Briarwood School ENJOY ENGAGE LEARN

E-Safety Policy

History of policy changes/review

Author: Briarwood School

Date	Page	Details of change
Sept 2014		Created
Sept 2015		Reviewed
Sept 2016		Reviewed
April 2017	1, 2,	Reviewed – Removed CYPS and Replaced with Bristol City Council Trading with Schools
April 2017	1	Reviewed – Removed Sophos Antivirus and Replaced with BitDefender Endpoint Security - AM
Aug 2018		Reviewed and updated with GDPR information
Nov 2021		Reviewed and updated – Georgina Andrews 12/11/21 Combined with the following policies: - Cyber Security - Social Media - Acceptable Use - Electronic Information and Communications Systems - Bring your own device policy - E Safety

CONTENTS

E-SAFETY POLICY

Section 1 – Policy and Practice

Core Principles

The internet and technology is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with access to quality Information and Communication Technology (ICT) as part of their learning experience across the curriculum.

Everyone in the school community has a personal responsibility to work towards keeping themselves and others safe online. This policy applies to staff members and governors, and all users of the School's ICT systems are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an agreement of acceptable use, which can be found in the appendices of this policy.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this policy, please speak to a member of ELT.

The E Safety Policy has combined 6 previous policies entitled:

- Cyber Security Policy
- Social Media Policy
- Acceptable Use Policy
- Electronic Information and Communications Systems Policy
- Bring Your Own Device Policy
- E Safety Policy

Aims

The aims of this policy are to:

1. Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
2. Identify the 4 categories of risk (Content, Contact, Conduct and Commerce)

3. Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
4. Promote the professional, ethical, lawful and productive use of the School's ICT systems and infrastructure.
5. Define and identify unacceptable use of the School's ICT systems, external systems and social networking sites and specify the consequences of non-compliance.
6. Establish systems and controls to protect the School from cyber criminals and associated cyber security risks, as well as to set out an action plan should the School fall victim to cyber-crime
7. Deliver an effective approach to online safety, which teaches and empowers us to protect and educate the whole school community in its use of technology and data security

The 4 key categories of risk

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

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- 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
- 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;
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- ✓ Teaching online safety in schools
- ✓ Preventing and tackling bullying
- ✓ 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.

Roles and Responsibilities:

Below lists the roles and responsibilities of the school community:

Governing Body

E safety is monitored by the Operations Committee and safeguarding by the Wellbeing Committee and safeguarding governor. The governing board has overall responsibility for monitoring this policy and holding the EHT to account for its implementation. The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs through the use of CPOMS. as provided by the designated safeguarding lead (DSL). All Governors will ensure they have read and understood this policy, agree and adhere to the terms on acceptable use of the schools ICT systems and the internet.

Executive Head teacher

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

DSL

The Designated Safeguarding Leads take over arching responsibility for online safety in school, in particular:

- Supporting the EH in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the EH 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 online using CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the school's Positive Behaviour Management Policy
- Updating and delivering staff training on online safety (appendix 2 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 EH and/or governing board

The ICT Coordinator

The ICT Coordinator is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis 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

ICT Technician

The ICT Technician is responsible for:

- 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 daily basis
- Support with day to day issues via the ICT Helpdesk

Staffing Body

All staff, including contractors, 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 1), and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure 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 on Arbor and dealt with appropriately in line with the school's Positive Behaviour Management 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'

Parents and/or Carers

Parents and/or carers are expected to notify a member of staff of any concerns or queries regarding this policy. Please note, Parents 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 International
- ✓ Parent resource sheet – Childnet International
- ✓ Healthy relationships – Disrespect Nobody

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 1).

Bristol City Council

Internet access is monitored by Bristol City Council Trading with Schools IT Helpdesk, using the filtering system in place. They are responsible for blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files. This system filters out many different categories of websites, including web chat (social networks), and other potentially offensive websites. If someone tries to log on to a filtered website, they will be presented with a blue screen and be unable to proceed. Information about their computer and login username are also recorded in a central database. This database can be accessed by ELT and the I.T technician.

Section 3 – Cyber Crime

Cyber Bullying

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 one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and Addressing

To help prevent cyber-bullying, we will endeavour to teach pupils to understand to the best of their ability what it is and what to do if they become aware of it happening to them or others. We will ensure pupils know how to report a concern to a member of staff and that concerns will be taken seriously and they will be supported throughout the process.

The school will discuss cyber-bullying with pupils in the most suitable way, adapting these learning experiences to meet their individual needs. When appropriate, they will discuss why it occurs and the forms it may take.

