BELMONT ACADEMY

BELMONT

E-Safety Policy

Policy Author	Nicola Lyon-Lee
Date of policy	November 2019
Review Cycle	Annually
Review Date	November 2020
Signature of Chair of Governors	Janet Saunders

This policy should be read in conjunction with:
Child Protection and Safeguarding Policy
Anti-bullying Policy
Behaviour Management Policy
Code of Conduct

Belmont Academy ICT and E-Safety policy

Teaching and learning.

At Belmont Academy, we believe that the use of the internet is an essential teaching tool and will allow the students a wider curriculum. The students are taught how to use the internet to research information, locate appropriate websites, and to send and receive information. They are shown how to publish information in a secure setting.

Our internet access is designed to support learning but to also protect the students. We use a filtering system that is appropriate to their needs. The students are taught how to access the internet in a safe way and this is re-enforced every year and throughout the year. As is, how to keep your personal details private through internet use or emails.

At Belmont we take a proactive approach to ensuring online safety. We actively seek to raise awareness of the risks involved in social media use and site that might pose a risk to users. This is done through PSHE lessons, assemblies, cyberbullying events and Safer Internet Day. We have established links with the local police to support this.

Managing internet access.

Each year group has an individual username/password; this allows us to monitor their access to websites and any research they may be carrying out. The filtering of the school internet is covered by our Internet Service Provider Atomwide, which manages internet security on behalf of LGFL. The Computing Leader works in conjunction with ATS who provide our technical support, to ensure systems to protect pupils are reviewed and improved. If any staff or pupils come across unsuitable on-line materials, the site is reported to the Computing Leader and ATS technicians, logged and appropriate action taken. All staff work together to ensure that the filtering system is effective but does not limit learning. In addition, the school has installed iTalc software, which allows teachers to monitor, limit, and if necessary block where students browse on the Internet via its web limiting options.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Software must only be used with appropriate licences.

Students work, photos or names will not be published in such a way that they can be identified by people outside of the school or misused in any way. Parental permission is gained before publishing any photos or names. If a photograph is used there must not be the pupil's name and if a name is given the pupil's photograph must not be used. Any items that are published do not have a reference to the student through the file names. Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing

Every care is taken to make sure that students are not able to access any social networking sites at school. If a site is found to be accessible, it is reported to the ICT technician who will rectify the problem.

Each term, students are reminded of how to keep safe online and this will incorporated into the Computing curriculum. This includes the use of social networking site and the importance of keeping their personal details private.

Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for students and most of these are not supposed to be used by pupils of primary school age.

In the event that a child should access a social media website , parents will be informed and the safeguarding policy should be referred to and followed.

Managing technologies

Mobile phones are not allowed to be used during school time. Students are not allowed to bring mobile phones into school unless they are in Year six and travel home unaccompanied. Students are required to hand them in to the school office before school and they are returned to the students before they leave at the end of the day. The phones are switched off and stored in a locked cupboard throughout the day.

Pupils are not permitted to bring in or wear watches that allow them to access messages or take photographs such devices include Apple watches and V-Tech watches.

In the event that a child should be found to have a mobile phone or watch with such access in their possession, the phone should immediately be confiscated and handed to the school office. Parents should then be informed to collect the device.

ICT System Security

The security of our ICT systems is reviewed and the virus protection is updated regularly through our external provider ATS.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Staff to refer to the ‘Procedures for handling confidential information policy.’ New provisions are now in place to follow the GDPR updated regulations which came into force in May 2018. The School have appointed a data protection officer to advise and manage compliance with the regulation. Full details of our data protection officer can be found on our website.

All staff have signed declaration of usage agreements and are receiving training in the new International Data Protection Policy. All data removed from site should be via password protected USB encrypted by ATS.

Staff are aware of their responsibilities to protect personal data. In the event that personal data should be leaked staff, relevant staff members will be subject to disciplinary action.

Policy Decisions

Authorising Internet access

All pupils will have internet safety rules explained to them Appendix A for KS1&2 pupils.

Parents will have the internet safety explained and will be asked to sign to give their permission for pupil use; Appendix B for KS1&2 pupils.

All staff must read a copy of this policy and sign the 'Acceptable use of ICT: staff Agreement form' Appendix C before using any school ICT resource.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

With some pupils access to the Internet is by adult demonstration with directly supervised access to specific, approved on-line materials.

Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources before being allowed to access the internet from the school site.

Assessing risks

At Belmont, we take every precaution to prevent students from accessing inappropriate materials. However, due to the complexity of the internet, it is not possible to guarantee that unsuitable material will never be seen on a school PC.

Handling e-safety complaints

Complaints of Internet misuse are dealt with by a senior member of staff.
Any complaints about staff misuse are referred to the Headteacher.
Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
Pupils and parents will be informed of consequences for pupils misusing the Internet.

