Brentford School for Girls

E-SAFETY & ACCEPTABLE USE POLICY

Rev	*Date*	*Description*
	September 2024	*Next review due*
4	*September 2023*	Reviewed
3	September 2022	Reviewed
2	September 2021	Reviewed
1	September 2019	Initial version

INTRODUCTION

Brentford School for Girls recognises the benefits that can be made to education through the use of Information and Communication Technology (ICT). Advances in ICT have brought about fresh challenges enabling us to learn in new and exciting ways. ICT offers us a means of carrying out tasks to a higher standard more efficiently and, in education, raising standards and streamlining educational administration.

E-Safety encompasses internet technologies and electronic communications such as mobile telephones and wireless technology. Use of the school's ICT equipment by any members of the school community must be in accordance with this policy. Any use which infringes this policy will be treated very seriously by the School Governing Body.

This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents/guardians and visitors) who have access to and are users of school IT systems, both in and out of school. The school will deal with cyber-bullying or other e-safety incidents covered within this policy and associated behaviour and anti-bullying policies and will inform parents/guardians of incidents of inappropriate e-safety behaviour that take place in or out of school.

AIMS

- To ensure safe and appropriate use of the internet and related communication technologies
- To use ICT to deliver the statutory requirements of the curriculum
- To use ICT to raise educational standards, to promote pupil achievement, to support the
- Professional work of staff and to enhance the school's management information systems
- To create an environment in which staff use ICT confidently in their work and students use their ICT skills confidently to enhance their learning.

ICT CONSIDERATIONS AND KCSIE 2023

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into four risk areas of risk:

- content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism

- contact: being subjected to harmful online interaction with other users; for example: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: online behaviour that increases the likelihood of, or causes, harm; for example, 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, and

- commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

The use of mobile phones is not permitted during the school day. (unless directed by staff in lessons i.e. EAL) (Please refer to the behaviour policy for the sanction related to this) students are allowed to access their mobile phones at the beginning and end of the school day.

FILTERS AND MONITORING

Regular monitoring takes place on an adhoc daily basis, using the schools Impero security systems unless there is a cause for concern. Regular checks are made with the Network Manager/ Assistant Headteacher on a weekly and half termly basis to review the effectiveness of these procedures and to keep up to date with evolving cyber-crime technologies.

The appropriateness of any filtering and monitoring systems are a matter for individual schools and will be informed in part by the risk assessment required by the Prevent Duty.

STAFF TRAINING

All staff receive regular updates via safeguarding bulletins and training which includes the understanding and the expectations , applicable roles and responsibilities in relation to filtering and monitoring. All staff are required to ensure that children are taught about safeguarding, including online safety. Staff are encouraged to ensure students are using online platforms safely through their teaching and pastoral duties.

LFGL (Undressed)

Schools should respond to all signs, reports and concerns of child – on –child sexual violence and sexual harassment, including those that have happened outside of the school premises and/or online. All staff working with children are advised to maintain an attitude of ‘it could happen here’ and this is especially important when considering child on child abuse.

INFORMATION AND SUPPORT

There is a wealth of information available to support schools and parents to keep children safe online. The following list is shared with staff, students and parents:

Organisation/Resource	**What it does/provides**
thinkuknow	NCACEOPs advice on online safety
disrepectnobody	Home office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
swgfl	Includes a template for setting out online safety policies
Internet matters	Help for parents on how to keep their children safe online
Parentzone	Help for parents on how to keep their children safe online
childnet cyberbullying	Guidance for schools on cyberbullying

pshe association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
educateagainsthate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation
The use of social media for online radicalisation	A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
UKCCIS	The UK council for Child Internet Safety's website provides; Sexting advice Online safety: questions for governing bodies Education for a connected world framework
NSPCC	NSPCC advice for schools and colleges
Net-aware	NSPCC advice for parents
Harmful online challenges and online hoaxes	Advice for preparing for any challenges and hoaxes, sharing info with parents and carers and where to get help and support
Commonsensemedia	Independent reviews ,age ratings, and other information about all types of media for children and parents
Searching ,screening and confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
lgfl	Advice and resources from the London Grid for Learning
Harmful online challenges and online hoaxes	Advice for preparing for any online challenges or hoaxes, sharing with parents and carers and where to get support

LEADERSHIP AND MANAGEMENT

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy through the Governors' Achievement, Progress and Pupil Welfare Committee. The day to day responsibility for e-safety lies with the Head of School (Pupil Support).