All staff, governors and volunteers will receive training on cyber-bullying, its impact and ways to support pupils, as part of our mandatory safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that 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's Positive Behaviour Management policy and log the incident on CPOMS. 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 consider the pupils level of understanding, their primary need and whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material
- Retain it as evidence
- Report it to the police

Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Cyber Crime

Cyber-crime is simply a criminal activity carried out using computers or the internet. It takes shape in a variety of different forms, e.g. hacking, phishing, malware, viruses or ransom attacks.

The following are all potential consequences of cyber-crime which could affect an individual and/or individuals:

- Cost
- Confidentiality and data protection;
- Potential for regulatory breach;
- Reputational damage;
- Business interruption; and
- Structural and financial instability.

Given the seriousness of the consequences noted above, it is important for the School to take preventative measures and for staff to follow.

Cyber Security

Cyber security has been identified as a risk for the School and every employee needs to contribute to ensure data security. The School has invested in technical cyber security measures, but we also need our employees to be vigilant and act to protect the School IT systems. The School have put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as controls and guidance for staff.

Virus protection (BitDefender Endpoint Security) is also purchased by the Bristol City Council Trading with Schools ICT Team and is installed by the Schools' ICT Technician who is responsible for ensuring that it is updated regularly. Laptop users also should make sure that this has been installed and contact the ICT Technician if you have a query regarding installation. Users should avoid clicking on links to unknown websites or downloading large files.

Technology Solutions

The School have implemented the following technical measures to protect against cyber-crime:

- ✓ Firewalls;
- ✓ Anti-virus software (which updates daily)
- ✓ Anti-spam software;
- ✓ Auto or real-time updates on our systems and applications;
- ✓ Web filtering;
- ✓ Secure data backup;
- ✓ Encryption;
- ✓ Deleting or disabling unused/unnecessary user accounts;
- ✓ Deleting or disabling unused/unnecessary software;
- ✓ Using strong passwords; and
- ✓ Disabling auto-run features.

Cyber-crime incident management plan

The incident management plan consists of four main stages:

(i) Containment and recovery: To include investigating the breach, utilizing appropriate staff to mitigate damage and where possible, to recover any data lost.

(ii) Assessment of the ongoing risk: To include confirming what happened, what data has been affected and whether the relevant data was protected. The nature and sensitivity of the data should also be confirmed, and any consequences of the breach/attack identified.

(iii) Notification: To consider whether the cyber-attack needs to be reported to regulators (for example, the ICO and National Crime Agency) and/or colleagues/parents as appropriate.

(iv) Evaluation and response: To evaluate future threats to data security and to consider any improvements that can be made.

Where it is apparent that a cyber-security incident involves a personal data breach, the School will invoke our Data Breach and Protection Policy rather than follow out the process above.

Section 4 – Electronic Information and Communication Systems

The School's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service.

This section of the policy outlines the standards that the School requires all users of these systems to observe, the circumstances in which the School will monitor use of these systems and the action the School will take in respect of any breaches of these standards.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the General Data Protection Regulation (GDPR) and all data protection laws and guidance in force.

Staff are referred to the School's Data Protection Policy for further information. The School is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications)

Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of staff are required to comply with the provisions set out in this policy at all times to protect the School's electronic systems from unauthorized access or harm.

The School has the right to monitor all aspects of its systems, including data which is stored under the School's computer systems in compliance with the GDPR.

This section of the policy deals with the use (or misuse) of computer equipment, e-mail, internet connection, telephones, iPads (and other mobile device tablets), IPhones (and all other mobile phones), personal digital assistants (PDAs) and voicemail, but it applies equally to the use of fax machines, copiers, scanners, and the like.

Acceptable Use

Briarwood School provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of staff, governors and pupils, it is important that all staff members and governors follow the guidelines detailed in this section of the policy. All equipment that constitutes the School's ICT systems is the sole property of the School.

All staff will be provided with training at induction and refresher training as appropriate; when there is a change to the law, regulation or policy; where significant new threats are identified and in the event of an incident affecting the School or any third parties with whom we share data.

Equipment Security and passwords

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

All users of the ICT systems at the School must first be registered. Following registration, a network user account will be created, consisting of a username, password and an e-mail address. All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

Passwords are unique to each user and staff are required to select a strong password that is at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol). Passwords must be regularly changed and never re-used. Passwords must not be shared with anyone. Users are provided with their own login passwords which can be used to monitor any action taken when logged on and every user is responsible for the action taken while their username is in use. Staff are encouraged not to save passwords to website's also in case of a breach.

Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct. Staff must make sure the device locks if left inactive for a period of time.

Staff are required to log off or lock their device when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. SLT may do spot checks from time to time to ensure compliance with this requirement. Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Members of staff who have been issued with a laptop, iPad (or other mobile device tablet), must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the machine is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g. ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers.

Users must report any security breach or suspected breach of their network, email or application account credentials to ELT. Users must also report any mistakes as soon as possible. If your concern relates to a data protection breach you must follow our Data Breach Policy.

School ICT systems' capacity and security will be reviewed regularly and security strategies will be periodically discussed with the LA.

Systems Use and Data Security

Members of staff should not delete, destroy or modify any of the School's existing systems, programs, information or data which could have the effect of harming or exposing to risk or harm the School's, its staff, students, or any other party. Users are not permitted to make any physical alteration, either internally or externally, to the School's computer and network hardware.

If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage. All Software requests should be made to SLT. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

Users must not turn off or attempt to alter any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that have installed on their computer, phone or network or the School IT systems.

Users should only access areas of the Schools computer systems to which they have authorised access. Staff without authorisation should only be allowed to use terminals under supervision.

Where consent is given all files and data should always be virus checked before they are downloaded onto the School's systems. If in doubt, the employee should seek advice from SLT.

No device or equipment should be attached to our systems without the prior approval of SLT. This includes, but is not limited to, any PDA or telephone, iPad (or other mobile device tablet), USB device, i-pod, digital camera, MP3 player, infra red connection device or any other device.

Staff should not attempt to gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

We use a range of online programmes which store personal information in order to support and safeguard our pupils, including our assessment system Onwards and Upwards, Sleuth (behaviour), Motional (wellbeing), Arbor and CPOMS (safeguarding). Other school information that relies on our "Microsoft 365" accounts, including email, calendar, OneDrive files, Microsoft Teams and OneNote information can also be accessed remotely. All these and any other cloud based system must only be accessed on a device provided by school that has full password security or a mobile device that has full security in place and is not used by anyone else. These systems must NEVER be accessed on a public machine.

SeeSaw is an online system used to communicate with Parents and them with us. SeeSaw is extremely secure and fully GDPR compliant, with a full set of privacy features. Content posted to SeeSaw is fully monitored SLT. Only content related to a specific pupil can be posted to their timeline and staff need to be aware that they are tagging the correct child when posting. Whilst messages can also be sent on SeeSaw, all guidelines related to emails apply to content on SeeSaw too – content must be appropriate, professional and courteous and fully respectful of the child and their family.

Monitoring and Maintenance

The School may exercise its right to monitor the use of its ICT systems. Individual laptops/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the School's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by SLT to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Staff must ensure they keep operating systems up to date by always installing the latest updates.

On the termination of employment for any reason, staff are required to provide a full handover detailing the drives, folders and files where their work can be located and accessed. The School reserves the right to require employees to hand over all School data held in computer useable format.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy, or any other school policy;
- investigate a suspected breach of the law, this policy, or any other school policy.

The School reserves the right to disconnect devices or disable services without notification.

If staff have any concerns over the security of their device, they must seek advice from SLT.

Email Communications

Each teacher is provided with a "bristol-schools.uk" email address provided by Bristol City Council and accessed using Office 365 at https://mail.office365.com/

Any emails that are sent from a school account to an email ending in bristol.gov.uk, bristol-schools.uk, gsi.gov.uk / gsx.gov.uk / gse.gov.uk/ gcsx.gov.uk are automatically encrypted. We now also have the ability to send encrypted emails to a Third Party email system. If you need to send emails containing sensitive or confidential information, simply type "encrypt: " (with no speech marks but ensuring there is a space after the colon) in the subject line and this will then be encrypted. The receiver, if not on our email system, will need a one-time passcode (sent to their email address) to access the email.

The School's email system can be accessed from both the School computers, and via the internet from any computer. Wherever possible, all School related communication must be via the School email address.

Where possible staff should access their e-mails at least once every working day, stay in touch by remote access when travelling or working out of the office. Staff should endeavour to respond to e-mails marked 'high priority' as soon as is reasonably practicable.

The School recognises that it is not always possible to control incoming mail. Any material which would be considered as inappropriate or unprofessional, sexually explicit or offensive should be deleted at once.

Staff who receive an e-mail which has been wrongly delivered should return it to the sender of the message. If the e-mail contains confidential information or inappropriate material (as described above)

it should not be disclosed or forwarded to another member of staff or used in any way. SLT should be informed as soon as reasonably practicable.

