





E- SAFETY POLICY

|  |  |
| --- | --- |
| Date of Implementation | September 2019 |
| Review Date | August 2020 |
| Chair Governor | Mr Naheem Khan |

**Aims**

* To educate students in using new technologies appropriately and safely.
* To ensure that the curriculum builds students’ resilience to the risks new technologies may pose.
* To support a curriculum where students are taught to be critically aware of the materials they access on-line.
* To ensure that all staff, students and parents are offered training in how to deal with the risks of new technologies.
* To ensure that all students are given opportunities to develop as responsible users and stay safe when using the internet and other new technologies.

# Principles

* This policy should be read in conjunction with the School Behaviour and Discipline Policy, the Safeguarding & Child Protection Policy and the Anti-Bullying Policy.
* This policy applies to all members of the school who have access to and are users of the school ICT systems, both in and out of school.
* Blackwater Academy will ensure that the network/infrastructure is as safe as is reasonably possible.
* As part of the Prevent agenda school will ensure an effective filtering and monitoring system to prevent radicalisation and access to extremist views.

# Roles and Responsibilities

* Governors are responsible for the approval and review of the E-Safety Policy. The relevant Governors sub-committee will receive regular information about E-Safety incidents and monitoring reports. The designated E-Safety Governor is:

**Mr Naheem Khan**

* The Head Teacher is responsible for ensuring the safety of members of the school community.
* The designated E-Safety Officer is:

**Mr Kyle Morrison**

who is designated by the Head teacher as the Safeguarding Leader, who will have the day to day responsibility for E-Safety.

**Designated E-Safety Officer is responsible for ensuring:**

* that the school’s ICT infrastructure is secure and is not open to misuse or malicious attack;
* that the school meets e-safety technical requirements and any relevant Local Authority regulation.
* E-Safety policy and guidance regarding security is using effective filtering and monitoring service in accordance with the Prevent agenda;
* that users may only access the school’s networks through a properly enforced password protection policy.

They will also:

* Lead on e-safety issues.
* Take day-to-day responsibility for e-safety issues and have the major role in creating and reviewing the school’s e-safety policies/documents.
* Ensure that all staff are aware of the procedures to be followed in the event of an e-safety incident.
* Provide training and advice for staff.
* Liaise with the relevant Local Authority personnel.
* Create a log of e-safety incidents to inform future e-safety policy developments.
* Meet regularly with the e-safety Governor to discuss current issues, review incident logs and filter or change control logs.
* Attend relevant external Training meetings.
* Report regularly to the Senior Leadership on the current e-safety health of the school.

**Teaching and support staff**

The internet is an essential element of 21st century life in education, business and social life. Blackwater recognises that it has a duty to provide students with internet access as part of their learning experience, regardless of their learning abilities and attainment levels. In order for such opportunities to take place teaching and support staff should ensure that:

* they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
* they have read, understood and signed the school Staff Acceptable Use Policy/ Agreement
* they report any suspected misuse or problem to the E-Safety Officer,
* digital communications with students/pupils (email/Virtual Learning Environment (VLE)/ voice) should be on a professional level and only carried out using official school systems;
* they monitor ICT activity in lessons, extra-curricular and extended school activities and are vigilant when pupils access the internet particularly for websites which may contain extremist’s views.
* 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.
* Staff should also ensure that no reference is made on social media to students, parents/carers or school staff
* **Students:**
* 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
* have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
* will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying
* should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s E-Safety Policy covers such actions, if related to their membership of the school. The school has no jurisdiction over private student use of the internet or social media but will assist parents and the police if required to do so.
* be aware of potential extremist/radicalisation threats and know how to report these.

**When working with SEN students it should be remembered that:**

* Those with learning disabilities may make literal interpretations of content, which may affect how they respond.
* They may not understand some of the terminology used.
* Those with more complex needs may not always understand the concept of friendship and therefore trust others naively.
* They may not know how to make judgements about what information is safe to share. This can lead to confusion about trusting contacts on the internet.
* Some students may be vulnerable to being bullied or extremism/radicalisation because they don’t even recognise it.
* Some students may not even recognise that their own on-line behaviour may be perceived by others as bullying.

