Blackfen School for Girls

Acceptable User Policy for School's ICT Network, School email and Internet Policy

Head Teacher: Mr M Brown
Chair of Governors: Mr S Fitz-Gerald

	Date	Name	Signature
Policy Date	October 2021		
Review Date	October 2022		
Review Period	Annually		
Lead Person	AHT Curriculum & Assessment	Andy McGee	
Prepared by	AHT	Andy McGee	
Verified by	Head Teacher	Matthew Brown	
Approved by	Chair of Governors	Stuart Fitz-Gerald	

Blackfen School for Girls

Rationale
Blackfen School for Girls believes that the appropriate use of ICT & new technologies improves students learning and the teaching across the curriculum to good or outstanding. The policy outlines the practice expected of all users in order to maintain and develop our provision. It sets out the legal aspects and identifies the responsibilities of all users of the resources.

This policy is part of the developing of e-safety at Blackfen and the embedding of the following principles in the practices of all staff, students and stakeholders:

- Keep all personal information private.
- Consider the long-term implications of any content posted on-line
- To eliminate the uploading or posting of inappropriate, offensive or illegal content to their own or other online spaces.
- Read and adhere to any website's terms and conditions of use, including those around age restrictions.

Outcomes
The School provides a safe & reliable working environment which enables all users to benefit from the technology in place.

Legal Procedures
All users must obey the applicable laws relating to the use of IT services, Freedom of Information, Data protection and respect copyright as set out in Appendix 3 Legal procedures.

Use of the School Network, SIMS and Office 365 (in school or out of School via remote logins) all users must:

- Only use their own account and password to access the School's network and facilities, must not use another person's username and/or password to access the school system and must not use computers that have been left logged on by others without switching user.
- Sign up and use the School's two-step authentication process when accessing their School provided Office365 login or their School network login remotely, from outside School (Staff only).
- Read the School bulletin & check their school email daily (Staff only).
- Follow the guidance in Appendix 1 when using the School email systems. Be polite. Never send or encourage others to send abusive messages. Always use appropriate language. Remember that you are a representative of the School, and others can view what you say.
- Always respect the rights and beliefs of others, and remember that humour and satire can often be misinterpreted.
- Not make or distribute any images, sounds, messages or other materials which are obscene, harassing, inflammatory, malicious, fraudulent or libellous and must not discriminate against age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, sex or sexual orientation.
- Never write down or reveal personal information to anyone, especially a home address, a personal telephone, a personal login and/or password to the School Network, website, social networking site etc.
- Contact CTS immediately if you think someone has obtained any of your personal information (Staff can ring Extension 3115 or email askit@blackfen.bexley.sch.uk).
- Never disrupt use of services by others. This includes not interfering with, or delete, the work of other students and teachers or try to 'hack' any system to get around any security measures put in place to protect it & yourself.
- Understand that any activity that threatens, or is damaging to the school ICT systems, or that attacks or corrupts other systems, is forbidden.
- NOT attempt to plug personal laptops or any other personal devices into the network.
- Be aware that the school network, email and Internet use is monitored by Blackfen and CTS staff and if it is found that they are being abused, then the facilities may be withdrawn without notice.
- Should only view and use websites and material that is needed for school work and should not try to bypass the internet filtering system to gain access to any website that would be normally blocked.
- Should not use the school's facilities for personal financial gain, gambling, political purposes or advertising.

- Must not attempt to contact a student or their parent/carer(s) using their own personal mobile phone number, tablet, laptop or similar device using their contact details stored in SIMS (Staff only).
- Must block or delete students or their parent/carers attempting to contact you on own personal mobile phone, tablet, laptop or similar device (Staff only).

Use of Hardware, all users must

- Never attempt to move, disconnect or in any other way, tamper with any IT equipment and never attempt to rectify faults in equipment. All requests & faults should be reported to CTS by emailing askit@blackfen.bexley.sch.uk or ringing Ex 3115.
- Never leave a PC unattended to which they are logged into. Always lock the screen or save your work and log out. The School reserves the right to log out any user and are not responsible for the loss of any unsaved work.
- Log out of a shared computer (e.g. in the Library, Sixth Form Study area) for someone requiring it for study or other legitimate use if they are using for recreational purposes.
- Only use external hard drives for storage or back-up – Always save work into your user area or your School provided OneDrive, where it can be backed up.
- Should not attempt to download or install any software from the Internet onto the School network.