The School monitors all e-mails passing through its systems for viruses. Staff should be cautious when opening e-mails from unknown external sources or where for any reason an e-mail appears suspicious (such as ending in '.exe'). SLT should be informed immediately if a suspected virus is received. The School reserves the right to block access to attachments to e-mail for the purpose of effective use of the system and compliance with this policy. The School also reserves the right not to transmit any e-mail message.

Email Etiquette

The School's e-mail facility is intended to promote effective communication within the business on matters relating to the School's business activities and access to the School's e-mail facility is provided for work purposes only.

Staff are strictly prohibited from using the School's email facility for personal emails at any time unless previously agreed by ELT. Staff should always consider if e-mail is the appropriate medium for a particular communication. The School encourages all members of staff to make direct contact with individuals rather than communicate by e-mail wherever possible to maintain and enhance good working relationships.

Members of staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages. If such messages are received, they should not be forwarded and should be reported to a member of the Senior Leadership Team immediately. If you feel that you have been harassed or bullied, or are offended by material sent to you by a colleague via e-mail, you should inform SLT who will usually seek to resolve the matter informally. If an informal procedure is unsuccessful, you may pursue the matter formally under the School's formal grievance procedure.

All members of staff should remember that e-mails can be the subject of legal action for example in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of staff who sent them and the School. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the School in the same way as the contents of letters or faxes.

E-mail messages may of course be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail is obliterated and all e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software. This should be borne in mind when considering whether e-mail is an appropriate forum of communication in the circumstances of the case and if so the content and language used.

The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the School does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school business is not permitted, unless in agreement with ELT.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Sending or forwarding chain junk mail, cartoons or gossip either within or outside the School is prohibited.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using a secure method including email encryption will be used when sending an email with sensitive information.
- Password protection on sensitive documents. The sender must ensure that the password is sent separately to the intended recipient (i.e. in a separate email or over the phone).
- Emails should not contain children's full names in the subject line and preferably, not in the main body of the text either. Initials should be used wherever possible.
- Access to school/setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication, and this will be recorded in the relevant files/records (such as safeguarding).
- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Where possible, emails must not contain personal opinions about other individuals, e.g. other staff members, children or parents. Descriptions of individuals must be kept in a professional and factual manner.
- Selling or advertising using the systems or broadcast messages about lost property, sponsorship or charitable appeals is prohibited.
- Agree to terms, enter into contractual commitments or make representations by e-mail unless the appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter.
- Downloading e-mail, text, music and other content on the internet which is subject to copyright protection is prohibited, unless it is clear that the owner of such works allows this.
- Send messages from another worker's computer or under an assumed name unless specifically authorised.

- Send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.
- E-mail may normally only be used to communicate internally with colleagues and students (where appropriate and necessary) and externally to parents, suppliers and third parties on academic/service related issues.

Internet Access

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to the School, especially if a member of staff has accessed, downloaded, stored or forwarded inappropriate material from the website. Staff may even be committing a criminal offence if, for example, the material is pornographic in nature.

Staff must not therefore access from the School's system any web page or any files (whether documents, images or other) downloaded from the web which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

As a general rule, if any person within the School (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that the School's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Staff should not under any circumstances use School systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information even in their own time.

Remember also that text, music and other content on the internet are copyright works. Staff should not download or e-mail such content to others unless certain that the owner of such works allows this.

The School's website may be found at http://www.briarwood.bristol.sch.uk/
This website is intended to convey our core values and excellence in the educational sector. All members of staff are encouraged to give feedback concerning the site and new ideas and inclusions are welcome. All such input should be submitted to the ICT Lead.

Staff should be aware that any personal use of the systems may be monitored and, where breaches of this policy are found, action may be taken under our Disciplinary Policy and Procedure.

The School reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers that personal use is excessive or otherwise in breach of this policy.

Internet access is monitored by Bristol City Council Trading with Schools IT Helpdesk, using the filtering system in place. This system filters out many different categories of websites, including web chat (social networks), and other potentially offensive websites. If someone tries to log on to a filtered website, they will be presented with a blue screen and be unable to proceed. Information about their computer and login username are also recorded in a central database. This database can be accessed by ELT and the I.T technician.

On occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website must be reported immediately to SLT. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Staff are not permitted to share access details to the School's network or Wi-Fi password with anyone else.

