TBAP
Multi-Academy Trust

E-Learning Safe Use Policy

2016-17

CSS Commissioning & School Support

AP ACADEMY OCTAGON

the bridge AP academy

TBAP Teaching School Alliance

courtyard AP ACADEMY

beachcroft AP academy
TOGETHER EVERYONE ACHIEVES MORE

TBAP CAMBRIDGE AP ACADEMY

Latimer AP academy

TBAP Residence Broadfield Park

1619 AP TBAP Academic ACADEMY

TBAP Octavia AP Academy

TBAP Unity Academy

This policy applies to all members of the Trust community (including staff, learners, volunteers, parents/carers, community users, visitors) who have access to and are users of ICT systems, both in and outside of the TBAP academies.

Why is ICT systems access important?

Technology offers unimaginable opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile, and learners are using technology at an even earlier age.

ICT systems access in TBAP academies increases the opportunities for learners to access a wide range of resources in support of the curriculum and learning.

It supports the professional work of staff and enhances the school's management information and business administration practice.

Access to the TBAP network and the internet is necessary for staff and learners. It is an entitlement for all learners as it helps them to develop a responsible and mature approach to accessing information.

What are the benefits to the Academy?

The Learning Platforms Framework Agreement delivered access to a virtual learning space for all schools following a number of studies and government projects that indicated the benefits to be gained through the appropriate use of the ICT systems including the internet in education.

These benefits include:

- Access to world-wide educational resources including museums and art galleries;
- Information and cultural exchanges between learners world-wide;
- News and current events;
- Cultural, social and leisure use in libraries, clubs and at home;
- Discussion with experts in many fields for learners and staff;
- Staff professional development - access to educational materials and good curriculum practice; communication with the advisory and support services, professional associations and colleagues;
- Exchange of curriculum and administration data with the LA, EFA and DfE, using correct security procedures.

How will the Trust ensure Internet use provides effective learning?

- Curriculum planning will identify opportunities to enrich and extend learning activities via access to the internet
- Learners will be given clear objectives for internet use
- Learners will be provided with access to relevant and suitable web resources
- Learners will be informed that checks can be made on files held on the system
- Learners using the internet will be supervised appropriately
- Internet access will be purchased from a supplier that provides a service designed for learners. This will include filtering appropriate to the age of learners
- The school will work with statutory authorities and the Internet Service Provider to ensure systems to protect learners are regularly reviewed and improved

How will learners be taught to assess Internet content?

- ICT teaching incorporates internet content issues, for instance the value and credibility of web materials in relationship to other media
- Learners will be taught to validate information before accepting it as true, and to discriminate between fact and opinion
- Learners will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed
- Learners will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV
- Learners will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable
- Young learners will be encouraged to use the internet to enhance rather than replace existing methods of research
- Learners will develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Learners will be taught to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Learners will be expected to know and understand policies on the use of ipads in lessons. They should also know and understand policies on the taking/use of images and on cyber-bullying.

How will Internet access be authorised?

- Internet access is a necessary part of the statutory curriculum. It is an entitlement for learners based on responsible use
- Parents will be informed that young learners will be provided with monitored internet access
- Learners must apply for internet access individually, by agreeing to the Acceptable Use Policy

How will the risks be assessed?

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for learners. The academies will supervise learners and take all reasonable precautions to limit users access that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal.

- The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risks will be reviewed
- Staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken

The Executive Head Teacher will ensure that the policy is implemented effectively.

How will the Trust ensure Internet access is safe?

- All users will be informed that Internet use will be monitored
- The ICT technical leads will be responsible for checking internet logs on a daily basis and reporting to the Head of School
- Access to the internet logs will be restricted to senior members of staff

- Any failure of the filtering systems will be reported directly to the ICT technical team
- The Trust reserves the right to remove access to any website it considers inappropriate
- The Trust will work in partnership with parents, the statutory authorities, DFE and the Internet Service Provider to ensure systems to protect learners are reviewed and improved where necessary
- The ICT team will ensure that daily checks are made to ensure that the filtering methods selected are effective in practice
- If staff or learners discover unsuitable sites, the URL (address) and content will be reported to the network manager
- Any material that the academy suspects is illegal will be referred to the appropriate authorities
- All staff in the Trust are made aware of e-safety issues and receive up-to-date training
- All users will be provided with a username and secure password
- Users are responsible for the security of their username and password and will be required to change their password every term
- All users are expected to lock their device when they have moved away from their workstation
- All learners will receive training and guidance on the use of personal devices
- All learners receive a planned e-safety curriculum that teaches them how to stay safe, protect themselves from harm and how to take responsibility for their own and others safety.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and learning guide activities
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that learners should 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
- Where learners are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- Reporting routes are clearly understood by the whole Trust, for example online anonymous reporting systems (CEOP Report Abuse button).

Parents/Carers E Learning Support

Parents/Carers play a crucial role in ensuring that their child understands the need to use the internet in an appropriate way. The Trust will take every opportunity to help parents understand these issues through parent workshops, website information and e-safety literature. Parents and Carers will be encouraged to support the Trust in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents sections of the website
- their children's personal devices in the academy

The internet is a communications medium that is freely available to any person wishing to publish a Website with no editorial intervention. While access to appropriate information

should be encouraged, learners will generally need protected access to the internet. The level of protection will be appropriate to the needs of the learner.

How will the security of the school ICT system be maintained?

