Online Safety Policy

Policy title:	Online Safety Policy
Function:	For information and guidance about online safety at The Blue Coat School. This document forms part of the portfolio of policies designed to inform students and parents.
Status:	For Approval
Statutory guidance:	Keeping Children Safe in Education (DfE 2025) Working together to Safeguard Children (DfE 2023) Sexual Violence & sexual harassment between children in schools & colleges (OFSTED 2021) The Education Act (2002) Teaching Online Safety (2023) The Children Act (2004)
Audience:	Students, Parents, Staff, Leaders, Trustees, Local authority, General public
Ownership:	Assistant Headteacher and DSL, Headteacher, Trust Board
First published:	February 2026
Reviewed by:	Trust Board
Next review:	Every year – February 2027

Contents **Page**

1. Statement of Intent 3

2. Legislation and guidance 3

3. Roles and responsibilities 4

4. Educating pupils about online safety 8

5. Educating parents/carers about online safety 9

6. Cyber-bullying 9

7. Acceptable use of the internet in school 12

8. Pupils using mobile devices in school 12

9. Staff using work devices outside school 12

10. How the school will respond to issues of misuse 13

11. Training 13

12. Monitoring arrangements 14

13. Links with other policies 14

Appendix 1: KS3, KS4 and KS5 acceptable use agreement (pupils and parents/carers) 15

Appendix 2: ICT ACCEPTABLE USE POLICY (staff, PGCE students, trustees, volunteers and visitors) 17

Appendix 3: online safety training needs – self-audit for staff 27

1. Statement of Intent

At The Blue Coat School, we aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

1. Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

2. Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

3. Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying

4. Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

This Online Safety Policy should be read alongside the Online Safety Operational Handbook, which contains detailed operational procedures, technical controls, cyber security measures and step-by-step actions that support the implementation of this policy.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance,

Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools

- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Trust Board

The Trust board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Trust Board will make sure all staff undergo online safety training as part of child protection and safeguarding training and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Trust Board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Trust Board will coordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Trust Board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The trustee board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;

- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
- Having effective monitoring strategies in place that meet their safeguarding needs.

The trustee who oversees online safety is Paul Chadwick.

All trustees will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputy designated safeguarding leads are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and trustee board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Staff and School Operations Manager and ICT Co-ordinator to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT Co-ordinator and other staff, as necessary, to address any online safety issues or incidents

- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (Appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or trustee board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- The DSL is responsible for ensuring that the Online Safety Operational Handbook remains up to date and reflects current practice, technical arrangements and cyber-security requirements. The Handbook outlines the operational detail that underpins this policy, including filtering and monitoring processes, cyber-incident reporting, data security expectations and staff procedures.

This list is not intended to be exhaustive.

3.4 The ICT Co-ordinator

The ICT Co-ordinator with the support of APEX is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting the incident immediately to the DSL.
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 2).

4. Educating pupils about online safety

All students will be taught about online safety as part of the curriculum. Students will be taught about online safety as part of the ICT, Computing and in Personal Development.

All schools have to teach:

Relationships and sex education and health education in secondary schools

In KS3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in KS4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be explicitly taught as part of other subjects, where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

The school will raise parents' awareness of internet safety in letters, monthly safeguarding newsletters and all other communications home. Online safety information will also be communicated via our website. This policy will also be shared with parents via the school website. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the relevant year group team or DSL. Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online
- If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their tutor groups and during ICT lessons.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information and newsletters on cyber-bullying to families so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence
- Before a search, the authorised staff member will:
- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or

- Commit an offence

If inappropriate material is found on the device, it is up to the DSL or another authorised member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves
- If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:
- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy
- Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and families may be familiar with generative chatbots such as ChatGPT.

The Blue Coat recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography which is pornographic content created using AI to include someone's likeness.

The Blue Coat will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, trustees and visitors to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day. Mobile phones must be switched off when pupils enter through the school gates. Should a student use their mobile phone throughout the day it will be confiscated and must be collected from reception at the end of the day by a parent/ carer.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected
- access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in Appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT Co-ordinator.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and internet acceptable use policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct.

The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, threatening, harassing and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such
- Content Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMS.

This policy will be reviewed every year by the designated safeguarding lead. At every review, the policy will be shared with the trustee board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

The Online Safety Operational Handbook will be reviewed termly and updated as required following cyber risk assessments, changes to filtering and monitoring systems, or new safeguarding guidance.

13. Links with other policies

This online safety policy is linked to our:

- Online Safety Operational Handbook includes procedures, technical standards, filtering and monitoring details, incident response workflows, cyber-security measures and staff operational responsibilities
- ICT Acceptable Use Policies (Staff, Students, Visitors)
- Information Policy
- Cyber Security Policy
- Child protection and safeguarding policy
- Rewards and Behaviour policy
- Staff disciplinary procedures
- Code of conduct
- Complaints procedure

Appendix 1

ICT
ACCEPTABLE USE POLICY

Student Name:

1 **Sending/Receiving/Downloads**

- I understand and agree my child must not use email for misrepresentation of The Blue Coat School, distribution of chain letters, unsolicited mass communications or distribution of protected data.
- I understand The Blue Coat School does not actively monitor the contents of emails, however does monitor for patterns that may indicate misuse. The school reserves the right to investigate all information stored on provided systems and services, including but not limited to, cloud storage and email.
- I understand and agree that my child will not use the school's computer facilities to produce material which is likely to cause any type of offence to other students, staff or any other person associated with the school or the wider community.
- I understand and agree that my child accessing content that is deemed unsuitable by the school management or trying to access any sites on the Internet that contain pornographic, racist, violent, illegal, immoral, objectionable, offensive, inappropriate is unacceptable.
- I understand and agree that my child will not send or receive material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- I understand and agree that my child will not plagiarize (the bulk copying of other's work).
- I understand and agree that my child must not open an email attachment from an unknown source or perform actions that could leave them and others at risk from Viruses, Trojans and other unsafe programs.
- I understand and agree that my child will not under any circumstances attempt to use or search for proxy bypass sites, or any other tool to attempt to bypass the school filters.
- I understand and agree that my child will not deliberately and knowingly break copyright laws (including but not exclusively the Copyright, Designs and Patents Act 1988) by posting, downloading, or distributing copyright material.

2 **Keeping safe and secure**

- I understand and agree that my child will change their password regularly, keep it a secret and ensure it is suitably complex and cannot be guessed easily- e.g. Alpha Numeric minimum seven characters.
- I understand and agree that my child will immediately inform an ICT technician if they suspect that another person knows their password and agree that my child will not use or attempt to use another person's login session or details.
- I understand and agree that my child will be e-Safe while on-line for their own protection and not reveal any personal information when using the Internet, including names, addresses, images, videos, banking details and telephone numbers of others or themselves using school equipment. I understand that this is sensible advice when using

the internet at home too.

- I understand that my child will not change their office 365 display image without express permission of the ICT Co-Ordinator or a member of SLT
- I understand and agree that my child will not post messages on any internet message board, or similar online service (social networking included) that could bring their or the Blue Coat School's name or reputation in to disrepute or lead to a breach in confidentiality.
- I understand and agree that my child will not be 'friends' with staff on social networking sites.
- I understand and agree that my child is not permitted to share recorded videos/lessons made by teachers within or outside of the Blue Coat School.
- I understand and agree that my child should think carefully about what is acceptable language and appropriate with regards to what they type and post on Microsoft Teams Chat.
- I understand and agree that my child should think carefully about what is acceptable language and appropriate behaviour with regards to what they say and do during Microsoft Teams meetings/lessons.
- I understand and agree that my child must hang up at the end of the Microsoft Teams lesson/meeting once instructed to do so. The teacher must be the last person in the meeting to hang up.

3 Respecting School ICT Equipment

- I understand and agree that my child will not damage computers, computer systems, related accessories or network hardware/software or attempt circumvent any of the school's filtering programs or restriction policies for any reason.
- I understand and agree that if my child discovers damage they will report it to a member of ICT staff.
- I understand and agree that my child should not disconnect/connect, open or relocate any piece school ICT equipment or accessory (mice, keyboards etc.) without express permission from the ICT Network Co-Ordinator. (Laptops excluded).
- I understand and agree that my child will not attempt to use the school Wi-Fi, network points or any other non-approved activity.
- I understand and agree that my child will not use the school's facilities to install any programs/run games or perform other non- school related tasks.
- I understand and agree that the school has e-Safe monitoring software that keeps logs of all potential violations. If my child suspects that someone has been using their details they will report it immediately.

Sixth Form Only:

Sixth Form students have access to the school's BYOD Wifi network and can login using their normal school username and password. Students should only access internet on their own devices in school via the school BYOD network.

I HAVE READ, UNDERSTOOD AND ACCEPT ALL OF THE ABOVE. I UNDERSTAND THESE RULES ARE IN PLACE TO KEEP MY CHILD AND OTHERS SAFE. IF THEY FAIL TO FOLLOW THE ABOVE POLICY, I UNDERSTAND THEY MAY FACE SERIOUS CONSEQUENCES. IN ALL CASES A RECORD WILL BE KEPT OF THE VIOLATIONS

Student Name	
Student Signature	**Date**

Appendix 2

THE BLUE COAT SCHOOL

ICT ACCEPTABLE USE POLICY – STAFF

NAME:

LAPTOP NAME:

LAPTOP SERIAL NUMBER:

I have successfully signed into Microsoft Teams	
I have successfully signed into One Drive	
I have successfully signed into my email account	
I have successfully signed into Bromcom	
I have read and understood the contents of this ICT Acceptable Use Policy	

I have received a protective case	N
I have received a stylus	N

Signed _____ Date:

Please return this signed sheet to IT Team pigeonhole in the staffroom

Page 2 – 4 to be retained by the USER for reference

1. **IT Acceptable Use Policy**

   In order to access the technology available in schools, users are required to register their use. By registering as a user of the school computer facilities you have agreed to adhere to the following Acceptable Use Policy (AUP). Failure to adhere to the provisions of this policy may lead to denial of access to part, or all the facilities, or other measures such as disciplinary action, if deemed appropriate.

2. **Registration**

   IT facilities including e-mail and internet are available to staff providing that they agree to abide by certain protocols designed to maintain the integrity and security of such facilities.

3. **User IDs and Passwords**

   Staff will be assigned a network user ID and password via the IT Team. Staff passwords should be changed periodically. Access to passwords will be strictly controlled.

   Use of a network ID belonging to another member of staff is not permitted under any circumstances. Users must not disclose their network passwords and must take all reasonable precautions to ensure that their password remains confidential.

   Should a user disclose their password to another they will be held responsible for any improper actions committed under that use ID. Users should bear in mind that someone using their User ID and password can impersonate them in e-mail and damage their work and/or their reputation. E-mail addresses will be unique to individuals.

4. **Acceptable Use of Facilities**

   - Teaching and learning
   - Research
   - Educational and personal development
   - Administration and Management of school business
   - Development work associated with the above
   - Some personal use is acceptable, but such use must be within the bounds of what is deemed reasonable.

5. **Unacceptable Use of Facilities**

   - Use of Internet ‘chat’ lines whilst on duty
   - Disclosure of official e-mail addresses for excessive social communication
   - The creation, transmission, viewing or copying (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material. Indiscretions in this

area may be deemed to constitute an act(s) of gross misconduct which could lead to **instant dismissal**.

- The creation or transmission of material which is designed or likely to cause annoyance, inconvenience, or needless anxiety
- The creation or transmission of defamatory material
- The transmission of material such that it infringes the copyright
- The transmission of unsolicited commercial or advertising material
- Deliberate unauthorised access to facilities/services accessible via the network
- Deliberate activities with any of the following characteristics:
    i. Wasting staff effort on networked resources
    ii. Corrupting or destroying other users' data
    iii. Violating the privacy of other users
    iv. Disrupting the work of other users
    v. Using the network in such a way that denies service to other users
    vi. Continuing to use an item of networking after being requested to cease
    vii. Other misuse, such as the introduction of 'viruses.

6. **Other issues you should be aware of**

- Licensing and copyright – The copying of software is illegal; the use of unlicensed software is also illegal.
- Loans – where hardware or software is loaned the outward and inward transaction should be recorded.
- Access – it is an offence to access or to attempt to access systems, data or other facilities software which are not authorised under the user's ID. Any costs incurred by the school from such usage will be reimbursed by the user to the school.
- Executable files – users will not be permitted to store any executable files (*.exe or *.com) on the network without written authority. If such files are found and no such authority exists, the files will be deleted, and disciplinary action taken.
- User network ID's and passwords – these should be kept confidential. In sensitive areas you should always log out of the machine when leaving the desk to avoid the risk of access to your workspace.

7. **E-mail**

The school email facility is for school business related emails only and the school reserves the legal right to access/monitor individual school accounts for school business purposes. Staff are advised to have their own personal accounts for personal email use.

Judgement as to whether material is regarded as offensive may lie with the recipient. A message, depending upon its content, can form the basis of a claim under the Sex or Disability Discrimination Acts or Race Relations Act consequently you should be mindful of the content.

DO

- Send messages that are clear, concise, and easily understood
- E-mail people that you know or people that you have a valid reason to contact
- Use the e-mail system for communication that is beneficial to your work at The Blue Coat School
- Remember that all correspondence can be identified, and the account holder will always be held responsible for actions undertaken under that ID

DO NOT

- Send unsolicited e-mail of a trivial nature
- Disseminate material that may be found to be offensive by the recipient
- Open e-mail messages when origins may be dubious, this may help avoid the importation of viruses

Bromcom

Users must use Bromcom responsibly, ethically, and legally. Acceptable use includes, but is not limited to:

- Accessing and using the MIS for legitimate educational, administrative, or operational purposes.
- Protecting user credentials and access to the MIS.
- Complying with all applicable laws, regulations, and institutional policies.
- Ensuring that all information provided through the MIS is accurate, complete, and up to date.

8. Teams Good Practice

- The expectations' regarding safe and responsible use of Microsoft Teams applies to all members of The Blue Coat School community.
- All members of The Blue Coat School community are expected to engage in Microsoft Teams meetings and Chats in a positive and responsible manner.
- All members of The Blue Coat School community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on Microsoft Teams.
- All members of The Blue Coat School community will be e-Safe while on-line for their own protection and not reveal any personal information when using Microsoft Teams, including names, addresses, images, videos, banking details and telephone numbers of others or themselves.
- All members of The Blue Coat School community will not post messages on Microsoft Teams that could bring their or the Blue Coat School's name or reputation into disrepute or lead to a breach in confidentiality.
- Concerns regarding the online conduct of any member of The Blue Coat School community on Microsoft Teams, will be managed in accordance with existing policies, including anti-bullying, allegations against staff and child protection.

- All students should hang up at the end of the Microsoft Teams lesson/meeting once instructed to do so. The teacher must be the last person in the meeting to hang up.
- All students are required to always have their webcam on during Team meetings.
- All members of The Blue Coat School community should not post, chat, or attend meetings using Teams at inappropriate times during the day. Posts, chats, and meetings should take place during school hours.

9. **Data Protection**

Users are advised to be mindful of legislation concerning the protection of data, particularly regarding the transfer of personal data.

10. **Suspension of Access**

Should users be found to be using the network or other networked resources irresponsibly their access rights may be suspended to prevent further infringements. More serious breaches may be subject to disciplinary action and possible dismissal, pending further investigation.

11. Laptop and Accessories

Staff are responsible for the safekeeping of their laptop and accessories associated with their laptop including charger, stylus, and protective case. If items are lost, damaged or stolen, this should be reported to the IT department immediately using helpdesk@bluecoatschool.org.uk providing a full explanation. If a replacement is needed this will be purchased through the user's departmental budget.

12. **Software**

The laptop you have been provided with has had software testing carried out by the IT Team. However, you will need to follow the instructions attached to sign into your personal One Drive and Microsoft Teams.

Once you have signed into the software listed on the front page, please sign off on the front page of this document upon a successful login and return this document to the IT pigeonhole once you have signed into all software.

THE BLUE COAT SCHOOL

ICT ACCEPTABLE USE POLICY

PGCE STUDENTS

NAME:

LAPTOP NAME:

LAPTOP SERIAL NUMBER:

I have successfully signed into Microsoft Teams	
I have successfully signed into One Drive	
I have successfully signed into my email account	
I have successfully signed into Bromcom	
I have read and understood the contents of this ICT Acceptable Use Policy	

Signed _____ Date: February 2026

Please return this signed sheet to IT Team pigeonhole in the staffroom

Page 2 – 4 to be retained by the USER for reference

13. **IT Acceptable Use Policy**

In order to access the technology available in schools, users are required to register their use. By registering as a user of the school computer facilities you have agreed to adhere to the following Acceptable Use Policy (AUP). Failure to adhere to the provisions of this policy may lead to denial of access to part, or all the facilities, or other measures such as disciplinary action, if deemed appropriate.

14. **Registration**

IT facilities including e-mail and internet are available to staff providing that they agree to abide by certain protocols designed to maintain the integrity and security of such facilities.

15. **User IDs and Passwords**

Staff will be assigned a network user ID and password via the IT Team. Staff passwords should be changed periodically. Access to passwords will be strictly controlled. Use of a network ID belonging to another member of staff is not permitted under any circumstances. Users must not disclose their network passwords and must take all reasonable precautions to ensure that their password remains confidential. Should a user disclose their password to another they will be held responsible for any improper actions committed under that use ID. Users should bear in mind that someone using their User ID and password can impersonate them in e-mail and damage their work and/or their reputation. E-mail addresses will be unique to individuals.

16. **Acceptable Use of Facilities**

- Teaching and learning
- Research
- Educational and personal development
- Administration and Management of school business
- Development work associated with the above
- Some personal use is acceptable but such use must be within the bounds of what is deemed reasonable.

17. **Unacceptable Use of Facilities**

- Use of Internet ‘chat’ lines whilst on duty
- Disclosure of official e-mail addresses for excessive social communication
- The creation, transmission, viewing or copying (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material. Indiscretions in this area may be deemed to constitute an act(s) of gross misconduct which could lead to **instant dismissal**.

- The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety
- The creation or transmission of defamatory material
- The transmission of material such that it infringes the copyright
- The transmission of unsolicited commercial or advertising material
- Deliberate unauthorised access to facilities/services accessible via the network
- Deliberate activities with any of the following characteristics:
    i. Wasting staff effort on networked resources
    ii. Corrupting or destroying other users' data
    iii. Violating the privacy of other users
    iv. Disrupting the work of other users
    v. Using the network in such a way that denies service to other users
    vi. Continuing to use an item of networking after being requested to cease
    vii. Other misuse, such as the introduction of 'viruses.

18. **Other issues you should be aware of**

- Licensing and copyright – The copying of software is illegal; the use of unlicensed software is also illegal.
- Loans – where hardware or software is loaned the outward and inward transaction should be recorded.
- Access – it is an offence to access or to attempt to access systems, data or other facilities software which are not authorised under the user's ID. Any costs incurred by the school from such usage will be reimbursed by the user to the school.
- Executable files – users will not be permitted to store any executable files (*.exe or *.com) on the network without written authority. If such files are found and no such authority exists the files will be deleted and disciplinary action taken.
- User network ID's and passwords – these should be kept confidential. In sensitive areas you should always log out of the machine when leaving the desk to avoid the risk of access to your workspace.

19. **E-mail**

The school email facility is for school business related emails only and the school reserves the legal right to access/monitor individual school accounts for school business purposes. Staff are advised to have their own personal accounts for personal email use.