Use of Internet based Social Media (e.g. TikTok, Facebook, Twitter, Snapchat, YouTube, Pinterest, Instagram, WhatsApp etc)
Staff (including governors, volunteers, and contractors):

- Must not follow, have as their friend, contact or similar any parent/carer(s) on social media and must not attempt to contact students or their parent /carer(s) via social media.
- Must block or delete parents and students attempting to befriend or follow them via social media.
- Should not publish anything on social media that they would not want their employer or students to see.
- Must not use social media to discuss or share School matters of a confidential matter or that are in anyway critical of the School.
- Must not put anything on social media that could damage, yours, the School's or anybody connected to the School's reputation (Photographs etc.).
- Must never use their own cameras or phone to record, photograph or film any children in school.
- Finding their image or a video clip from school on the Internet should take the following action: (1) Contact the site directly to have the item removed; (2) Inform the link LT and CTS to report the incident.
- Should not link their school email address to any social networking site.

NB
Staff (including governors, volunteers, and contractors)

- If the AUP use of social media is not followed, as outlined above, an investigation may be carried out and this could lead to disciplinary action. In the case of Governors, it could lead to suspension, as it may damage the reputation of the School's Governing Body.
- Please be aware that access to most social media sites via the School network are blocked. Members of LT, Student Welfare & other designated staff have access to social media websites to check content and investigate incidents of misuse as part of their job description.
- Staff should regularly check their security settings on social media. These security settings are often changed by the providers and so staff should check these regularly. It is recommended that security settings are set to the highest level possible, e.g. 'Friends only' on Facebook, set your Twitter account to private so that private and personal information, photographs etc cannot be seen publicly by those other than your 'friends', followers or similar.
- Are responsible for the content of their own social media account(s). If a member of staff has shared their confidential login and password details of any of their social media accounts with anyone else or any of their accounts has been 'hacked' and/or taken over by someone else they will still be held responsible for the content posted to their account, in respect to this AUP. At the very least, once they regain control of any of their social media account they will be expected to remove any content that does not meet any of the AUP outlined here.

Students

- Must not share or publish anything on social networking sites that identifies themselves as a Blackfen student.
- Must not share or publish anything on social networking sites that they would not want their parent/carer or other responsible adult to see.
- Must not share or publish anything on social media about a Blackfen student, their family or their friends, including their image without gaining their permission first.
- Must never share or publish anything on social media about anyone employed by Blacken School for Girls or provide a contracted service, including their image.
- Must not try to follow, send a friend request, contact or similar any member of staff at Blackfen via social media or using their own personal mobile phone, iPad, tablet, laptop etc.
- Need to be aware that bullying another Blackfen student using the Internet, social networking sites, the School network, Office 365, School e-mail etc is still bullying and will be treated as such by the School. Students can expect to be sanctioned as set out in the School's Behaviour Charter, whether the incidents have been posted in School or out of School.
- Caught viewing or sharing inappropriate material, including that of another student or persons employed by the School, on a computer or on their own mobile device via social media or otherwise, will receive a serious sanction as set out in the School's Behaviour Charter.
- Need to understand that the School has a robust filter for the internet and a system for monitoring computer usage, However, out of School and particularly on mobile phones connected to mobile networks, there is often no supervision, monitoring or filtering.
- Must not link their school email address to any social networking site.
- Are responsible for the content of their own social media account(s). If a student has shared their confidential login and password details of any of their social media accounts with anyone else or any of their accounts has been 'hacked' and/or taken over by someone else they will still be held responsible for the content posted to their account, in respect to this AUP. At the very least, once they regain control of any of their social media account they will be expected to remove any content that does not meet any of the AUP outlined here.

Parent/Carers

- Are to understand that the school has a clear policy on the use of Internet based Social Media (e.g. TikTok, Facebook, Twitter, Snapchat, YouTube, Pinterest, Instagram, WhatsApp etc) and that they and their child should actively support this. The impact of social media use is often felt in schools, and this is why we expect certain behaviours from students when using social media at all times.
- Must not take or obtain images of other students or staff and then share online, photographs, videos etc., without permission.
- Should understand that the school will take any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour in accordance with the School's Behaviour Charter.
- Should understand that their child has agreed in the Acceptable User Policy to not to search for or share any material that could be considered offensive, harmful or illegal. This might include bullying or extremist/hate/discriminatory content.
- Must support the school by promoting safe and responsible use of the internet, online services and digital technology at home and will inform the school if they have any concerns.
- Are responsible for the content of their own social media account(s). If a parent/carer has shared their confidential login and password details of any of their social media accounts with anyone else or any of their accounts has been 'hacked' and/or taken over by someone else they will still be held responsible for the content posted to their account, in respect to this AUP. At the very least, once they regain control of any of their social media account they will be expected to remove any content that does not meet any of the AUP outlined here.