- The whole system will be reviewed with regard to threats to potential threats from internet access
- No personal data should be sent over the internet unless it is encrypted or otherwise secured
- Virus protection will be installed and updated regularly
- Personal storage devices such as USB memory sticks, MP3 players, digital cameras & floppy discs may not be brought into school without specific permission and a virus check. Any unauthorised items may be confiscated, placed in a secure area and returned to the user at the end of the school day
- Devices that are taken and used away from the school will be subject to regular scrutiny to ensure that malicious applications do not breach network security systems and that no data is inappropriately removed from the site.

How will e-mail be managed?

Learners are expected to use e-mail

- Communications with persons and organisations will be managed to ensure appropriate educational use and that the good name of the Trust is maintained
- Learners may send and receive e-mail as part of planned lessons

How will publishing on the Web be managed?

- The Executive Headteacher will delegate editorial responsibility to a member of staff to ensure that content is accurate and quality of presentation is maintained
- Web sites will comply with the Trust's guidelines for publications
- Learners will be taught to publish for a wide range of audiences which might include governors, parents or young children
- All material must be the author's own work, credit the sources used and state clearly the author's identity or status
- The point of contact on the website will be the school address and telephone number. Home information or individual e-mail identities will not be published
- Photographs published on the Web will not have full names attached and anonymity will be protected where necessary

Social Media

Social media sites such as Facebook and Twitter can be used for learning purposes and sharing of good practice. Staff should not authorise friend or follow requests from learners.

How will incidents be handled?

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the academy 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 outside of the TBAP academies, but is linked to the membership of the Trust.

The management of the acceptable use of the Internet in school is achieved by:

- Protection software installed on the network;
- Acceptable Use Policy adopted by the school;
- Staff handbook containing this policy signed for by the appropriate staff;
- A range of disciplinary procedures for infringements of the policy;

Whenever a learner or staff member infringes the policy, the final decision on the level of sanction will be at the discretion of the Trust's management team.

Learners: Category A infringements

- Accessing non-educational sites during lessons
- Unauthorised use of e-mail
- Use of file sharing sites on school premises
- Transmission of commercial or advertising material

Sanctions:
The ICT leader or relevant subject leader will discuss appropriate use of the internet with the learner and the probable consequences of continued misuse. The learner's attention will be drawn to the *'Rules for Responsible Internet Use'* and the incident will be recorded in SIMS.net in line with the whole school behaviour policy.

Category B infringements

- Continual access to non-educational sites during lessons after being warned
- Unauthorised use of email after being warned
- Unauthorised use of social networking sites/applications, including chat rooms and newsgroups/forums.

Sanctions:
The infringement will be brought to the attention to the designated member of staff who will telephone the learner's parents/ carers informing them of her/ his continued misuse of the internet. The Consequences of continued misuse will be made clear to all concerned. The learner's attention will be drawn to the *'Rules for Responsible Internet Use'* and the incident will be recorded in SIMS.net in line with the whole school Behaviour policy.

Category C infringements

- Accidentally accessing offensive material and not logging off or notifying a member of staff of it
- Any purchasing or ordering of items over the internet

Sanctions:
The infringement will be brought to the attention of the Head of School or designated member of staff who will write to the learner's parents/ carers to inform them of her/ his continued misuse of the internet and to request a meeting at which this behavior may be addressed.

The learner's attention will be drawn to the *'Rules for Responsible Internet Use'* and s/he will be placed on report, in line with the whole school Behaviour Response Code. The learner's use of the internet will be closely monitored for half a term. Future use will depend on an appropriate response to the imposed sanctions.

Category D infringements

- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the Trust or academies name into disrepute
- Deliberately corrupting or destroying others' data, violating privacy of others
- Cyber-bullying in all forms
- Identity theft (hacking profiles) and sharing profiles

Sanctions:

The infringement will be brought to the attention of the Head of School who will write to the learner's parents/ carers to inform them of her/ his continued misuse of the Internet and to request a meeting at which this behaviour may be addressed. **Exclusion will be considered where the Executive Headteacher deems this appropriate**.

The learner's attention will be drawn to the *'Rules for Responsible Internet Use'* and s/he will be placed on report, in line with the whole school Behaviour Response Code.

Future access to the Internet will be at the discretion of the Head of School

Staff

The following activities will be considered a breach of the Trust code of staff conduct and will result in disciplinary action.

- Excessive use of Internet for personal activities not related to professional development
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1998
- Bringing the school name into disrepute
- Befriending learners on personal social media accounts

How will staff and learners be informed?

- Rules for internet access will be posted near computer systems
- The Acceptable Use Statement or Rules for Responsible Internet Use will be printed as posters
- All staff will be provided with the e-learning safe use policy, and its importance will be explained. The policy will be made available to parents on request.

E-Safety will be a key focus in all areas of the curriculum and staff will reinforce e-safety messages across the curriculum through assemblies and learning guide tutor time.

The school has installed computers with Internet access to help our learning. These rules will keep us safe and help us be fair to others.

- I will only access the system with permission from an adult;
- I will not access other people's files;
- I will use the computers for schoolwork and homework;
- I will not bring memory devices (USB's) from outside school unless I have been given permission;
- I will only e-mail people I know, or those approved by my teacher;
- The messages I send will be polite and responsible;
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;
- I will report any unpleasant material or messages sent to me. I understand that this report would be confidential and would help protect other learners and myself;
- I understand that the school may check my computer files and may monitor the internet sites I visit.

Signed: **----------**
(Chair of Board)

Date:

Signed: **----------**
(CEO)

Date: