Bullers Wood Multi-Academy Trust

E-Safety Policy

Bullers Wood School and Bullers Wood School for Boys

Policy created by: Deputy Headteacher (ICT)	**Date of Adoption: 1st September 2018**	**Date to be Reviewed: July 2019**	**To be reviewed by AHT ICT**

The use of ICT in Bullers Wood Schools

The use of ICT in Bullers Wood Schools

Bullers Wood MAT aims:

- to use ICT within teaching and learning to raise educational standards and promote achievement
- to develop a coherent approach to the use of ICT and make informed judgments about when and how to apply aspects of ICT to obtain optimum benefit
- to encourage both staff and students to recognize and use ICT applications which are fit for purpose
- to develop students' critical thinking and problem solving skills
- to provide a wide range of opportunities for student creativity and imagination
- to encourage students to be independent learners
- to develop analytical and evaluative skills
- to develop students' research skills, including the ability to use information sources

The hardware and software provided by the Schools must be used sensibly and appropriately so that it does not become damaged. Students must not cause any damage to the resources. During lesson time students may only use the ICT resources for the applications specified by the class teacher. They may not engage in personal work which is not part of the lesson. The internet and email are provided for the purpose of research and communication related to the curriculum.

Students should be aware of and understand the implications of the '15 rules for responsible ICT use' Appendix A. Staff should be aware of and understand the implications of the 'Acceptable Use policy' Appendix B.

ICT is taught both as a discrete subject and to support and enrich other subjects; up to date information may be gained through Internet access. Personalised Learning packages are available to encourage independent learning. Subject specific software allows students to extend their skills. Subject leaders regularly review available hardware and software resources to support learning needs and develop learning opportunities. Classrooms are equipped with interactive whiteboards and dedicated desktop(s). The School makes specialist ICT provision for the teaching of ICT, modern languages, Art, Design Technology, Music Technology. ICT rooms are available for booking by other subjects. ICT is also valuable as a means of supporting students with additional education needs.

The Schools have specialist software to support administrative requirements, including SIMS information management systems with applications for Financial Management, Student and Staff records, Assessment, Recording and Reporting and Timetabling.

Legislation

The School is governed by the following legislation

Data Protection Act – The School uses data relating to staff and students in accordance with the Data Protection Act. Student data is collected to enable staff and support agencies to provide a high quality of education and to monitor and record student performance and attendance. Student performance data is communicated to parents/carers through regular reporting opportunities.

The School uses students' images to promote events and as a part of teaching and learning. Parents/carers are required to complete a consent form for the use of student images. See Appendix C. Students' names will not be linked to images as a means of identification.

Copyright - Staff and students should ensure that, when downloading and copying material from the Internet, these activities comply with copyright legislation. Further Information may be obtained from www.cla.co.uk

Computer Misuse - The use of computers for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Monitoring of Use - Staff and students should be aware that Internet traffic can be monitored and traced to the individual user and that the School has the right to monitor the use of the School's computer systems, including the use of the Internet and the interception and monitoring of email. Inappropriate material will be removed without warning and files will be subject to deletion if unauthorized use of the Schools' computer

system is taking place. If appropriate each School's behaviour (students) or disciplinary (staff) procedures will then be invoked. Where applicable, police or local authorities may also become involved.

Bullers Wood School E-Safety Policy

The E - Safety policy is part of Bullers Wood Safeguarding Policy and Procedure and relates to other policies including Behaviour and Citizenship.

The Schools seek to do the following:

- Raise awareness and understanding of e-safety issues amongst students whilst using Bullers Wood equipment
- Ensure staff understand the importance of e-safety in safeguarding and develop their understanding of the signs and indicators of abuse
- Ensure all members of staff are aware of actions required to assist a child or young person who reports abuse
- Staff and students know how to report online abuse
- Ensure all staff know how to respond to a young person who discloses abuse
- Establish safe access to the Internet for children and young people
- Provide a systematic means of monitoring children known or thought to be at risk of harm
- Ensure that all adults who have access to children's information have been checked as to their suitability and have an advanced DBS disclosure, as well as a List 99 Check

Managing the Internet Safely

The Internet is a powerful tool in teaching and learning but must be used sensibly and appropriately. All young people need to learn to evaluate everything they read, hear and view and to refine their own communications with others via the Internet. Bullers Wood Internet access is designed expressly for students to use on its projects. Students will be advised on what Internet use is acceptable, what is not and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the project requirements and student's age.

Staff and students may not knowingly search for material that is profane or obscene (pornography), advocates illegal acts, or that advocates violence or discrimination towards other people.