Internet access is provided for academic and professional use, with reasonable personal use being permitted. Staff must not therefore access from the School's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

YouTube is allowed onto handhelds and Chromebooks but this is only added if need be to groups or individual devices. YouTube is automatically in a safe mode along with google as a search engine.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct

Examples include:

- accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the School and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School);
- downloading or disseminating material in breach of copyright;
- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;

- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal. Where evidence of misuse is found, the School may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

File Storage

Staff members have their own personal area on the network, as well as access to shared network drives. Any school related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files.

No confidential, or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email. No school data is to be stored on a home computer.

The school's filing system can be accessed remotely using the "Schoolcloud" webpage or "GlobalProtect".

USB sticks are now prohibited.

Digital cameras

The School encourages the use of digital cameras, iPads/Pods and other video equipment; however staff should be aware of the following guidelines:

- Photos should only have the pupil's name if they are on display in school only. Photos for the website or press must only include the child's first name.
- The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones, iPads or similar.
- All photos should be downloaded to the School network as soon as possible.
- The use of mobile phones for taking photos of pupils is not permitted, unless previously agreed with ELT

Protecting Personal Data

Personal data of all stakeholders will be recorded, processed, transferred and made available according to the General Data Protection Act, 2018 (please see Data Protection Policy for more information).

Section 4 – Social Media

Social Networking

Briarwood School recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Twitter, LinkedIn, blogs and Wikipedia. However, staff use of social media can pose risks to the school's confidential and proprietary information, its reputation and it can jeopardise our compliance with our legal obligations.

This section of the policy deals with the use of all forms of social media including Facebook, Instagram, LinkedIn, Twitter, all other social networking sites, and all other internet postings, including blogs. It applies to the use of social media for both work and personal purposes, whether during work hours or otherwise, regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff.

Staff are allowed to use social networking sites at their discretion only in their own time and on their own ICT equipment. Bristol City Council Trading with Schools IT Helpdesk will block/filter access to open social networking sites across school devices.

Staff are also expected to be aware of what they write on social networking sites is generally in the public domain. Staff are personally responsible for what they communicate in social media. Staff should remember that what they publish might be available to be read by the masses (including the School itself, future employers and social acquaintances) for a long time. Staff should keep this in mind before they post content. Staff should also avoid social media communications that might be misconstrued in a way that could damage the School's reputation, even indirectly.

Personal use of social media is never permitted during working time or by means of our computers, networks and other IT resources and communications systems. Staff should not use a work email address to sign up to any social media and any personal social media page should not make ANY reference to their employment at Briarwood School. Staff must not take photos or posts from social media that belongs to the School for their own personal use. Staff must ensure that their profile and any content posted are consistent with the professional image they are required to present to colleagues, pupils and parents. Staff are also asked not to include the name of the school in any information on their social networking profile.

Staff should never make contact with other pupils (past or present), parents or carers on Facebook except with specific permission from the EHT or DSL. Staff should never post any

details whatsoever, including first names or photos, of pupils or parents/ carers of the school. Staff must ensure that their profile and any content posted are consistent with the professional image they are required to present to colleagues, pupils and parents. Staff must avoid posting comments about confidential or sensitive School related topics. Even if Staff make it clear that their views on such topics do not represent those of the School, such comments could still damage the School's reputation and incur potential liability.

If a member of Staff is uncertain or concerned about the appropriateness of any statement or posting, he or she should refrain from making the communication until he or she has discussed it with their Line Manager. If a member of Staff sees content in social media that disparages or reflects poorly on the School, it's Staff, pupils, parents, service providers or stakeholders, he or she is required to report this in the first instance to SLT without unreasonable delay. All staff are responsible for protecting the School's reputation.

The key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the School, staff and students at all times and must treat colleagues, students and associates of the School with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly, and users should ensure that neither their personal or professional reputation and/or the School's reputation, nor the reputation of individuals within the School are compromised by inappropriate postings.
- Use of social networking sites for school business is not permitted, unless via an officially recognised school site and with the permission of ELT.
- Members of staff will notify SLT if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the School/setting.
- No school information, communication, documents, videos and/or images should be posted on any personal social networking sites.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos, which show pupils of the School who are not directly related to the person posting them, should be uploaded to any site other than the School's Website.
- No comment, images or other material may be posted anywhere, by any method that may bring the School or, the profession into disrepute.
- Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook). If, in exceptional circumstances, users wish to do so, please seek advice from ELT.