Communications Policy

Introducing the e-safety policy to pupils

All pupils will have e-safety guidance presented each time they log on and before they are allowed to proceed. The Computing curriculum includes units of learning on E-safety for each year group, as does the SEAL curriculum. Assemblies and workshops are planned and delivered to reinforce this message throughout the year.

Staff and the e-Safety policy

All staff have access to the School e-Safety Policy and will sign a copy of the acceptable use staff agreement Appendix C as part of their induction. Staff are informed that network and Internet traffic are monitored and traced to the individual user. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Enlisting parents' and carers' support

Parents and carers attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Website. The school asks all new parents to the sign the e-safety policy.

In the event that pupils are accessing irrelevant materials at home such as *Fortnite,* parents will be given advice to raise their awareness of inappropriate games that are trending via the parent mail system.

Cyberbullying

Cyber-bullying is unfortunately another area which is growing rapidly. It is different from more traditional forms of bullying. Some pupils have 24 hour access to the internet or a mobile phone and so it can be hard to escape. The audience for the bullying can be potentially huge and comments and pictures are likely to stay online forever. We use assemblies, PSHCE and our links with the safer neighbourhood team to educate our pupils about the dangers of cyber bullying.

As with all forms of bullying, the School will deal with this in accordance with the Anti-bullying policy, even if the cyber-bullying is happening outside School hours. A referral to the Police and /or Anti-bullying Project will be made as appropriate.

If parents / guardians have any concerns that their child is being cyber-bullied, they should please print off any available evidence and report it to the School as soon as

possible. In this instance the school safeguarding policy should be referred to and the behavior policy code enforced.

Photographic images

Photographic images (which includes photographs from camera, digital cameras or video) can be valuable in a number of ways; to record evidence of pupil's work, to demonstrate a pupil's involvement in the life of the school, to promote the school such as in our prospectus and to show pupil's engagement in activities for displays. We follow Government guidance for the use of photographs by using group photos in preference to individual photos, by either using a pupil's name or their photo but not both and by not keeping photos when a child is no longer in school. We will seek specific permission from parents for use under the following circumstances;

- For photographs to be used in school publications which may also be used on the school website.
- For photographs to be used for external publications (pupils named) including newspaper articles.
- School productions/school journey (DVD&Photos) to be shared with the families of those taking part.

School staff must only use school equipment, not personal e.g. their mobile phones, for taking photographs.

In the event that staff are using personal equipment, they will be subject to disciplinary action.
In the event that parents are using personal devices inappropriately to record images, they will be confronted and requested to remove the stored material immediately.

Should pupils be found to be sharing images online the safeguarding proceedures should be followed and the behaviour code enforced where necessary.

Appendix A: To be explained to KS1& KS2 pupils

Keeping safe: stop, think, before you click!
12 rules for responsible ICT use

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will keep my login and password to approved curriculum linked websites and learning platforms confidential.
- I will not bring files into school without permission.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.

Appendix B: To be signed by all parents

E-Safety Agreement Form: KS1& 2 Parents/ Carers

Parent/Guardian Name: ……………………………………………………

Pupil Name: ……………………………………………………………….

As the parent or legal guardian of the above pupil(s) I grant permission for my daughter or son to have access to use the Internet, e-mail and other ICT facilities at school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access e-mail employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that in school, staff can check my child's computer files and monitor the internet sites they visit, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's safety.

Parent/Guardian Signature: …………………………………………………

Date: ___/___/___

Appendix C: To be signed by all staff

ICT Acceptable Use: Staff Agreement Form

- I will only use the school's E-mail/Internet/Intranet for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to inappropriate materials to the appropriate line manager.
- I will not download any software or resources from the Internet that can compromise the network, or is not adequately licensed.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will not connect a computer or laptop to the network/Internet that does not have up-to-date version of anti-virus software.
- I will not use personal digital cameras or camera phones for transferring images of pupils or colleagues without permission.
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.
- I will not allow unauthorised individuals to access E-mail/Internet/Intranet.
- I understand that all Internet usage will be logged and this information could be made available to my manager on request.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities and that I will notify the school of any 'significant personal use' as defined by HM Revenue & Customs.
- I will only use LA systems in accordance with any Corporate policies.
- I understand that failure to comply with the Usage Policy could lead to disciplinary action.

Outside of school:

- I will not give out my personal details such as home/mobile phone number; home or e-mail address to pupils unless the need to do so is agreed with senior management.
- I will not seek to establish social contact with pupils or parents on social networking sites for the purpose of securing a friendship or to pursue or strengthen a relationship.
- I will not name the school or people within it on a social media site, or bring it into disrepute by my comments.

I have read the Acceptable Usage Rules.

User Signature

I agree to abide by the above Acceptable Usage Rules.

Signature…………………………… Date: ………………………………….

Full Name: …………………………………………………………………….(printed)

Job Title: ……………………………………………………………………………….