Infrastructure and Software:

Bullers Wood School and Bullers Wood School for boys:

- Have additional user-level filtering in-place;

- Ensures network health through appropriate anti-virus software etc. and network set-up so staff and Students cannot download executable files such as .exe / .com / .vbs etc.;
- Ensures their network is 'healthy' by having in house health checks annually on the network;
- Ensures the Deputy Headteacher/AHT (ICT) / Network Manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows students access to Internet logs;
- Uses security time-outs on Internet access where practicable / useful;
- Uses individual log-ins for students and all other users;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Never allows personal level data off-site unless it is on an encrypted device;
- Uses 'safer' search engines and activates 'safe' search where appropriate;
- Ensure that staff inform IT services department of planned software purchases so that installation, licenses and compatibility can be carefully managed.

Ensures students only publish within appropriately secure learning environments such as Bullers Wood Schools VLE

Some material available via the Internet is unsuitable for students. Bullers Wood Schools will work in partnership with parents, the Local Authority, DfE and the Internet Service Provider to ensure that systems are in place to protect students and that these are reviewed and improved where appropriate. However, due to the international scale and linked nature of the Internet, it is not possible to guarantee that unsuitable material will never appear on a School computer. The School cannot accept liability for information accessed or any consequences of Internet use.

Policy and procedures:

Bullers Wood School and Bullers Wood School for Boys:

- Supervises students' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older students have more flexible access;
- We use a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, social networking sites and any other sites not deemed as needed for educational purposes;
- Encourages staff to preview all sites before use or only use sites accessed from managed 'safe' environments such as the VLE
- Plans the curriculum context for Internet use to match students' ability, using child-friendly search engines where more open Internet searching is required;

- Is vigilant when conducting 'raw' image search with students e.g. Google or Lycos image search;
- Informs users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the IT Services Department, the Deputy Headteacher/AHT (ICT) or a Head of Year. Our systems administrators report to LA where necessary. Staff can also report any incidents.
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks social networking sites for specific purposes / Internet Literacy lessons;
- Only uses Bullers Wood VLE for student's own online creative my site areas;
- Has blocked student access to music downloads
- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme; Appendix D
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in line with the School behaviour management system;
- Ensures the named Child Protection and Safeguarding Officer has appropriate training;
- Ensures parents provide consent for Students to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their daughter's / son's entry to the School; Appendix C
- Makes information on reporting offensive materials, abuse / bullying etc available for students, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Managing email

Email is now an essential means of communication for staff at Bullers Wood School and increasingly for students. Directed email use in Schools can bring significant educational benefits through increased ease of communication between students and staff, or within local and international school projects. All staff and students are provided with their own school email address. Students must immediately inform a teacher, staff must immediately inform the Network Manager, if they receive inappropriate or offensive email.

External emails should be written carefully and, where appropriate, authorised before sending as they represent the School and are in the public domain. External emails include a disclaimer.

It is an offence to send obscene, indecent or menacing pictures. The forwarding of anonymous messages and chain letters is not permitted. The use of obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language is not permitted. Emails found to be containing such language may be subject to the School's behaviour (for students) or disciplinary procedures (for staff).

Staff and students should be aware that emails can be required to be available to external parties under the Freedom of Information Act.

Bullers Wood School:

- Does not publish personal email addresses of students or staff on the School website. Bullers Wood School will use office@bwsgirls.org or office@bwsboys.org for any communication with the wider public.

- If one of our staff or students receives an email that we consider is particularly disturbing or breaks the law we contact the police.
- Accounts are managed effectively, with up to date account details of users
- Messages relating to or in support of illegal activities may be reported to the authorities.
- Spam, phishing and virus attachment can make email dangerous; filtering software is used to stop unsuitable mail.

Students:

- We only use Bullers Wood School email with Students.
- Students can only use the School domain email accounts on the School system.
- Staff can only use the School domain email accounts to communicate with students.
- Students are introduced to, and use email as part of the ICT scheme of work.
- Students are taught about the safety and 'netiquette' of using email i.e.
    - not to give out their email address unless it is part of a school managed project or someone they know and trust and is approved by their teacher and parent/carer;
    - that an email is a form of publishing where the message should be clear, short and concise;
    - that any email 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;
    - they must not reveal private details of themselves or others in email, such as address, telephone number, etc.

- to ‘Stop and Think Before They Click’ and not open attachments unless sure the source is safe;
- the sending of attachments should be limited;
- embedding adverts is not allowed;
- that they must immediately tell a teacher / responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages,
- not to delete malicious of threatening emails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them;
- that forwarding ‘chain’ email letters is not permitted;

- Students sign the School Agreement Form to say they have read and understood the E-Safety rules, including email and we explain how any inappropriate use will be dealt with. Appendix A

Staff:

- Staff use Bullers Wood School email systems for professional purposes;
- Access in school to external personal email accounts may be blocked;
- Email sent to an external organisation is written carefully (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the School ‘house-style’;
  - the sending of attachments should be limited;
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed.