Judgement as to whether material is regarded as offensive may lie with the recipient. A message, depending upon its content, can form the basis of a claim under the Sex or Disability Discrimination Acts or Race Relations Act consequently you should be mindful of the content.

DO

- Send messages that are clear, concise, and easily understood
- E-mail people that you know or people that you have a valid reason to contact
- Use the e-mail system for communication that is beneficial to your work at The Blue Coat School
- Remember that all correspondence can be identified, and the account holder will always be held responsible for actions undertaken under that ID

DO NOT

- Send unsolicited e-mail of a trivial nature
- Disseminate material that may be found to be offensive by the recipient
- Open e-mail messages when origins may be dubious, this may help avoid the importation of viruses

20. **Bromcom**

Users must use Bromcom responsibly, ethically, and legally. Acceptable use includes, but is not limited to:

- Accessing and using the MIS for legitimate educational, administrative, or operational purposes.
- Protecting user credentials and access to the MIS.
- Complying with all applicable laws, regulations, and institutional policies.
- Ensuring that all information provided through the MIS is accurate, complete, and up to date.

21. Teams Good Practice

- The expectations' regarding safe and responsible use of Microsoft Teams applies to all members of The Blue Coat School community.
- All members of The Blue Coat School community are expected to engage in Microsoft Teams meetings and Chats in a positive and responsible manner.
- All members of The Blue Coat School community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on Microsoft Teams.
- All members of The Blue Coat School community will be e-Safe while on-line for their own protection and not reveal any personal information when using Microsoft Teams, including names, addresses, images, videos, banking details and telephone numbers of others or themselves.
- All members of The Blue Coat School community will not post messages on Microsoft Teams that could bring their or the Blue Coat School's name or reputation into disrepute or lead to a breach in confidentiality.
- Concerns regarding the online conduct of any member of The Blue Coat School community on Microsoft Teams, will be managed in accordance with existing policies, including anti-bullying, allegations against staff and child protection.

- All students should hang up at the end of the Microsoft Teams lesson/meeting once instructed to do so. The teacher must be the last person in the meeting to hang up.
- All students are required to always have their webcam on during Team meetings.
- All members of The Blue Coat School community should not post, chat, or attend meetings using Teams at inappropriate times during the day. Posts, chats, and meetings should take place during school hours.

22. **Data Protection**

Users are advised to be mindful of legislation concerning the protection of data, particularly regarding the transfer of personal data.

23. **Suspension of Access**

Should users be found to be using the network or other networked resources irresponsibly their access rights may be suspended to prevent further infringements. More serious breaches may be subject to disciplinary action and possible dismissal, pending further investigation.

24. Laptop and Accessories

Staff are responsible for the safekeeping of their laptop and accessories associated with their laptop including charger, stylus, and protective case. If items are lost, damaged or stolen, this should be reported to the IT department immediately using helpdesk@bluecoatschool.org.uk providing a full explanation.

The Blue Coat School Liverpool reserves the right to bill the assigned user or their university for any loss or damage to school equipment caused by the user's carelessness or negligence.

25. Software

The laptop you have been provided with has had software testing carried out by the IT Team. However, you will need to follow the instructions attached to sign into your personal One Drive and Microsoft Teams.

Once you have signed into the software listed on the front page, please sign off on the front page of this document upon a successful login and return this document to the IT pigeonhole once you have signed into all software.

Appendix 3

Online safety training needs – self-audit for staff

Name of staff member/volunteer: Date:

Question Yes/No (add comments if necessary)

1. Do you know the name of the person who has lead responsibility for online safety in school?

2. Are you aware of the ways pupils can abuse their peers online?

3. Do you know what you must do if a pupil approaches you with a concern or issue?

4. Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?

5. Are you familiar with the school's acceptable use agreement for pupils and parents/carers?

6. Are you familiar with the filtering and monitoring systems on the school's devices and networks?

7. Do you understand your role and responsibilities in relation to filtering and monitoring?

8. Do you regularly change your password for accessing the school's ICT systems?

9. Are you familiar with the school's approach to tackling cyber-bullying?

10. Are there any areas of online safety in which you would like training/further training?