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, Appendix 1 | 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 |
| Aug 2018 | | Reviewed and updated with GDPR information |
| Aug 2019 | | Reviewed |
| Aug 2020 | | Reviewed<br>Clarification on portable storage - no longer allowed at all.<br>Information added regarding the Social Media policy and school Facebook page. |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# E-SAFETY POLICY

## Writing and Reviewing the E-Safety Policy

The E-Safety co-ordination will be a shared role between the ICT and GDPR Strategic Lead, ICT Technician and Senior Management Team.

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

- Electronic Information and Communication Systems Policy
- Information Security Policy
- Data Breach Policy
- Data Protection Policy
- Data Retention Policy

## 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.

Internet use is a part of the statutory curriculum and is a necessary tool for staff and pupils.

Everyone in the school community has a personal responsibility to work towards keeping themselves and others safe online.

## Infrastructure

School ICT systems' capacity and security will be reviewed regularly. Internet access is provided through Bristol City Council which is a filtered service. It is designed expressly for pupil use and will include filtering appropriate to the age of the pupils.

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.

Security strategies will be periodically discussed with the LA.

USB sticks cannot be used – there are secure cloud systems (NextCloud and OneDrive) in place to support home working.

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

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 password that cannot be easily broken and which contains at least 6 characters including both numbers and letters.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team who will liaise with the ICT and GDPR Strategic Lead as appropriate and necessary. 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.

If given access to the School e-mail system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership Group and/or ICT and GDPR Strategic Lead 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.

Logging off prevents another member of staff accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that he or she was not the party responsible.

Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of ICT and GDPR Strategic Lead.

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.

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.

## Policy and Practice

### Roles and Responsibilities:

The ICT and GDPR Strategic Lead, ICT Technician and Senior Management Team (SMT) will manage and monitor E-Safety as part of their safeguarding responsibilities.

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 the ICT and GDPR Strategic Lead.

YouTube is currently accessible only on PCs under adult supervision. The supervising adult must login to YouTube first using: Username: pupil@briarwood.bristol.sch.uk Password: Briarwood2016 – the majority of inappropriate content will then be filtered out. YouTube is not permitted on ANY hand held devices, including iPads and iPods. It should be inaccessible on all school devices but if this is not the case, please contact the ICT and GDPR Strategic Lead immediately.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The school has clearly set out roles and responsibilities in relation to internet use and these can be seen in the Appendix and in the related polices referred to at the beginning of this document.

## Misuse and Complaints

If staff or pupils discover an unsuitable site, it must be reported to the SMT who will immediately report it to BCC Trading with Schools IT Helpdesk to ensure it is filtered out.

Complaints of internet misuse will be dealt with by a senior member of staff and any complaint about staff misuse must be referred to the head teacher.

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

Login 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. Any students using computers can use the generic "pupil" log in, which does not require a password.

## Education and Training

## E Safety

Teaching of E-Safety has been rolled out across the school in light of the higher ability intake of students who can access the internet more independently. This includes:

- Department assemblies about E-Safety
- School displays
- Lessons about E-Safety specifically targeted at higher ability classes, delivered as part of our new Computing curriculum.

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

## Managing Internet Access for Teaching

Pupils will not carry out internet searches unless they have first been tested by a teacher/adult to ensure that they do not produce results containing inappropriate material. Safer "child friendly" ways of searching the internet are also available.

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.

## Training

The ICT and GDPR Strategic Lead will attend regular training in order to keep up to date with the latest recommendations.

E-safety will continue to form part of our In Service Training. There will be regular briefings for staff. Staff will receive training on how to carry out internet searches safely and efficiently and minimise risk. This will be led by Senior Management and/ or the ICT and GDPR Strategic Lead. Any bespoke training needs which arise between these times can be referred in the first instance to the ICT and GDPR Strategic Lead.

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

## Electronic Communications (e-mail and text)

Please see the "ELECTRONIC INFORMATION AND COMMUNICATION SYSTEMS POLICY" (Email Etiquette and content section) for more information about appropriate email communication.

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/

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 must not reveal personal details of themselves or others in any online communication or arrange to meet anyone.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

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 forwarding of chain messages is not permitted.

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

Teachers will agree with the class any timescales and responses to online messages and rules for collaborating online.

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.

## Social networking and personal publishing

Bristol City Council Trading with Schools IT Helpdesk will block/filter access to open social networking sites.

Higher Ability students can use SeeSaw to send messages to each other's SeeSaw Accounts in a secure environment.

Higher Ability students will be taught about the potential risks of social networking 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.

Staff are allowed to use social networking sites 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 Facebook except with specific permission from the Headteacher or ICT and GDPR Strategic Lead. Staff are also expected to be aware of what they write on social networking sites, especially Twitter which 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. Staff are also asked not to include the name of the school in any information on their social networking profile.

## Published content and 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.

The ICT Co-ordinator and SLT 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.

Pupils' full names will not be used anywhere on the web site, particularly in association with photographs.

We have our own Facebook page – no photos or names of children are put on this at all – please see the separate Social Media policy for details.

## Protecting personal data

Personal data of all stakeholders will be recorded, processed, transferred and made available according to the General Data Protection Act, 2018. See the Data Protection Policy, Data Breach Policy, Data Retention Policy and Information Security Policy for further information.

## Conclusion

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.

Everyone in school has a personal responsibility to work towards keeping themselves and others safe online.

# 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.

No USB sticks or portable storage will be used to store school information. Cloud Storage is available (OneDrive) that is managed by ICT Services. 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. 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 the school's ICT and GDPR Strategic Lead.

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 the Headteacher or ICT and GDPR Strategic Lead.

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 Headteacher. Staff are also expected to be aware of what they write online, especially on Twitter which 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 Co-ordinator or 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 covered by the "GDPR Staff and Pupil Consent" spreadsheet, a copy of which can be found on TEACHERS:\GDPR\GDPR Staff and Pupil Consent.

Staff will at all times work to maximise the safety of pupils within their care in their use of the internet. You Tube 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.