Brentwood School

Network Acceptable Use Policy: Pupils

Policy Owner:	Head of ITSS		
Relevant to:	Whole School (3-18)		
Relevant Legislation/Guidance:	Independent School Standards Regulations (2014) Meeting Digital and Technology standards in School and Colleges - DfE Independent Schools Bursars Association - Guidance to Schools SWGfl - Guidance for Schools UK Council for Child Internet Safety (UKCCIS) LGfL - Guidance for Schools NSPCC - NSPCC Learning National Cyber Security Centre Brentwood School Artificial Intelligence (AI) Senior School Guidance		
Last reviewed by:	SLT August 2024		
Last approved by and date:	SLT 29th August 2024		
Last Updated:	August 2024		
Next review due:	September 2027		
Current version published:	19th September 2024		
Circulation:	All staff	Governors	Website
Related & supporting documents:	Behaviour Policy	iPad/Macbook Acceptable User Agreement	Safeguarding Policy

NETWORK ACCEPTABLE USE POLICY: PUPILS

Contents:

Scope

This policy applies to all pupils who use school IT Systems as a condition of access.

Network Acceptable Use Policy

Students are responsible for good behaviour and should exemplify the school values when using the school network and associated services, just as they are in a classroom. This policy forms part of the School Rules and any misuse by pupils may lead to disciplinary action following the Behaviour policy.

While no technological solution can be 100 per cent effective in guaranteeing safety when using the internet, devices and related systems, it can help to minimise the risks to pupils. To that end, several controls have been implemented.

Internet Filtering

Brentwood School uses Smoothwall, a recognised accredited filtering system by the UK Internet Safety Centre. All internet traffic that passes across the Smoothwall filter is automatically filtered and secure (HTTPS) traffic can also be inspected once a certificate has been installed. Internet filtering software helps to minimise the possibility of pupils intentionally or otherwise accessing inappropriate materials. All school-issued devices are filtered on and off-site.

The filtering software in place uses category filtering and a real-time page scanning system to analyse inappropriate content. In addition, the School regularly reviews the blocked and unblocked categories on an age-appropriate basis. Access levels and filtering rules across the school vary according to age. These access levels are set in accordance with the guidance given by DfE whilst considering the need for delivering an age-appropriate curriculum. Internet filtering is further supported by URL filtering on the Firewall provided by Palo Alto Networks. If the filtering software is impacting the learning experience it should be reported to the relevant teacher or the Information Technology Support Services Department (ITSS) directly so that it can be investigated. We must maintain a clear balance between our safeguarding obligations and ensuring that this does not impact teaching and learning.

Network Security and Endpoint Protection

Along with a next-generation firewall, the school has implemented a next-generation antivirus software that minimises viruses and attacks on the school network system and school-owned devices. Portable storage devices cannot be connected to school devices to minimise the risk of infection. If a user suspects that a device may be infected or experiences suspicious behaviour then this should be reported to ITSS immediately.

Passwords

The school has implemented complex passwords for all network users and it recommends the 'three random words' method recommended by the National Cyber Security Centre. Passwords help to protect the school's network and computer system and password security is the responsibility of the user. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as personal passwords widely used. Users should not disclose their passwords, nor keep a list of them where they may be accessed, it must be changed immediately if it appears to be compromised. Users should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which they do not have access rights

Use of Property

Any property belonging to the school should be treated with respect and care and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the ITSS Department.

Online behaviour

As a member of the school community, users should always act according to our values of Virtue, Learning and Manners in addition, they should follow these principles in all online activities:

- The school cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Users should ensure that online communications and any content shared online is respectful of others and composed in a way they would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or that may reasonably be assumed likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as their own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.

Using the school's IT systems

Whenever users access the school's IT systems (including by connecting their own device to the network) they should follow these principles:

- Remember that any control measures have been implemented for the safety and security of the user as well as the security of the school network and systems.
- Only access school IT systems using their own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that they do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors the use of the IT systems and that the school can view

content accessed or sent via its systems.
- Do not upload any digital data (including video clips or images) identifying other pupils or staff without the prior consent of those involved.
- Keep themselves and others safe by not revealing their or other people's personal addresses, telephone numbers, bank account details etc.

Monitoring and access

Parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

All school devices are filtered off the school site as well as at school and are subject to the same filtering rules and restrictions.

Breach reporting

The Data Protection Act 2018, requires the school to notify personal data breaches if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must generally report personal data breaches to the Information Commissioner's Office (ICO) without undue delay (ie within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If pupils become aware of a suspected breach they should report it to the ITSS Department so that it can be investigated.

Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of users. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but you must report any such potential breach.