The IT Network Manager is responsible for ensuring that:

- The school's ICT infrastructure is secure and meets e-safety technical requirements
- The school's password policy is adhered to
- The school's Impero filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- The network team keeps up to date with e-safety technical information
- The use of the school's ICT infrastructure (network, remote access, e-mail, SharePoint, etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the Head of School for investigation/action/sanction. **RESPONSIBILITIES**

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.

- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The risk of being subject to radicalisation.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

• content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism

• contact: being subjected to harmful online interaction with other users; for example: 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: online behaviour that increases the likelihood of, or causes, harm; for example, 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

Education

Opportunities to teach safeguarding, including online safety, are discussed at paragraph 85-87. Resources that could support schools include:

Teaching online safety in school – DFE guidance how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.

• UKCIS has recently published its Education for a connected world framework. Online safety is a whole school and college issue. The framework aims to support the development of the curriculum and is of particular relevance to PSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond and to be central to a whole school approach to safeguarding and online safety. It covers early years through to age 18.

• The PSHE Association provides guidance to schools on developing their PSHE curriculum – www.pshe-association.org.uk

• Parent Zone and Google have developed Be Internet Legends a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils.

Filters and monitoring

Impero is used to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn and how often they access the IT system and the proportionality of costs vs risks.

Guidance on e-security is available from the National Education Network-NEN. Buying advice for schools is available here: buying for schools. And may be used if further advise is needed.

Whilst filtering and monitoring are an important part of the online safety picture in school, it is only one part. A whole school approach to online safety is in place and a clear policy on the use of mobile technology in Brentford School for Girls is in place, please see ICT policy. During lockdown it is the responsibility of parents/carers to monitor their daughters' online learning. This will not be the responsibility of the school due to students learning from home.

The filters and monitoring systems are in place, and do not "over block" or lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Reviewing online safety

Technology in this area evolves and changes rapidly. A free online safety self-review tool for schools can be found via the 360 safe website. UKCCIS have recently published Online safety in schools: Questions for the governing board

Staff training

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 81) including online safety which , amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring at induction and the requirement to ensure children are taught about safeguarding, including online safety (paragraph 85),and that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach in accordance with KCSIE 2023

Information and support

There is a wealth of information available to support schools, colleges and parents to keep children safe online. The following list is not exhaustive but should provide a useful starting point;

Organisation/Resource	**What it does/provides**
thinkuknow	NCA CEOPs advice on online safety
disrespectnobody	Home Office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
swgfl	Includes a template for setting out online safety policies
internet matters	Help for parents on how to keep their children safe online

parentzone	Help for parents on how to keep their children safe online
childnet cyberbullying	Guidance for schools on cyberbullying
pshe association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
educateagainsthate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
the use of social media for online radicalisation	A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
Harmful online challenges and online hoaxes	
UKCCIS	The UK Council for Child Internet Safety’s website provides: • Sexting advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
LGFL (undressed)	
NSPCC	NSPCC advice for schools and colleges
net-aware	NSPCC advice for parents
commonsensemedia	Independent reviews, age ratings, & other information about all types of media for children and their parents
searching screening and confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
lgfl	Advice and resources from the London Grid for Learning

The school should have a clear policy on the use of mobile or smart technology. Amongst other things this will reflect the fact that many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e,3G,4G and 5G)

This access means some children, whilst at school sexually harass their peers via their mobile and smart technology, share indecent images, consensually and non-consensually (often via large chat groups) and share pornography and other harmful content. Schools should carefully consider how this is managed on their premises and reflect this in their policies.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other school policies; specifically Anti-Bullying, Pupil Behaviour and Child Protection.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

Teaching & Support Staff

In addition to elements covered in the Staff Accessible Usage Policy (AUP), all teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters, including an understanding of filtering and monitoring in accordance with KCSIE 2023 and of the current school e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Usage Policy (AUP)
- The E-safety issues are embedded in all aspects of the curriculum and other school activities
- The students understand and follow the school's e-safety and acceptable usage policies
- The students have a good understanding of research skills and the need to avoid plagiarism and
- uphold copyright regulations
- They monitor ICT activity in lessons and extra-curricular activities
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Pupils

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Usage Policy, which they will be required to sign before being given access to school systems.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy also covers their actions out of school, if related to their membership of the school.