**Parents/Carers:**

Parents/carers play a crucial role in ensuring that their children can use new technologies safely.

At Blackwater Academy we will take every opportunity to help parents understand these issues through parents’ evenings, newsletters, the school website and information about national/ local e-safety campaigns/literature.

Parents and carers will be responsible for:

* endorsing (by signature) the Student Acceptable Use Policy
* accessing the school website on-line student/pupil records in accordance with the relevant school Acceptable Use Policy
* parents are responsible for their use of social media and should understand that school has the right to take action if there are inappropriate or offensive comments or images made online regarding staff.

# Training

Students:

* a planned e-safety programme should be provided as part of the curriculum and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school;
* key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities;
* students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information;
* students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school;
* students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
* staff should act as good role models in their use of ICT, the internet and mobile devices.

**Teaching Staff and Support Staff:**

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

* an audit of the e-safety training needs of all staff will be carried out regularly through questionnaires;
* a planned programme of formal e-safety training will be made available to staff;
* 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.

# Infrastructure

The school will be responsible for ensuring that its infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

* There will be regular reviews and audits of the safety and security of school ICT systems.
* Servers, wireless systems and cabling must be securely located and physical access restricted.
* All users will have clearly defined access rights to school ICT systems.
* All users will be provided with a username password by the ICT coordinator which will be used when accessing the system within the school.
* There is a suitable filter to ensure that children are safe from terrorist and extremist materials when accessing the internet.

# Curriculum

**E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum:**

The school internet access is designed expressly for student use and includes filtering using software appropriate to the needs of Blackwater’s students.

* in lessons where internet use is pre-planned, it is best practice that students 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 students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
* it is accepted that from time to time, for good educational reasons, 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 that the Network Manager can temporarily remove those sites from the filtered list or the period of study. Any request to do so, should be auditable, with clear reasons for the need.
* students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
* students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
* students should not be unsupervised while in an ICT classroom.

# Use of Digital and Video Images

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. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

* 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 and full names should never be used alongside images.
* staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
* 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.
* students must not take, use, share, publish or distribute images of others including staff without their permission.
* photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
* students’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
* written permission from parents or carers will be obtained before photographs of students are published on the school website.

# Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

* fairly and lawfully processed;
* processed for limited purposes;
* adequate, relevant and not excessive;
* accurate;
* kept no longer than is necessary;
* processed in accordance with the data subject’s rights;
* secure;
* only transferred to others with adequate protection.

Staff must ensure that they:

* 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;
* do not allow students to log on as staff.

# Communications including use of Mobile Phones

* students are not allowed to use mobile phones anywhere on school site including break and lunch times.
* students will have their mobile phones confiscated if they are seen out on school site
* the official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school e-mail to communicate with others.
* users need to be aware that email communications will be monitored
* users must immediately report, to the nominated person Miss Brookes in accordance with the school policy, the receipt of any offensive e-mail.
* any digital communication between staff and students/pupils or parents/carers (email, chat, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.

**Other e-safety issues: -**

**E-Mail**

1. Students are not given their own e-mail accounts on the school system, but where appropriate an approved e-mail for their use may be set up for curriculum purposes and this should be closely monitored.
2. In any e-mail communication, students must not reveal their personal details or those of others or arrange to meet anyone.
3. E-mail sent to any external organisation should be written and checked carefully, before being authorised for sending, in the same way as a letter on school headed notepaper.
4. The forwarding of any chain mail correspondence is not permitted.

**The School Website**

1. The contact details on the school website are the school address, the e-mail address, a contact number for the Head teacher and Chair of Governors and approved photos. Other staff or student personal information is not permitted.
2. The e-safety coordinator will be responsible for all website updates and their conformity with regulations.
3. Where student images are used to illustrate the nature of activities offered by Blackwater Academy it will only be with parental/carers permission.
4. No full names will be used in association with any photographs on the website.

**System Security and Management in practice**

1. Blackwater will ensure that systems to protect students are under constant review and improvement when necessary.
2. All machines attached to the network will be covered by anti-virus software which is frequently updated.
3. Firewalls and routers are configured to prevent unauthorised use of software.
4. All servers will be located in a secure location and physical access will be restricted.
5. The Administrator password will be kept secure and a copy sealed in an envelope in the school safe to allow for emergency access to network resources should the need arise.