Email Protocol and Email Policy

Communication between staff and pupils should be confined to work-related matters. All users have a responsibility to ensure that these systems are used appropriately and not for purposes that may contravene the School's Anti-Bullying and Child Protection Policies. Communications

should ensure that all involved are treated with courtesy and respect and in line with our school values.

Risks: All electronic communication should be considered as a business tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature electronic communications seems to be less formal than other written communication, the same laws apply. Therefore, users must be aware of the risks of electronic communication:

- Be 'Legal, Decent, Honest and Truthful'
- If you send communications with any libellous, defamatory, offensive, racist or obscene remarks, you and Brentwood School can be held liable.
- If you forward communications with any libellous, defamatory, offensive, racist or obscene remarks, you and Brentwood School can be held liable.
- If you unlawfully forward confidential information (including images), you and Brentwood School can be held liable.
- If you unlawfully forward or copy messages without permission, you and Brentwood School can be held liable for copyright infringement.
- If you send an attachment that contains a virus, you and Brentwood School can be held liable.

By following the guidelines in this policy, the sender of the communication can minimise the risks involved in the use of email systems. If any user disregards the rules set out in this policy, the user will be fully liable. The consequences of what may be considered an illegal act vary by age and full details are given on 'The age of criminal responsibility' section of the NSPCC website.

Requirements: The following rules are required by law and are to be strictly adhered to:

- It is strictly prohibited to send or forward communications containing libellous, defamatory, offensive, racist or obscene remarks. If you receive an e-mail of this nature, pupils must promptly notify their Form Tutor.
- Only forward a message from another sender if intended for work-related matters.
- Do not send unsolicited messages. An unsolicited message is any communication that is sent without prior request or consent.
- Do not forge or attempt to forge messages.
- Do not send messages using another person's account or mobile device.
- Do not disguise or attempt to disguise your identity when sending messages.
- Do not download viruses or software designed to damage computer systems or send (as attachments) or download programs, batch files or scripts.

Be tolerant of others' mistakes as some people are new to electronic communication. If you do receive any communication which breaks one of the rules above or which worries you in any way, show it as soon as possible to a member of staff.

Use of Artificial Intelligence

Guidance on the use of AI is provided in this document, this document is specifically for those students from Year 9 to Upper 6th. However, all users should be aware of the age restrictions in place for using Generative AI models and should pay particular attention to the potential issues with using personal information.

Breaches of this policy

A deliberate breach of this policy by any user will be dealt with as a disciplinary matter using the school's usual Behaviour policy. In addition, a deliberate breach by any person may result in the school restricting that person's access to school IT systems.

If you become aware of a breach of this policy, you should report it to the Head of ITSS.

ANNEX A: Online Home Learning Acceptable Use Policy

Rules to be observed by pupils

- I will only use technology for school purposes as directed by my teachers.
- I will not reveal my passwords to anyone.
- I will be responsible for my behaviour and actions when using technology (Google suite, Tapestry, Zoom and other interactive applications), this includes the resources I access and the language I use.
- I will make sure that all my communication with pupils, teachers or others using technology is responsible and appropriate.
- If online meetings are used e.g. Zoom, I will ensure that my camera is turned off when I join the meeting and only turn it on when requested to do so by my teacher.
- I will not deliberately browse, download, upload or forward material that could reasonably be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of staff.
- If online meetings are used, I will not record or take photos of my classmates or teachers during a face-to-face session.
- I understand that when using Google Classroom/Tapestry and other applications provided by the school my use can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to help keep me safe and that if they are not followed, school sanctions will be applied and my parent/guardian will be contacted.
- I will not hold pupil-pupil Zoom meetings on school devices without a teacher present.

Guidelines for pupils

In the unlikely event that a lesson is taking place online (eg Zoom) or you are joining an in-person lesson online, remember that this is an extension of the classroom and you should conduct yourself as you would in a classroom. This includes:

- Video conferencing from an environment that is quiet, safe and free from distractions (preferably not a bedroom).
- Be on time for your interactive session.
- Be dressed appropriately for learning.
- Remain attentive during sessions.
- Interact patiently and respectfully with your teachers and peers.
- Provide feedback to teachers about your experiences and any relevant suggestions.
- You MUST NOT record each other's online interactions.
- 1:1 interactions with staff may be recorded, the member of staff will advise you before they start recording.
- Make sure you end the session as soon as the teacher indicates to do so.

Annex B: Prep Pupil user Agreement, EYFS & KS1

For Parents:

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents/guardians are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.
- that we would like the help of parents to read through the points below with their child and help them understand these points as best they can for their age.

For Pupils:

- I will be polite and responsible when I communicate with others
- I will ask a teacher or adult if I want to use the computers/tablets
- I will only use activities that a teacher or adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or adult if I see something that upsets me on the screen