E mails

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately inform a member of staff if they receive an offensive e-mail.
- Pupils must not reveal any details of themselves or others such as address or telephone number, or arrange to meet anyone in any e-mail communication without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- E-mails sent to external organisations should be written carefully and authorised before sending in the same way as a letter written on school headed paper.
- Pupils should use the school e-mail system for work and educational purposes and NOT for personal chat or for social networking.

- When communicating with pupils and parents, staff should only use their school e-mail account.

Remote Learning

Parents/guardians play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents understand these issues. Parents and guardians will be responsible for:

- Parents/guardians will be required to read through and sign alongside their child's signature.
- Endorsing (by signature) the Pupil Acceptable Usage Policy.
- Accessing the school website in accordance with the relevant school Acceptable Usage Policy.
- Supporting the schools e-safety policy.
- During any online learning at home parents/guardians will be responsible for monitoring their daughter. This will not be the responsibility of the school.

MANAGEMENT OF INTERNET ACCESS

- The school ICT system capacity and security will be reviewed regularly asKCSIE 2023
- Virus protection will be installed and updated regularly.

Digital Images

- The school's record of parental permissions granted/not granted must be adhered to when taking images of our pupils.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Headteacher or the Network Manager.
- Where permission is granted the images should be transferred to school storage systems and deleted from privately owned equipment at the earliest opportunity.
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Social networking and personal publishing

- The school will block access to social networking sites for students unless being used for education purposes.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Staff and pupils must not place personal photos on any social network space without considering how the photo could be used now or in the future.
- Staff should be aware of the potential risk to their professional reputation by not adding pupils, parents or friends of pupils as 'friends' on their social network site and are strongly recommended not to do so.
- If inappropriate comments are placed on social networking sites about the school or school staff should be reported to the designated lead for CP and then advice would be sought from the relevant agencies, including the police if necessary.
- Pupils will be taught about e-safety on social networking sites as we accept some may use it outside of school.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The school has active website and twitter accounts which are used to inform, publicise school events and celebrate and share the achievement of students.

Websites

- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Staff will preview any recommended sites before use.
- “Open” searches (e.g. “find images/ information on...”) are discouraged when working with younger pupils who may misinterpret information.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff.
- **All** users must observe copyright of materials published on the Internet.
- Staff setting an internet task will regularly check what is being viewed by the pupils. Pupils are also aware that all internet use at school is tracked and logged.
- The school only allows the Network Manager and the Senior Management Team to access computer usage.

Copyright

- Pupils will be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations and staff will monitor this.
- Pupils are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- If using a search engine for images staff and pupils should open the selected image and go to it’s website to check for copyright.

Managing Filtering

- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- If staff or pupils discover unsuitable sites, the URL address and content must be reported to the Network Manager.
- ***Impero*** is used to monitor all activity, including anti-extremism and radicalisation.

Use of Own Equipment

- Privately owned ICT equipment should never be connected to the school’s network without the specific permission of the Head teacher or Network Manager.
- Pupils cannot bring their own removable data storage devices into school.
- Pupils should not bring in their own equipment unless asked to do so by a member of staff.
- Mobile phones are not permitted during the school day and should not be used in school, unless students are in the 6th form, then these can be used in the 6th form centre.

Use of School Equipment

- No personally owned applications or software packages should be installed on to school ICT equipment;
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- All staff should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Passwords

- Passwords or encryption keys should not be recorded on paper or in an unprotected file.
- Passwords should be changed at least every 3 months.

- Users should not use the same password on multiple systems or attempt to “synchronise” passwords across systems
- Pupils should only let school staff know their in-school passwords.
- Pupils must inform staff immediately if passwords are traced or forgotten. Pupils must see a member of the Network Team to have their password reset.

EDUCATION AND TRAINING

PUPILS

- E-safety education is provided as part of PSHCE and is regularly revisited across the curriculum and through tutor time.
- Pupils are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Pupils are helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in school.
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

STAFF

- The Assistant Headteacher responsible for IT in school, will ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy, including online safety as well as an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring, and ensure an understanding of the Acceptable Usage and Child Protection Policies.
- Staff who require additional training can refer to the Child Exploitation and Online Protection (CEOP) website and if further training is required they can speak to their line manager or the Deputy Head (Resources & Community).

MONITORING

All use of the school’s Internet access is logged and the logs are randomly but regularly monitored by ***Impero***, the school’s external provider. Whenever any inappropriate use is detected it will be followed up by the Network Manager with the support of the Designated Safeguarding lead (DSL).

Any e-safety incidents must be reported immediately to the Headteacher (if a member of staff) or Head of School (if a pupil) who will investigate further following e-safety and safeguarding policies and guidance.