Compliance

Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

- Breach our Electronic information and communications systems policy;
- Breach our obligations with respect to the rules of relevant regulatory bodies;
- Breach any obligations they may have relating to confidentiality;
- Breach our Disciplinary Rules;
- defame or disparage the School, its Staff, its pupils or parents, its affiliates, partners, suppliers, vendors or other stakeholders;
- Harass or bully other Staff in any way or breach our Anti-harassment and bullying policy;
- Unlawfully discriminate against other Staff or third parties or breach our Equal opportunities policy;
- Breach our Data protection policy (for example, never disclose personal information about a colleague or children online);
- Breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

Educational or Extra Curricular Use of Social Media

If your duties require you to speak on behalf of the School in a social media environment, you must follow the protocol outlined below.

The EHT may require you to undergo training before you use social media on behalf of the School and impose certain requirements and restrictions with regard to your activities.

Likewise, if you are contacted for comments about the School for publication anywhere, including in any social media outlet, you must direct the inquiry to the EHT and must not respond without advanced written approval.

Staff Protocol for use of Social Media

Where any post is going to be made on the School's own social media (Facebook and Twitter feed), the following steps must be taken:

1. No personally identifiable information about children, staff or parents is to go on the school Twitter feed or Facebook page. This includes names or identifiable photographs. These forums are for general school news only. Even if a child has permission to have their photos on the website, they still should not be posted on to the school's social media sites, due to the ease of commenting, sharing and tagging on these sites - this adds to the risk of the school losing control of these images.

2. Ensure that there is no identifying information relating to a child/children in the post - for example any certificates in photos are blank/without names or the child's name cannot be seen on the piece of work.

3. Our main communication with parents, especially regarding pupil achievement, is still through SeeSaw, however general information about classes or the school can be posted on Social Media. The school newsletter should not be shared directly to social media but a link to the newsletter on the school website can be posted.

4. The proposed post must be presented to SLT for confirmation that the post can 'go live' before it is posted on any social media site.

5. PA to the Executive Headteacher posts the information, but all staff have responsibility to ensure that the Social Media Policy has been adhered to.

Recruitment

The School may use internet searches to perform pre-employment checks on candidates in the course of recruitment. Where the School does this, it will act in accordance with its data protection and equal opportunities obligations.

The School Web-Site

The contact details on the web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

ELT and the EH's PA will take overall editorial responsibility and ensure that content is accurate and appropriate.

Photographs that include pupils will be selected carefully. The Admin team have a list of those parents who have given permission for their child's photo to be displayed on the website. This is updated annually.

Pupils' full names will not be used anywhere on the web site, and no names will be given alongside photographs in keeping with our GDPR policy.

Photographs for use of Social Media

Any photos for the school website or social media pages (Facebook and Twitter posts may only be taken using school cameras/devices or devices. Where any device is used that does not belong to the School all photos must be deleted immediately from the device, once the photos have been uploaded to a device belonging to the School.

Respecting intellectual property and confidential information

Staff should not do anything to jeopardise School confidential information and intellectual property through the use of social media.

In addition, Staff should avoid misappropriating or infringing the intellectual property of other School's, organisations, companies and individuals, which can create liability for the School, as well as the individual author.

Staff must not use the School's logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without express prior written permission from the Head Teacher.

To protect yourself and the School against liability for copyright infringement, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the Head Teacher in the first instance before making the communication.

Section 5 – Own Devices

Mobile Devices

Mobile devices within the context of this policy includes any mobile phone, tablet, laptop, MP3/iPod or other device which is capable of connecting with the internet or mobile networks or taking image or sound recordings.

Mobile phones are permitted in school, with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard/locker.
- Personal mobile phone cameras are not to be used on school trips. The School provides [digital cameras/trip phones] for this purpose.
- All phone contact with parents regarding school issues will be through the Schools phones. Personal mobile numbers should not be given to parents at the School.

WhatsApp is not permitted for use on School issued devices or personal devices for School business. Members of staff are able to use WhatsApp on their own devices for personal communication however, staff should not communicate internally with other staff members for School business using their personal WhatsApp accounts, sharing School related information which could include categories of personal data.

Staff are able to use devices at work and outside of work for work related activities provided the terms of this policy are met. The School reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

The safety of the user's own device is the responsibility of the user.

No personal equipment should be connected to or used with the School's ICT systems.

When out of School, staff should access work systems on their mobile device using remote access via The Cloud.

Any apps or software that are downloaded onto the user's device whilst using the School's own network is done at the users risk and not with the approval of the School.

Devices may not be used at any time to:

- Store or transmit illicit materials;
- Store or transmit proprietary information belonging to the School;
- Harass others;
- Act in any way against the School's Acceptable Use section of this policy and other safeguarding and data related policies.

Technical support is not provided by the School on the user's own devices.