- Staff sign the Acceptable Use Policy (Appendix B) to show that they have read and understood the E-Safety rules, including email and we explain how any inappropriate use will be dealt with.

Use of digital and video images

The purpose of the School website is to inform about the School and to facilitate communication with parents/carers, students, and prospective parents/carers and students, as well as other parties (e.g. job applicants). The Headteachers have the overall editorial responsibility and ensures that content is accurate and appropriate. The delegated member of each school’s SLT and E-Safety Officer oversees who has the authority to upload content into sections of the website.

The copyright of all material must be held by the School, or be attributed to the owner where permission to reproduce has been obtained.

At Bullers Wood School and Bullers Wood School for Boys:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;

- Uploading of information is restricted to:
- Headteacher, Deputy Headteacher/AHT (ICT) and IT Services Department Staff (authorised through Headteacher) – all areas.
- The School web site complies with the School's guidelines for publications;
- Most material is the School's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the School address and telephone number. Home information or individual email identities will not be published;
- Photographs published on the web do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the School agreement form when their daughter / son joins the School; Appendix C
- Digital images / video of students are stored in the teachers' shared images folder on the network and images are deleted regularly – unless an item is specifically kept for a key School publication for example the School year book.
- We do not use students' names when saving images in the file names or in the tags when publishing to the School website;
- We do not include the full names of students in the credits of any published School produced video materials / DVDs;
- Staff sign the School's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of students; Appendix B
- Students are only able to publish to their own my site area on the School VLE
- Students are taught about how images can be abused in their e-safety education programme;

Students must not use digital cameras or camera phones in school or on school trips and visits to take or distribute photographs of other students or staff without their knowledge or consent. Any student or staff member who is concerned that they have been photographed without their consent or that someone is misusing their camera or phone, should immediately report their concerns to a teacher or member of senior staff.

Twitter

The Schools have a Twitter account to correspond with parents and students; permissions will be authorised by the Schools. We ask that staff do not request to follow this account. All information posted on Twitter will be available to staff on the school calendar, VLE or in staff briefing.

If staff have a **Personal Twitter account** we remind them that "you are what you tweet". If they have a public account, anyone (including students) can read what they are saying.

As a member of staff at Bullers Wood School if you use Twitter or other social networking sites:

- You will never be derogatory to any member of staff or bring the school name into disrepute.
- You will never engage knowingly with a pupil outside of school.
- You will retain a personal/professional boundary at all times.
- You will never post pictures of the children or refer to them at any time.

We advise that staff ensure that their Twitter account is 'Private' in order to do this tick the "Protect my Tweets" option, under Tweet privacy, in Settings.

Social networking and personal publishing

The Internet has online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Students are encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photograph or image or address once published. Examples include: blogs, wikis, MySpace, Bebo, Piczo, Windows Live Spaces, MSN space, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

- Bullers Wood School will block access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, School attended, IM and email addresses, full names of friends, specific interests and clubs etc.
- Students are advised not to place personal photographs or images on any social network space. They should consider how public the information is and consider using private areas. Students are advised to be aware of the background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Teachers are advised not to run social network spaces for student use on a personal basis.
- Students are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students are encouraged to invite known friends only and deny access to others.

- Students are advised not to publish specific and detailed private thoughts.
- Teachers must not use personal accounts to communicate with or contact students on social networking sites for example 'Facebook'. Forums linked directly to the curriculum are set up in consultation with the Deputy Headteacher (ICT).

Managing equipment

The computer system / network is owned by the Schools and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.
The School reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely Bullers Wood School and Bullers Wood School for Boys:

- Ensures staff read and sign that they have understood the Acceptable Use Policy (Appendix B). Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- Provides students with an individual network log-in username. From Year 7 they are also expected to use a personal password;
- Makes it clear that staff must keep their log-in username and password private and must not leave them where others can find;
- Makes clear that students should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Makes clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;
- Has set-up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves (computers automatically lock after 40 minutes).
- Requests that teachers and students do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day / we automatically remotely switch off all computers at 17.00 for students and 18.00 for staff.