**Emerging Technologies**

* Any emerging technologies are examined for educational benefit with associated risk assessment before use is allowed at Blackwater Academy.
* Those in authority need to recognise that technologies such as i-phones can bypass school filtering systems and present a new route to undesirable material.
* Sexting- All Blackwater’s students will be informed about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the World Wide Web.
* Pornography- many children will come across this kind of content when searching the internet. It is important to teach what they should do if they come across this kind of material and who to talk to.

# Responding to Incidents of Misuse

If incidents are inappropriate, then they will be dealt with as soon as possible in a proportionate manner through the normal discipline procedures.

If any apparent or actual misuse appears to involve illegal activity i.e.

* child sexual abuse images;
* adult material which potentially breaches the Obscene Publications Act;
* criminally racist material;
* other criminal conduct, activity or materials;
* any material which may lead to radicalisation or expression of extremist views the matter will be reported to the Police/Prevent Team.

Then appropriate action will be taken following the strategies outlined in the school’s behaviour policy.

**Taken from: Keeping Children Safe in Education May 2016**

**Appendix A: Online Safety**

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation – technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

* Content: being exposed to illegal, inappropriate or harmful material.
* Contact: being subjected to harmful online interaction with other users.
* Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

# Filters and Monitoring

Governing bodies and proprietors should be doing all that they reasonably can to limit children’s exposure to the above risks from the school or colleges IT system. As part of this process governing bodies and proprietors should ensure their school has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the school’s IT system and the proportionality of costs VS risks.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part by the risk assessment required by the Prevent Duty.

The UK Safer Internet Centre has published guidance as to what “appropriate” might look like:

UK Safer Internet Centre: appropriate filtering and monitoring.

Guidance on e-security is available from the National Education Network – NEN. Buying advice for schools is available here.

Whilst filtering and monitoring are an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school approach to online safety. This will include a clear policy on the use of mobile technology in the school. Many children have unlimited and unrestricted access to the internet via 3G and 4G in particular and the school and college should carefully consider how this is managed on their premises.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place; they should be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

# Staff training

Governors and proprietors should ensure that as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 64) and the requirement to ensure children are taught about safeguarding, including online (paragraph 68), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

# Information and support

There is a wealth of information available to support schools and colleges to keep children safe online. The following is not exhaustive but should provide a useful starting point:

[www.thinkuknow.co.uk](http://www.thinkuknow.co.uk/)  [www.disrespectnobody.co.uk](http://www.disrespectnobody.co.uk/)  [www.saferinternet.org.uk](http://www.saferinternet.org.uk/)  [www.internetmatters.org](http://www.internetmatters.org/)  [www.pshe-association.org.uk](http://www.pshe-association.org.uk/)  [www.educateagainsthate.com](http://www.educateagainsthate.com/) [www.gov.uk/government/publications/the-use-of-social-media-for-onlineradicalisation](http://www.gov.uk/government/publications/the-use-of-social-media-for-onlineradicalisation)

**APPENDIX B**

**Student Acceptable Use Agreement for Blackwater Academy ICT Equipment**

* I will only use the school’s computers for schoolwork and homework
* I will only edit or delete my own files and not look at or change other people’s files without their permission
* I will keep any logins or passwords that are given to me, secret
* I will not bring files into school without permission, or upload inappropriate material to my work space
* I am aware that some websites and social networks have age restrictions and that I must respect them
* I will not attempt to visit internet sites that I know to be banned by the school
* I will only e-mail people that I know or who a responsible adult has approved
* I will not attempt to visit websites that I know to be banned by my school
* The messages that I send, or information that I upload, will always be polite and sensible
* I will not open an attachment or download a file, unless I know and trust the person that 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 friends, unless a trusted adult has given me permission
* I will never arrange to meet someone that I have only previously met on the internet, unless my parent/carer has given me permission and I take a responsible adult with me
* If I see anything that I am unhappy with or I receive a message that I do not Like, I will not respond to it but will show it to a teacher or responsible adult

**Student Signature\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Student Name (Print)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Parent/Carer’s endorsing signature\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Parent/Carer’s Name(Print)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date\_\_\_\_\_\_\_\_\_**