When using personal data, it is the user's responsibility to ensure they keep data secure on their device. This includes preventing theft and loss of data (for example through password protection and cloud back up), keeping information confidential (for example by ensuring access to emails or sensitive information is password protected) and maintaining that information.

The School does not accept responsibility for any loss or damage to the user's device when used on the School's premises. It is up to the user to ensure they have their own protection on their own device (such as insurance).

Staff are prevented from installing email applications which allow direct access to School emails without use of a login/password.

The use of camera, microphone and/or video capabilities are prohibited whilst in School unless this has been approved by ELT. If approved, any pictures, videos or sound recordings can only be used for School purposes and cannot be posted or uploaded to any website or system outside of the School network.

You must not use your device to take pictures/video/recordings of other individuals including staff without their advance written permission to do so.

If information is particularly sensitive then users should ensure that the data is either appropriately secured or deleted from the device (including from any local copies which may have been stored on the device.

In the event of any loss or theft of personal data, this must be reported immediately as a data breach in accordance with the School's Data Breach policy.

The School will not monitor the content of the user's own device but will monitor any traffic over the School system to prevent threats to the School's network.

The School may require access to a device when investigating policy breaches (for example, to investigate cyber bullying).

Section 6 - Education and Training

Educating Pupils

At Briarwood, our bespoke curriculum is highly adapted for our pupils in terms of ensuring it is meaningful to them whilst ensuring we are meeting their statutory curriculum needs. Relationships are taught predominantly within our Myself curriculum. The safe use of social media and the internet will also be covered where relevant jn an age and stage appropriated manner. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children and victims of abuse.

Pupils are taught about a range of E-Safety issues including social networking and gaming online sites and what information should not be shared on such sites as part of the "E-Safety" Computing scheme of work. The purpose of this is to acknowledge (although not condone) the reality that some pupils may already have access to social networking sites by this age. When appropriate, some of our more able pupils are able to use assessment app SeeSaw to send messages to each other's SeeSaw Accounts in a secure environment.

Pupil Access

Any students using computers can use the generic "pupil" log in, password: briarwood (Under Pupil Access). This was created to give it access to a Pupil folder on Schoolcloud which can in turn be put onto iPads.

Teachers should teach pupils about emailing using their school email address only. Pupils will be supported using e-mail and all staff should immediately tell a teacher/designated safeguarding lead if they or a pupil receive offensive e-mail or text. All pupil e-mails will be treated as public.

Pupils are prohibited from having mobile phones or other electronic equipment in school unless specified by SLT or for therapy reasons, for example, a communication device.

All users must be polite and considerate online and report any issues that are likely to cause offence to others.

Internet access is monitored by Bristol City Council Trading with Schools IT Helpdesk, using the filtering system in place.

Photos and videos of children can be taken whilst they are completing work, for assessment and celebration. These must be taken on school iPods or iPads unless otherwise agreed by ELT/DSL.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, it is recognised that it is not possible to guarantee that unsuitable material will never appear on a school computer.

Where appropriate, apps used directly by pupils will need to meet the requirements of the Information Commissioner Office Children Code for age appropriate design

Where apps are purchased for the use directly by pupils, they must ensure that the suppliers confirm that the app fully meets the requirement of the Children's Code for age appropriate design.

Educating Parents

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website.

This policy will also be shared with parents via our website.

Online safety will be covered during parents' evenings and concerns or queries about this policy can be raised with any member of staff who can pass this on to SLT.

There is also E-Safety information, including a presentation, available on our website to support parents.

Educating Staff

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, 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 the risks up and develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The Designated Safeguarding Leads 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.

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

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

The DSL alongside ELT will ensure regular training in order to keep up to date with the latest recommendations, including updating any policies due to changes in legislature.

E-safety will continue to form part of our In Service Training. There will be regular briefings for staff. Any bespoke training needs which arise between these times can be referred in the first instance to SLT.

All staff must read and sign the E-Safety Acceptable Use Agreement (Appendix 1) before using any school ICT resource.

Section 8 - Conclusion

Monitoring

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found on CPOMS.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. The review 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.

Failure to Comply with the Policy

Access to the internet and digital communication media have the potential to greatly enhance learning and engagement with parents, and our school is committed to extending these opportunities whilst maintaining the highest standards of safety. However, it is everyone in the school's personal responsibility to work towards keeping themselves and others safe online.

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours and regardless of whether the School's equipment or facilities are used for the purpose of committing the breach.

Any member of staff suspected of committing a breach will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details. Staff may be required to remove internet postings which are deemed to constitute a breach. Failure to comply with such a request may in itself result in disciplinary action.