- Has set-up the network so that users cannot download executable files/ programmes;
- Has blocked access to music download
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software installed.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the School, is used solely to support their professional responsibilities and that they notify the School of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any corporate policies e.g. Borough email or Intranet; Finance System, Personnel System etc.
- Maintains equipment to ensure Health and Safety is followed;

- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access the report writing module.
- Ensures that access to the School's network resources from remote locations by staff is restricted and access is only through School / LA approved systems.
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems e.g. technical support or SIMS Support through LA systems;
- Provides students and staff with access to content and resources through the VLE which staff and students access using their Shibboleth compliant username and password.
- Uses the DfE secure s2s website for all CTF files sent to other Schools;
- Ensures that all student level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the School ICT systems regularly with regard to security.

How will infringements be handled?

Whenever a student or staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the Headteacher at the school that the member of staff is employed at.. The following guidance will be used:

Students - Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

Possible Sanctions: referred to class teacher / tutor / senior manager / e-safety coordinator/removal of phone until end of week/contact with parent

Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups
- Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

Possible Sanctions: referred to Class teacher/ Head of Department / Guidance & Support Leader / eSafety Coordinator / removal of Internet access rights for a period / removal of phone until end of day / contact with parent

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

Possible Sanctions: referred to Class teacher / Year Tutor / eSafety Coordinator / Headteacher / removal of Internet and/or Learning Platform access rights for a period / contact with parents / removal of equipment

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform LA / Synetrix as appropriate

Category D infringements

- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the GDPR and Data Protection Act, updated DPA to 2018 and added GDPR
- Bringing the School's name into disrepute

Possible Sanctions – Referred to Headteacher / Contact with parents / referral to Inclusion suite / possible exclusion / removal of equipment / refer to Community Police Officer / LA e-safety Officer

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's email service provide

Staff

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the World Wide Web that compromises the staff members' professional standing in the School and community.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.

Sanction - referred to line manager / Headteacher. Warning given.

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any School / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the GDPR and Data Protection Act, updated DPA to 2018 and added GDPR
- Bringing the School name into disrepute.

Sanction – Referred to Headteacher / Governors through School disciplinary procedures; report to LA Personnel/ Human resources, report to Police

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the School's ICT managed service providers - to ensure there is no risk of students accessing inappropriate materials in the School.
- Identify the precise details of the material.

Child Pornography In the case of Child Pornography being found, the member of staff will be immediately suspended and the Police will be called.

How will staff and students be informed of these procedures?

- They will be fully explained and included within the School's E-Safety/Acceptable Use Policy. All staff will be required to sign the School's e-safety Policy acceptance form;
- Students will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Students will sign an age appropriate e-safety / acceptable use form;
- The School's E-Safety Policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the School.
- Information on reporting abuse / bullying etc will be made available by the School for Students, staff and parents.
- Staff are issued with the 'What to do if?' guide on E-Safety issues.

Appendix A

Keep safe: stop, think, before you click!
15 rules for responsible ICT use

The computer system is owned by the School. These rules will keep everyone safe and help us to be fair to others.

- I will only use the School's computers for Schoolwork and homework.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will keep my login and password secret.
- I will not bring files into School without permission.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the School.
- I will only email people I know, or my teacher has approved. Anonymous messages and chain letters are not permitted.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- The use of chat rooms is not allowed. I will never arrange to meet someone I have only ever previously met on the Internet.
- I will not communicate with staff on social networking sites such as 'Facebook'
- I will only email staff using my School email account
- If I use Twitter or other social networking sites I will never be derogatory to any member of staff or bring the School's name into disrepute.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher/responsible adult.

Student Signature: ..... Date: .....

Parent/ Carer name: …..... .....

Student name(s): ..... Form: .....

Appendix B

Acceptable Use Policy (AUP): Staff

Covers use of digital technologies in School: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the School's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Headteacher and Governing Body.
- I will only use the approved, secure email system(s) for any School business.
- I will keep my login and password secret
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Network Manager, Head of Department and e-safety Officer.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other School / LA systems.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I will ensure all documents are saved, accessed and deleted in accordance with the School's network security and confidentiality protocols.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the School's recommended system.
- I will not use personal digital cameras or camera phones for transferring images of Students or staff.
- I will use the School's Learning Platform in accordance with School's guidelines.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow School data security protocols when using any such data at any location.
- I understand that the Data Protection Policy requires that any information seen by me with regard to staff or Student information, held within the School's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.
- Use of the School's ICT resources for personal financial gain, gambling, political purposes or advertising (except School vacancies) is not permitted.

