THE BROOKSBANK SCHOOL
Aspire & Achieve

# E-Safety Policy

| | |
|---|---|
| **Version Number** | 1.0 |
| **Date of Issue** | July 2021 |
| **Date Approved** | July 2021 |
| **Date for Review** | July 2023 |
| **Approved by** | Head & Safeguarding Governor |
| **SLT Member Responsible** | Director of Finance and Resources |

*(To be read in conjunction with the documents listed on Page 4)*

# General

***Schools have a role, to such extent as is reasonable, to regulate the behaviour of students / pupils 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 is linked to membership of the school.***

***The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.***

**Teaching and Support Staff are responsible for ensuring that:**

- They have an up to date awareness of e-safety matters and of the current school e-safety policies and practices
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the E-Safety Co-ordinator for investigation.
- Digital communications with students e.g. e-mail or via Office365/Teams/Sharepoint should be on a professional level *and only carried out using official school systems*
- e-Safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the school e-safety and acceptable use policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned students / pupils 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.
- Videoconferencing will be supervised appropriately for the students' age and ability.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices e.g. requesting an encrypted memory stick from school.

When using e-mail the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. *Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).*
- Users need to be aware that email communications may be monitored.

Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such e-mail.

Any digital communication between staff and students/parents/carers (e.g. e-mail) must be professional in tone and content.

Use of digital and video images (photographic and video)
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 they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

**Students / pupils are responsible for:**

- Using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems.

**Parents / Carers will be responsible for:**

- Endorsing the Student Acceptable Use Policy

**Network Manager and IT Technical Staff responsibilities:**

- That the school's ICT infrastructure/network is secure and is as safe and secure as is reasonably possible and not open to misuse or malicious attack.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- The school's broadband access will include filtering appropriate to the age and maturity of students.
- The school will ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- That users may only access the school's networks through a properly enforced password protection policy:
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password by The ICT Manager who will keep an up to date record of users and their usernames.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

**Training and Support:**

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst students.
- Particular attention to e-Safety education will be given where students are considered to be vulnerable.

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's Behaviour Policy.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Sharepoint and information about national / local e-safety campaigns / literature.

*Our policy applies to all staff, governors and volunteers working in The Brooksbank School Sports College. All action taken to safeguard children will be in accordance with Calderdale Safeguarding Children Board which can be accessed on* www.calderdale-scb.org.uk

*This policy will be reviewed every three years in order to monitor its impact. Revisions of the policy and practice may be amended where necessary, such as after an incident or change in the national legislation.*

**Documents Associated with this Policy**

- E-Safety: Social Networking Policy: Staff
- E-Safety: Using Student Images Policy: Staff
- E-Safety: Acceptable ICT Use: Staff
- E-Safety: Acceptable ICT Use: Students
- E-Safety: Parent's Checklist re Protecting Their Children Online*
- E-Safety: Risks of Accessing Inappropriate Websites*
- E-Safety: Risks of Online Grooming*
- E-Safety: Cyberbullying*
- E-Safety: Facebook Checklist*
- E-Safety: Parent's Guide to Protecting Their Children Online*

* These documents are attached to paper copies of this policy and are available as separate documents on the school website and, for staff, Sharepoint.