The Blue Coat School

ICT ACCEPTABLE USE POLICY
(Staff)

Approved by the Governors' Safeguarding, Health and Safety Committee

Signed: _____

(H Andrews – Chair of Safeguarding, Health and Safety Committee)

Date: _____

This Policy for ICT Acceptable Use was devised by the Director of ICT & Digital Innovation and the Estates & Operations Manager in consultation with colleagues in the School.

Date of Next Review: Lent 2027

The Blue Coat School Birmingham Limited

POLICY FOR ICT ACCEPTABLE USE (Staff)

1. INTRODUCTION

1.1
The Blue Coat School believes in the educational value of a networked computer system, cloud systems and the Internet and recognises their potential to support and enrich the curriculum and the learning process of its pupils. Our goal is to provide a computer system, cloud systems and Internet access to promote educational excellence by facilitating resource sharing, innovation, and communication. Use of the computer system, cloud systems and the Internet is a privilege and requires responsible use. The use of the computer system, cloud systems and Internet is subject to acceptance of this acceptable use agreement and the rules, regulations and policies of the school.

1.2
The Internet links computers around the world and provides access to a wide variety of information and resources. The law affecting the Internet is developing and changing regularly. No acceptable use policy could identify each and every inappropriate use of the computer system, cloud systems and/or Internet and so The Blue Coat School will judge whether the use of the computer system, cloud systems and/or Internet is consistent with this acceptable use policy and its decision shall be final. If a user is unsure whether their use of the computer system, cloud systems or Internet is appropriate, the user shall confer with the Director of ICT & Digital Innovation, ICT Co-ordinator (Pre-Prep) or Estates & Operations Manager.

1.3
The implementation of this policy is the responsibility of all members of staff and it applies to all staff in the school including those in the Early Years Foundation Stage (Nursery and Reception).

1.4
The Blue Coat School reserves the right to modify this ICT Acceptable Use Policy at any time and in any manner.

1.5
The Blue Coat School Policy for ICT Acceptable Use is available on the school website.

2. ACCEPTABLE USE

2.1
The computer system, cloud systems and Internet access has been established for an educational purpose. The user understands and agrees to the following:

- The use of the system and Internet must be consistent with and in support of the educational goals and objectives of the school's curriculum and mission statement.
- The use of any material in violation of any law is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trademark or trade secret.
- The purchase or sale of any product or service is prohibited unless it is for school use.
- The listing of any advertisements or political materials is prohibited.
- Illegal activities of any kind are prohibited.

3. BEHAVIOUR

3.1
The user is expected to follow the generally accepted rules of computer use/'Netiquette'. These rules include, but are not limited to, the following:

1. The user must not use the Internet in any way that may bring the school into disrepute.
2. Be polite. Always use the system in an ethical and respectful manner.
3. Use appropriate language.
4. The user shall not reveal their name, home address, personal telephone number or any other personal information unless it is a member of staff making an on-line purchase for school.
5. The user shall not reveal the personal information of any other person.
6. The user shall not disrupt or congest the computer system, cloud systems or Internet in any manner.
7. The user shall not post anonymous messages.

8. The user shall not access, create, or distribute harassing, defaming, discriminatory, abusive, pornographic, fraudulent, obscene, racist, sexist, or threatening material or imagery.
9. The user shall not sign up to any website which has an age limit higher than that of the user.
10. The user shall not attempt to access blocked Internet sites.
11. The user shall only use school approved, licensed software and shall not use other programs or applications or download any information without permission.
12. The user shall not use the account or password of another user or attempt to impersonate any other person.
13. Confidential information shall not be transmitted over the Internet unless it is by a member of staff making an on-line purchase.
14. The user shall report any known or suspected misuse of the computer system, cloud systems and/or Internet.
15. The user shall not make any false complaints against any other user.
16. The user shall not access any Social Media unless access has been approved by the Director of ICT & Digital Innovation or Estates & Operations Manager.
17. The user shall not use the Internet in any way which may tease, bully or threaten any other user or cause offense, upset or discomfort in any way. Any such misuse may result in a user having their network logon suspended.

4. SERVICES

4.1
The school makes no warranties of any kind, whether express or implied, with respect to the use of the computer system, cloud systems and/or Internet. Use of any information obtained through the use of the computer system, cloud systems and/or Internet is at the user's own risk. The Blue Coat School does not accept any responsibility for accuracy of information obtained through the Internet or for any damage a user may suffer as a result of use of the computer system, cloud systems and/or Internet, including but not limited to, loss of data or interruption of service. The Blue Coat School is not responsible for any financial obligations arising from the unauthorized use of the computer system, cloud systems and/or Internet.

5. SECURITY

5.1
Security on any computer system and cloud systems is a high priority. If a user identifies a security problem, the user shall notify the Director of ICT & Digital Innovation or Estates and Operations Manager immediately, without discussing it or showing it to another person. Any user identified as a security risk may have their network account suspended.

6. VANDALISM

6.1
Vandalism includes, but is not limited to, any attempt to harm or destroy the computer system, cloud systems, hardware, software, or data of the school, another user or of any other agency or network that is connected through the Internet. Vandalism will result in a user's network account being suspended and may involve a referral to the appropriate law enforcement agencies.

7. PASSWORDS

7.1
A user of the computer network understands that the password chosen/given is for personal use only and shall not be shared with any other person. The password may be changed by the Estates & Operations Manager or Network Administrator at any time according to the needs of the school. Additionally, password changes are enforced every 90 days. There is also a lockout policy set which will lock out a user after five failed login attempts. This will expire after 30 minutes of inactivity or if manually unlocked by an administrator.

8. MONITORING

8.1
The computer system, cloud systems and all communications and information transmitted by, received by, or stored in the computer system and cloud systems including email, are the property of the school. A user should not expect that their use of the computer system, cloud systems and Internet is private. The school

has the right, at any time, to access, monitor, and disclose any use of the computer system, cloud systems and Internet, including but not limited to back-up files, email messages and the transmission, receipt or storage of information in the computer as it deems necessary. Monitoring will be conducted regularly to ensure system integrity and to ensure that all users are using the computer system, cloud systems and Internet responsibly. Any device which is connected to the school network, managed or unmanaged, is automatically filtered and monitored by the school filter: https://www.securly.com.

9. BRING YOUR OWN DEVICE (BYOD) – USE ONSITE

9.1
With the increased requirement for staff to use personal mobile devices to connect to the School's cloud services such as iSAMS, CPOMS, Google and InVentry Staff using two-step authentication, users should abide by the ICT Acceptable Use Policy while on the school premises and only use devices in accordance with it. This covers all geographical areas of the school. Any device which is connected to the school network, managed or unmanaged, is automatically filtered and monitored by the school filter: https://www.securly.com.

9.2
A user wishing to access the school network from their personal device should make an appointment to see the Estates & Operations Manager or Network Administrator who will facilitate this and advise on usage/restrictions.

9.3
Any device found to be accessing the school network in an unauthorized manner may be disabled remotely.

9.4
The use of removable external storage of any form is prohibited. Any authorized use of these items must be encrypted. School issued devices are also encrypted. If unsure, seek advice immediately from either The Director of ICT and/or Estates & Operations Manager.

9.5
All teaching staff are supplied with a school owned Apple laptop (or a Windows laptop in a few cases) and the majority of teaching staff are supplied with a school owned iPad. This negates the need for as much Bring Your Own Device usage and allows for greater flexibility and security. These devices are all managed remotely by the School's IT systems.

10. TERMINATION

10.1
The Blue Coat School has the right at any time to terminate or suspend any user's access to, and use of, the computer system, cloud systems and/or the Internet.

11. RESPONSIBILITY

11.1
A user understands that the computer system, cloud systems and Internet is to be used only for educational purposes. Any violation of the terms of this acceptable use agreement may result in the suspension or loss of computer system, cloud systems and Internet privileges, disciplinary action or appropriate legal action.

12. RELATED POLICIES, MONITORING AND POLICY REVIEW

12.1
This Policy should be read in conjunction with other related whole school policies including: Online Safety; Anti-Bullying; Behaviour Management and Exclusions, Social Media and Safeguarding and Child Protection.

12.2
This ICT Acceptable Use Policy will be presented to the Governors' Safeguarding, Health and Safety Committee for approval annually in the Lent Term. The minutes of this meeting will be presented to the Governors.

The Blue Coat School Birmingham Limited
ICT Acceptable Use Policy (Staff) statement

The computer system and cloud systems are owned by the school and are made available to staff to enhance their professional activities, including teaching, research, administration and management. The school's ICT Acceptable Use Policy has been drawn up to protect all parties - the pupils, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system, cloud systems or to monitor any Internet sites visited.

Staff requesting Internet access should sign a copy of this ICT Acceptable Use Policy (Staff) statement.

1. All Internet activity should be appropriate to staff professional activity or the pupils' education.

2. Access to the computer network should only be made via a user's authorized account and password, which should not be made known to any other person.

3. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.

4. Users are responsible for all email sent and for contacts made that may result in email being received.

5. Use of the computer systems and cloud systems for personal financial gain, gambling, political purposes or advertising is forbidden.

6. Copyright of materials must be respected.

7. Posting anonymous messages and forwarding chain letters is forbidden.

8. As email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.

9. Use of the network to access inappropriate materials such as pornographic, racist or offensive material is strictly forbidden.

Full name: _____

Signed: _____ Date: _____