- I will not send e mails containing libelous, defamatory, offensive, racist or obscene remarks. If I receive an email of this nature I will notify the Network Manager and Deputy Headteacher (ICT).
- I will not forge or attempt to forge email messages.
- I will not send email messages using another person's account.
- I will not copy a message or attachment belonging to another user without permission from the originator.
- I will not disguise or attempt to disguise my identity when sending mail.
- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.
- I will not engage in any online activity that may compromise my professional responsibilities. This includes communicating with students on social networking sites such as 'Facebook'. If I use Twitter or other social networking sites:

    - I will never bring the School's name into disrepute.
    - I will never be derogatory to any member of staff
    - I will never engage knowingly with a pupil outside of school
    - I will retain a personal/professional boundary at all times
    - I will never post pictures of the children or refer to them at any time

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the School's most recent Acceptable Use Policy on an annual basis.

I agree to abide by the School's most recent Acceptable Use Policy.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the School's ICT resources and systems.

Signature …….…… Date ……

Full Name …….....(printed)

Job title . . . . . .

Authorised Signature: Deputy Headteacher/AHT/E-Safety Officer. I approve this user to be set-up.

Signature ……..... Date ……

Full Name ……..…(printed)

Appendix C **ICT**

As the parent or legal guardian of the above student(s), I grant permission for my daughter or son to have access to use the Internet, School VLE, email and other ICT facilities at School.

I know that my daughter or son has signed an e-safety agreement form and that they have a copy of the 15 'Rules for responsible ICT use'.

I accept that ultimately the School cannot be held responsible for the nature and content of material accessed through the Internet and mobile technologies, but I understand that the School will take every reasonable precaution to keep students safe and to prevent students from accessing inappropriate materials. These steps include using an educationally filtered service, restricted email access, employing appropriate teaching practice and teaching e-safety skills.

I understand that the School can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the School by promoting safe use of the Internet and digital technology at home and will inform the School if I have any concerns over my child's e-safety.

Parent /guardian signature: ..... Date: .....

Use of Digital Recording of images, Photography, Video & Audio

From time to time we take photographs or videos of students to use in displays in School, on our website and in publicity such as the local newspapers. We require your permission to do so and should be grateful if you would sign and return the whole form as soon as possible. Thank you.

This form is valid for the whole of your daughter's time at Bullers Wood School. Permission can only be rescinded in writing to the School.

I agree/do not agree* that photographs and videos can be taken, and acknowledge that copyright of such photography or videoing belongs to Bullers Wood School.

I agree/do not agree* that my daughter's name may be used in conjunction with the photograph/video.

Please state beside each of the following whether you give or refuse permission for any photographs or videos of the above named student to be used for that purpose:
*delete as appropriate

Displays	Yes/No *

Publications	Yes/No *
Publicity and promotions	Yes/No *
Electronic media or video e.g. School's Web site	Yes/No *

Parent /carer signature: ..... Date:.....

Appendix D

Guidance: What do we do if?

An inappropriate website is accessed <u>unintentionally</u> in School by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the Headteacher/e- safety Officer and decide whether to inform parents of any children who viewed the site.
3. Inform the School technicians and ensure the site is filtered

An inappropriate website is accessed <u>intentionally</u> by a child.

1 Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions with Guidance and Support Leader & Head of Department.
2 Notify the parents of the child.
3 Inform the School technicians and ensure the site is filtered.

An adult uses School IT equipment inappropriately.

1. Report the misuse immediately to the Headteacher / e-safety Officer and ensure that there is no further access to the PC or laptop.
2. If the material is offensive but not illegal, the Headteacher should then:
   - Remove the PC to a secure place.
   - Instigate an audit of all ICT equipment by the School's ICT managed service providers to ensure there is no risk of students accessing inappropriate materials in the School.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (contact Personnel/Human Resources).
   - Inform Governors of the incident.
3. In an extreme case where the material is of an illegal nature:
   - Contact the local police or High Tech Crime Unit and follow their advice.
   - If requested to remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of School time.

1 Advise the child not to respond to the message.
2 Refer to relevant policies including e-safety , Anti-bullying and PSHE and apply appropriate sanctions.
3 Secure and preserve any evidence.

4 Inform the sender's email service provider.
5 Notify parents of the children involved alongside the Guidance and Support Leader
6 Inform the police if necessary.

Malicious or threatening comments are posted on an Internet site about a Student or member of staff.

1. Inform Headteacher/e-safety Officer.
2. Secure and preserve any evidence.
3. Inform and request the comments be removed if the site is administered externally.
4. Endeavour to trace the origin and inform police as appropriate.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named Child Protection Safeguarding Officer in School and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Consider the involvement of police and social services.
4. Inform LA e-safety and Child Protection Safeguarding Officer.
5. Consider delivering a parent workshop for the School community.

All of the above incidences must be reported immediately to the Headteacher and e-safety Officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the Internet or mobile technology: they must be able to do this without fear. This can be done using Speak Out button on the student VLE