Policy A3 – E-safety Policy

1. **Introduction**

1.1 Students and Staff have an entitlement to technology to support teaching and learning, including access to the Internet. The e-safety policy for the University of Brighton Academies Trust is designed to help to ensure safe and appropriate access and behaviours.

2. Scope

2.1 This document has been written in order to produce clear guidelines for everyone within the Trust community, including, but not limited to, staff (any-term), volunteers, agency staff, visitors, students and any other users of Information Communication Technology (ICT) at the Trust. Hereinafter referred to as "Users".

2.1 This policy applies to all sites in the Trust however, where applicable, the individual sites may append additional guidelines to this policy based on a specific individual need or requirement. Therefore this would become non-exhaustive policy and we recommend that you check with your establishment directly to obtain the complete policy set applicable to you.

3. Why do we need an e-safety policy?

3.1 The appropriate use of the Internet and other technologies can extend and enhance learning in previously unattainable ways. However, the use of these new technologies can put young people at risk within and outside the academy due to the same strengths that make them attractive tools for learning; their scale and collaborative nature.

3.2 The Internet has the capacity to instantly connect users to content and to each other, but due to its international nature and relative immaturity as a medium, also presents unprecedented levels of risk to young people. Equally, the increasing prevalence of highly functional personal devices gives students access to powerful digital tools wherever they go. Some of the dangers students may face include:

- Access to illegal, harmful or inappropriate content,
- Access to content that promotes extremism and / or radicalisation,
- Losing control over personal information/ images,
- The risk of being groomed by those with whom they make contact, exposing them to physical and sexual risk,
- Exposure to, or engagement in cyber-bullying,
- An over-reliance on unreliable sources of information and an inability to evaluate the quality,
- accuracy and relevance of information on the Internet,
- Plagiarism and copyright infringement exposing students to academic and legal risk,

3.4 This e-safety policy explains how the Trust and each academy are ensuring reasonable safeguards to manage and reduce these risks so that technology can impact positively on learning, teaching and administration.

4. Additional Notes

4.1 Many of these risks touch on areas covered by the Trust Anti-Bullying and Child Protection policies, which need to reference this E-safety policy.

4.2 It may not be possible to eliminate all of the above risks entirely, so it is important that students' understanding of the risks to which they may be exposed is built through good educational provision, so that they have the confidence and skills to face and deal with them.

4.3 The Education and Inspections Act 2006 empowers Headteachers to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but which are linked to by membership of the academy.

5. Monitoring Impact

5.1 Each academy will annually review and monitor the impact of the policy using:

- Logs of reported incidents,
- Internal monitoring of user data,
- Surveys/ questionnaires of users,

6. Staff Responsibilities

6.1 All Trust staff shall make themselves aware of the content of this policy and attend relevant e-safety training.

6.2 All teaching staff shall be responsible for contributing to the positive re-enforcement of e-safe behaviours through their day-to-day interaction with students and technology.

6.3 All teaching staff shall ensure that students' use of personal devices in their lessons (e.g. mobile phones, iPods) is for legitimate educational purposes and not for texting, accessing social networking sites or recording audio, video or still imagery without permission.

7. E-safety Co-ordinator

7.1 Each academy will designate a senior member of staff as the E-safety Co-ordinator. The E-safety Co-ordinator shall;

- Co-ordinate the academy e-safety education programme for students, staff, parents and governors,
- Maintain a record of e-safety incidents and the actions taken,
- Liaise with ICT Services over e-safety issues,
- Liaise with the Child Protection officer and pastoral behaviour managers where necessary,
- Maintain an up-to-date understanding of developments in e-safety,

8. Educational activities

8.1 E-safety education for students

8.1.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the e-safety provision in each academy. Children and young people need the help and support of the academy to recognise and avoid e-safety risks and build their resilience.

8.1.2 E-safety should be referenced in all areas of the curriculum and staff should reinforce e-safety messages whenever ICT is being used:

- A planned e-safety programme will be provided as part of both ICT and PSHCE lessons and will be regularly revisited – this will cover the use of ICT both in and outside school and will include;
- The safe and responsible use of the Internet,
- The safe and responsible use of mobile devices,

- The safe and responsible use of social media,
- The management of digital identity,

8.1.3 Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial activities.

8.1.4 In lessons where the Internet is accessed, it is best practice that students be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

8.1.5 It is accepted that students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request a temporary removal of those sites from the filtered list, for the period of study. Any request to do so should be auditable, time-limited and with clear reasons given.

8.1.6 Whenever the Internet is used for research, students should be taught to be critically aware of the content they access on-line and be guided to validate the accuracy of information. Equally, students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet. This is a critical cross-curricular responsibility.

8.1.7 Students should be helped to understand the need for the Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside the academy,

8.1.8 Rules for use of ICT systems will be posted in all rooms and may be displayed on log-on screens or desktop backgrounds,

8.1.9 Staff should act as good role models in their use of ICT, the Internet and mobile devices

8.2 E-safety education for parents/carers

8.2.1 Parents and carers may have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/ regulation of their children's on-line experiences. Parents can often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the Internet and can be unsure about what they should do about it.