NB - Students and Parent/Carers

- Parent/Carers should not use a student's Office365 email, Teams account or other School provided system to communicate with teachers or any other member of staff. These systems are for your child's use alone to participate in their learning. If a parent/carer wishes to discuss any aspect of their daughter's learning with a member of staff, they should contact by ringing the School or emailing using their own personal email.

- if the AUP is not followed, as outlined above, there will be an investigation carried out and in most cases, this will result in at least a serious sanction, exclusion or the School reporting a student to the Police as set out in the School's Behaviour Charter.
- The School has a robust filter for the internet and a system for monitoring computer usage, However, out of School and particularly on mobile phones connected to the mobile networks, there is often no supervision, monitoring or filtering. It is therefore a student's responsibility to adhere to this guidance or face the consequences of their actions as set out in the School's Behaviour Charter.

Key roles
AHT (Curriculum) & CTS: to liaise with staff to ensure implementation of procedures; to ensure that the AUP Policy is published to staff, students and parents and is reviewed according to schedule.

FLs: to ensure implementation of AUP procedures by their staff and the students whilst in their Faculty lessons.

Tutors & SSOs: to ensure implementation of AUP procedures by the students whilst in Community time and out of lessons.

Staff (including governors, volunteers, and contractors): to be aware of and to follow school AUP policy and to ensure students adhere to this at all times.
Students: to be aware of and follow school AUP policy at all times.

Related documents: the latest Curriculum Policy, Behaviour for Learning Policy, Anti-Bullying Policy, Safeguarding Policy, Code of Conduct, Health & Safety Policy, Behaviour Charter, Mobile Devices Policy.

Appendix 1 - Email

Under the Freedom of Information Act 2000, your Office 365 School email is not private. Therefore, any email sent or received from/to a School account is School property and can be used and disclosed to third parties if appropriate. Please note that writing an email about someone is treated the same as putting it in writing in the eyes of the Law.

Do not send email to people you do not know, unless you have a good reason and always re-read a message before sending.

Staff should consider the impact of when they send an email, particularly after school hours, at weekends or during School holidays.

Staff should only delete emails that they do not need to retain. If an email contains a discussion about a student or a member of staff, it should be retained or archived.

Students should only access their Email in their free time in School unless directed by a teacher to do so in lesson.

If Staff or a student receives an Email which upsets them in some way e.g. it is abusive or harassing, contact your line manager or SSO if a student.

Appendix 2 – Teacher Standards

In the Teacher Standards dated September 2012, under Personal and Professional Conduct 'A teacher is expected to demonstrate consistently high standards of personal and professional conduct.'

If a member of staff found not to be adhering to the AUP Policy as described above, they may find this being taken into consideration as part of their Appraisal process and could result in a member of staff facing disciplinary action.

Appendix 3 – Legal Procedures

All students, staff and stakeholders MUST

- Obey the applicable laws relating to the use of IT services, notably Complying with the Computer Misuse Act 1990 and the Criminal Justice Act 1994 amendment to the Obscene Publications Act under which it is a criminal offence to; create, store, download or transmit obscene material, hack or the deliberately introduce a virus.
- Adhere to the applicable laws relating to public authorities, notably the Freedom of Information Act 2000.
- Respect the copyright of all materials and software that are made available by the school and comply with the requirements of the Data Protection Act (19880. E.g. staff should not be showing a film, a TV programme, play a downloaded song on DVD or CD unless it is for educational purposes.
- not store electronic copies of copyrighted material like films or songs anywhere on the school IT network.
- Make themselves aware of the Prevent Strategy June 2011 and subsequent updates, and its application to the use of School ICT Network, School email and use of the Internet.
- Make themselves aware of the School's latest Safeguarding Policy and its application to the use of the School ICT Network, School email and use of the Internet.

Appendix 4 – Mobile Devices Policy summary

Mobile devices brought into School by students must remain switched off while on school site. This includes break and lunchtimes. Any student seen using a mobile device on school site at any time will have this device confiscated. Devices must not be seen or heard.
Staff should respect this policy by not openly using their mobile device on School site in front of students.

There are exceptions:

- Staff can allow students to use their mobile device as part of their learning in lesson.
- Students with diabetes or other serious health condition can access their device for glucose or other necessary readings.