Any unauthorised use of the School's ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which ELT considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The School reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the School's Disciplinary Policy and Procedure. Access is granted to the web, telephones and to other electronic systems, for legitimate work purposes only.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- Transmitting a false and/or defamatory statement about any person or organisation;
- Sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others;

- Transmitting confidential information about the School and any of its staff, students or associated third parties;
- Transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School;
- Downloading or disseminating material in breach of copyright;
- Copying, downloading, storing or running any software without the express prior authorisation of SLT
- Engaging in on line chat rooms, instant messaging, social networking sites and on line gambling;
- Forwarding electronic chain letters and other materials;
- Accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Misuse and Complaints

Due to the complex medical and sensory needs of our pupils, any misuse of the schools ICT systems will be investigated by SLT and a realistic, appropriate response will be taken in line with our behaviour and safeguarding policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Complaints of a safeguarding nature must be dealt with in accordance with schools safeguarding procedures.

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 Code of Conduct and staff disciplinary procedures. 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.

Links with other policies:

Our E-Safety policy will be reviewed annually. This policy should be read and adhered to in conjunction with the following policies:

- Child Protection and Safeguarding policy
- Behaviour Policy
- Staff Disciplinary Procedures
- Code of Conduct
- Data Protection Policy
- Complaints Procedure

APPENDIX 1

E-Safety Acceptable Use Agreement

Staff Roles and Responsibilities

Staff must never share their individual login password with anyone as these can be used to monitor action taken when logged on. Every user is individually responsible at all times for the action taken while their user name is in use.

To ensure data security, any portable device taken off the premises must be password protected. USB sticks are prohibited. Any personal mobile phones used to receive school emails must have full security protection.

The school's file system can be accessed remotely using the "Schoolcloud" webpage or "GlobalProtect". Our assessment system "Onwards and Upwards" is also a web based system, as is personal information stored in "Choose It Maker 3". Other school information that relies on our "Microsoft 365" accounts, including email, calendar, OneDrive files, Microsoft Teams and OneNote information can also be accessed remotely. All these and any other cloud based system must only be accessed on a device provided by school that has full password security or a mobile device that has full security in place and is not used by anyone else. These systems must NEVER be accessed on a public machine.

Personal devices cannot access the school's WiFi at any time.

The school and the Bristol City Council Trading with Schools IT Helpdesk are responsible for authorising any user of its internet or e-mail facilities, monitoring and policing their use.

Any member of staff who commits a serious offence in the use of the school's internet service may be subject to the school's staff disciplinary procedures.

Any user, adult or pupil, who breaks the law in respect of using the school's internet service, will be reported to the police.

Staff or administrative users will protect the school from computer virus attack or technical disruption by not downloading from the Internet any programs or executable files other than by agreement with SLT.

Never provide details or information of your own, or any other person or pupil that could relate to Briarwood School to internet sites including .i.e. Facebook, twitter, etc. Exceptions should be checked with SLT.

Staff are allowed to use social networking sites (or web blogs /forums/ chat rooms) at their discretion ONLY in their own time and on their own ICT equipment. Staff should never make contact with other pupils, parents or carers on these sites except with specific permission from the EHT. Staff are also expected to be aware of what they write online is generally in the public domain. Staff should never post any details whatsoever, including first names or photos, of pupils or parents/ carers of the school.

If you see any unacceptable site or material as a result of an innocent internet query, unsolicited pop-up window or in any other way, report it immediately to the ICT Technician. Action can then be taken i.e. contacting Trading with Schools to block the site or material.

Staff or approved adult school users should at all times abide by the copyright laws in respect of documents and materials downloaded from the internet.

Staff using a school laptop or other device off the school site, at home or elsewhere, will still have to abide by the school's E-Safety Policy. Colleagues will be aware that the misuse of such devices for activity not agreed by the school may be breaking the law under the Computer Misuse Act 1990. School devices ae monitored at all times, even when not on the cool network.

Always check that a pupil's parents/carers have given permission before submitting photos to the school website or any other area.

Staff will at all times work to maximise the safety of pupils within their care in their use of the internet. YouTube and Google need to be closely monitored when in use.

Colleagues will be aware of the ethos, standards, equalities and ethnic mix of the school and will not access any internet material, or work with the internet, in any way that infringes or offends these.

The E-Safety Policy for all school staff and approved adult users of the school will be posted on the school website and/or made available in the office and on the network in the Policies folder.

APPENDIX 2

Online safety training needs – self audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	Date:
Question	Yes/No
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	