8.2.2 Each academy will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, and other digital communications,
- Parents evenings,
- Family learning courses in e-safety, so that parents and children can together gain a better understanding of these issues,

8.3 E-safety education and training for staff

8.3.1 It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

8.3.2 An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process,

8.3.3 The designated E-safety Co-coordinator should ensure that all new staff receive e-safety training as part of their induction programme, It is important that both new and existing staff fully understand the Trust E-safety and Acceptable Use policies. Specific advice can be sought from the Trust central ICT services department,

8.3.4 The E-safety Co-ordinator will receive regular updates through attendance at Local Authority/ other information/ training sessions and by reviewing guidance documents released by DfE and others,

8.3.5 This E-safety policy and any updates will be presented to and discussed by staff in team meetings,

8.3.6 The E-safety Co-ordinator will provide advice/ guidance/ training to individuals as required,

8.4 E-safety education and training for Trustees and Local Board members

8.4.1 Trustees and Local Board members should take part in e-safety training/ awareness sessions, with particular importance for those who are involved in ICT/ e-safety/ health and safety/ child protection. This may be offered in a number of ways:

8.4.2 Attendance at training provided by the Trust, Local Authorities, National Governors Association or other relevant organisations,

8.4.3 Participation in information sessions for staff or parents

9. The use of images of students

9.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the Internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the Internet. Those images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term, e.g. there are many reported incidents of employers carrying out Internet searches for information about potential and existing employees. Each academy will inform and educate users about these risks and will act to reduce the likelihood of the potential for harm.

9.2 When creating digital images in lessons, all staff re-enforce students' understanding of the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet.

9.3 Staff are allowed to take digital/ video images to support internal educational use only. Such images should only be recorded using school equipment; personal equipment belonging to staff should not be used for such purposes,

9.4 Care should be taken when taking digital/ video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute,

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

9.6 Photographs published on an academy website or elsewhere that include students will be selected carefully by staff, and the appropriate checks and permissions will be sought prior to publishing,

9.7 Students' full names will not be used anywhere on the public website. This is to prevent third parties from identifying that a particular individual attends the academy. Forenames and year can be used, e.g. "Ben, Year 10".

9.8 Appropriate permission from parents or carers will be obtained before photographs of students / pupils are published on an academy website. This is part of the Acceptable Use Policy signed by parents/ carers on admission of their child. A list of those students whose image should not be used on the public website will be maintained between the Child Protection Officer and the member(s) of staff nominated to publish or request information to be published to the website

10. Technical e-safety provisions

10.1 Each academy, in conjunction with the Trust ICT Services, will be responsible for ensuring that their infrastructure/ network is as safe and secure as is reasonably possible and that procedures set out within this policy are implemented:

10.2 There will be regular reviews and audits of the safety and security of ICT systems,

10.3 All users will have clearly defined access rights to the ICT systems of each academy. This will be defined and accountable by the respective ICT lead / co-ordinator/s for the establishment,

10.4 Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security

10.5 The administrator passwords for the ICT system must also be available to the Academy Principal and kept in a secure, physical (e.g. fire safe) or electronic location software with encrypted storage.

10.6 Each academy, in conjunction with the Trust ICT Services, will use a sufficient Internet filtering system to restrict access to certain materials, adhering to current government guidelines and recommendations,

10.7 Each academy will reserve the right to use internal monitoring systems to intercept and record any IT use for safeguarding and security purposes,

10.8 Remote management tools may be used by staff to control workstations and view users' activity,

10.9 Each academy, in conjunction with the Trust ICT Services, will ensure that appropriate security measures are in place to protect infrastructure and end-user devices from accidental damage or malicious intent which might threaten users and / or the security of systems and data

11. Responding to e-safety incidents

11.1 Each academy will ensure that there are effective child protection mechanisms in place for students and staff to report any concerns that may arise. This includes, but is not limited to, at least one named and responsible Child Protection Officer per-site.

11.2 The E-safety Co-ordinator should;

- Liaise with ICT services, senior management and the Child Protection Officer as necessary to investigate the alleged incident and establish evidence of any breach or wrongdoing,
- Work with any students involved to resolve issues and educate users as necessary,
- Inform parents/ carers of the incident and any outcomes,
- Where the alleged incident involves staff misuse, the Principal should be informed,
- Outcomes of investigations will be reported to the Principal and to external services where appropriate (e.g. The Trust Central Services, Social Services, Police Service, the Child Exploitation and Online Protection Service).

12. Digital communications with students

12.1 The Trust recognise the benefits of allowing and facilitating digital communications with students, whether it be e-mail or any other Academy provided or advocated system. However staff must be aware of the professional risks and potential for false or otherwise accusation of misconduct and / or unprofessional conduct. Further clarification can be found in the acceptable usage policy.

13. Breaches of policy

13.1 Any violation of the standards, procedures or guidelines set out in this policy may be treated as a formal Academies disciplinary matter, which could result in dismissal, legal prosecution or both.

14. Legal frameworks

14.1 It is the users' responsibility to ensure they are compliant and work within all UK and E.U. applicable legislation in regards to the safe and legal use of ICT at the Academies, this includes but is not limited to the following:

- The Sexual Offences Act 2003
- The Racial and Religious Hatred Act 2006
- The Computer Misuse Act 1990 (sections 1 – 3).
- The Police and Justice Act 2006

- Communications Act 2003
- Data Protection Act 1998
- Malicious Communications Act 1988
- Copyright, Design and Patents Act 1988
- Public Order Act 1986
- Protection of Children Act 1978
- Obscene Publications Act 1959 and 1964
- Protection from Harassment Act 1997.
- The Regulation of Investigatory Powers Act 2000 (RIP)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

15. Policy status and review

Written by:	ICT Director
Owner:	ICT Director
Status:	Approved
Approval date:	UoBAT – Board of Directors 10/12/15 HAT – Board of Directors 17/12/15 Merger editorial changes 1 September 2017
Review Date:	2019/20