taken and recorded to prevent a reoccurrence.

The academy will provide enhanced/differentiated user-level filtering. Internet access will be filtered for all users.

6.3 Network security

6.3.1 All users will have clearly defined access rights to academy technical systems and devices.

6.3.2 All users will be provided with a username and secure password by School IT staff. Users are responsible for the security of their username and password.

6.3.3 The Network Manager and Principal/other designated senior person will have access to the main administrator password.

6.3.4 Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

6.4 Use of images and videos

6.4.1 The academy will ensure images and videos of students, staff, students' work and any other personally identifying material are used, stored, archived and published in line with the Data Protection Act, ICO guidance for schools, DfE guidance for schools and the Acceptable Use Policy.

6.4.2 When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images, in particular the risks attached to publishing their own images on the Internet e.g. social media sites.

6.4.3 Written permission from parents or carers will be obtained before photographs of students are published on the school website/social media/local press

6.4.4 In accordance with guidance from the ICO, parents/carers are able to take videos and digital images of their children at academy events for their own personal use, but should not be made publically available where other students are involved in the digital image or video.

6.4.5 Students must not take, use, share, publish or distribute images of others without their permission.

6.5 Data Protection

6.5.1 Personal data will be recorded, processed, transferred and made available according to the Trust Data Protection Policy (TPO/STA/25) and in compliance with the Data Protection Act (1998).

6.6 Social Media

6.6.1 Governors, staff, students and volunteers are expected to comply with the Trust Social Media Policy (TPO/STA/20).

7. Policy Review

7.1 This policy will be monitored as part of the Academy's annual internal review and reviewed on a three year cycle or as required by legislation changes.

7.2 An up to date copy of the policy will be available on the Trust website.

Appendix 1: Acceptable Use Policy

Acceptable Internet Use Statement for Students and Staff

At Brooke Weston Trust, students and teachers work in partnership within a learning community. Mutual respect, responsible attitudes to each other, to work and to property are at the foundation of each Academy's culture of achievement by all.

The computer systems at all BWT academies is the property of that academy and is a resource shared by all students and staff. Computer facilities, including portable units, are made available to students to further their education and to staff to enhance their professional activities, including teaching, research, administration and management. Each Academy's Internet Access Policy has been drawn up to protect all parties - the students, the staff and the Academy. Please contact the Principal for a copy of the Academy's Internet Acceptable Use Policy.

Key Points:
The Academy reserves the right to examine or delete any files, including emails, that may be held on its computer system and to monitor or restrict access to any Internet sites visited.

Students and staff using the Academy's computer system should sign a copy of this Acceptable Internet Use Statement and return it to:

General Office	in respect of Students.
Principal's Office	in respect of Staff (to remain on personnel file)

- All Internet activity should be appropriate to staff professional activity, student's education, or reasonable social use;
- Access to the Internet should only be made via the user's authorised account and password, which should not be made available to any other person;
- Activity that threatens the integrity of the Academy ICT systems, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all email sent and for contacts made that may result in email being received;
- Copyright of materials must be respected;
- Use of personal financial gain, gambling or political purposes is forbidden;
- Use of the network to access inappropriate material is forbidden.

Name	
Tutor Group / Department	

Signed		Student
		Parent
		Staff
Date		

Appendix 2: Online Safety guidance and resources

Online safety and the law	Useful links to external organisations
Computer Misuse Act 1990, sections 1-3 Data Protection Act 1998 Freedom of Information Act 2000 Communications Act 2003, section 1.2 Protection from Harassment Act 1997 Regulation of Investigatory Powers Act 2000 Copyright, Designs and Patents Act 1988 Racial and Religious Hatred Act 2006 Protection of Children Act 1999 Sexual Offences Act 2003 The Education and Inspections Act 2006	Ofsted: www.gov.uk/government/publications/school-inspection-handbook DfE: www.gov.uk/government/groups/uk-council-for-child-Internet-safety-ukccis CEOP: www.ceop.police.uk/safety-centre/ and childnet-int.org/ DfE Keeping Children Safe in Education Links to training E-safety support: www.e-safetysupport.com/online_training CEOP: www.ceop.police.uk/training NAACE: online safety training: www.naace.co.uk/ictcpd4free EPICT online safety training: www.epict.co.uk/#!esafetyinfo/cq8q Presentations www.swgfl.org.uk/Staying-Safe/e-safety-Movies www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware