BROOKE HILL ACADEMY TRUST

E-SAFETY SAFEGUARDING POLICY

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.
The school has an e-Safety Coordinator. This is the Designated Child Protection Coordinator as the roles overlap. It is not a technical role.

Children and Young People have increasing access to the internet either at home school or via mobile technology.

Although the internet can have many good features for education, making friends, staying in touch etc. there are also dangers associated with it. These would include availability of unsuitable websites, cyber-bullying, identity theft, on-line grooming and the use of inappropriate messaging.

To combat these, our school has an E-safety Safeguarding Policy, an Acceptable use of ICT Policy and Staff and undertake some form of E-safety/education training with the children.

There are training packages available for all ages of children as well as information for parents on the 'ThinkUKnow' website. We use the CEOP website to inform planning for e-safety lessons. The school offers a training session to parents annually.

Teaching and learning

Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction.
- The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Microsoft Teams

It is important that all staff who interact with children via the use of Microsoft Teams should continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Safeguarding and Child Protection Policy
Online teaching should follow the same principles as set out in the school code of conduct.
We will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.
Below are some things to consider when delivering virtual lessons, especially where webcams are involved:

- No 1:1s, groups only
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background.
- **Staff must only use platforms specified by senior managers and approved by our IT network manager / provider to communicate with pupils – We only use Microsoft Teams at Brooke Hill Academy Trust.**
- Staff should record, the length, time, date and attendance of any sessions held.

All sessions are recorded and this data is retained in line with the Trusts data retention policy and as part of the DfE Learning Platform provisioning of MS Teams the **Auditing** facility of Office 365 is **Turned On**.
By default audit logs are kept for a period of **90-Days.**

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.

The Virtual Learning Environment and E-mail

- Pupils may only use approved virtual learning and e-mail accounts on the school system.
- Pupils use of blogging should be monitored by the teacher who set up the blogging account.
- Pupil must be made aware this blogging is monitored and inappropriate material will be reported to the Headteacher/school leader for the relevant action to be taken.
- Pupils must immediately tell a teacher if they receive an offensive message.
- In e-communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- Staff or pupil personal contact information will not be published.
- The Admin and teaching staff will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Pupils' full names will not be used anywhere on a school Web site or other on-line space.
- Written permission from parents or carers will be obtained when each child starts at school before photographs of pupils are published on the school Web

site. We will consider using group photographs rather than full-face photos of individual children.

- Pupil image file names will not refer to the pupil by name.

Social networking and personal publishing

There are many social networking services available; Brooke Hill Academy is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Brooke Hill and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- **Blogging** – used by staff and students in school.
- **Twitter** – used by the school, staff and students as a broadcast service as well as staff contact being made to appropriate third parties to help enhance the children's learning. All comments must be moderated (see below)
- **Facebook** – used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Managing filtering

- The school works with EMpSN and RM filtering system to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials it must be immediately reported to the e-Safety Coordinator. This material **should not** be viewed by **anyone** else.
- The Headteacher will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use

- Video conferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Video conferencing and webcam use will be appropriately supervised for the pupils age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The school leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden. **Use of the school internet is prohibited for use on personal devices.**
- The use by pupils of cameras in mobile phones will be kept under review.

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2013.

Policy Decisions

Authorising Internet access

- All staff must read and sign the Acceptable use policy for ICT before using any school ICT resource.
- Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- As each child starts at school parents will be asked to sign and return a consent form.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor the Governors can accept liability for any material accessed, or any consequences of Internet access.

The school will annually audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be 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 the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

The school will liaise with local organisations to establish a common approach to e-safety.

Communications Policy

Introducing the e-safety policy to pupils

- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- E-Safety training will be embedded within the ICT scheme of work.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff will be informed that network and Internet traffic can be 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.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

- Parent and carers attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

- Parents will be invited to an E-safety session annually.

This policy is reviewed annually.