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. Listed in Appendix 2 are the responses that will be made to any apparent or actual incidents of misuse. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures (Appendix 3).

REVIEW AND EVALUATION

The E-Safety and ICT Acceptable Use Policy will be reviewed annually, to see if any amendments need to be made, this will be done by the Assistant Headteacher, responsible for IT in school and in conjunction with the ICT Strategy Group. If no amendments need to be discussed with Governors then no further action will be taken until the end of the three year cycle as per the front cover, where it will be discussed with the Governors' Pupils' Committee. (KCSIE 2021- School will consider carrying out an annual review of their approach to on line safety, supported by an annual risk assessment that considers and reflects the risks their children face)

APPENDIX 1

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

		Staff and other adults				Students and young people			
Communication Technologies		Permitted	Permitted at certain times	Not Permitted		Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones May be brought to school		✓					✓		
Mobile phones used in lessons				✓					✓ (unless agreed by teacher in lesson i.e. EAL)
Use of mobile phones in social time		✓							✓
Taking photographs on mobile devices				✓					✓
Use of tablets and other educational mobile devices		✓							✓
Use of school email for personal emails				✓					✓
Social use of chat rooms/facilities				✓					✓
Use of social network sites for educational purposes		✓						✓	
Use of educational blogs		✓			✓				

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person (in accordance with the school policy) the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email, chat, Learning Platform etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

APPENDIX 2

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage such that users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					✓
Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
Adult material that potentially breaches the Obscene Publications Act in the UK					✓
Criminally racist material in the UK					✓
Pornography					✓
Promotion of any kind of discrimination				✓	
Promotion of racial or religious hatred					✓
Threatening behaviour, including promotion of physical violence or mental harm					✓
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✓	

On-line gaming (educational)		✓			
On-line gaming (non-educational)/gambling				✓	
On-line shopping / commerce			✓		
File sharing			✓		
Use of social networking sites			✓		
Downloading video broadcasting e.g. YouTube	✓				
Uploading to video broadcast e.g. YouTube			✓		

APPENDIX 3

The guidance in this policy should be implemented with cross reference to the School's Child Protection, Anti-Bullying and Behaviour Policies. Note, attempts have been made to synchronise guidance and sanctions.

Incident involving students	Teacher to use school behaviour policy to deal with	Refer to Head of Year	Refer to Acting Deputy Headteacher who will refer to the police	Refer to Network Manager for action re security/filtering etc.
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/Inappropriate activities or refer to the safeguarding policy).		✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓			✓
Unauthorised use of mobile phone/ digital camera/ other handheld device		✓		
Unauthorised use of social networking/ instant messaging/ personal email	✓	✓		✓
Unauthorised downloading or uploading of files		✓		✓
Allowing others to access school network by sharing username and passwords		✓		✓
Attempting to access or accessing the school network, using another student's account or creating a fake account for pupils		✓		✓
Attempting to access or accessing the school network, using the account of a member of staff or creating a fake account for staff		✓		✓
Corrupting or destroying the data of other users		✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓		✓
Continued infringements of the above, following previous warnings or sanctions		✓	Community Police Officer referral	✓

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓	SLTP	✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓		✓

APPENDIX 4

Acceptable Use Policy (AUP): Staff Agreement Form

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 personal use deemed 'reasonable' by the Headteacher and Governing Body.
- I will not reveal my password(s) to anyone other than ICT Support staff if necessary.
- I will change my password on a regular basis as requested, as stated in the policy. I will use a strong password of random phrases with 12 characters minimum, including a capital letter, number or sign.
- If leaving the computer unattended I will lock the computer to prevent unauthorised access.
- I will not allow unauthorised individuals to access email/Internet/intranet/network, or other school/LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data protection policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business, (which is currently: Microsoft Outlook, GMail)
- I will only use the approved school email, school MLE or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- 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 E-Safety Officer Katie Coleman).
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network/Internet that is not encrypted and up-to-date with anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will use the school's Learning Platform in accordance with school advice.
- 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 agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- 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 Schools Data protection policy requires that any information seen by me with regard to staff or pupil 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 embed the school's e-safety curriculum into my teaching.
- I will only use school or external agency systems in accordance with any corporate policies.
- 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 understand that failure to comply with this agreement could lead to disciplinary action.

- I agree that the use of computers is monitored for the protection of both others and myself and that my internet usage will be checked from time to time.
- I will not access any information via the internet or store information that promotes radicalisation or extremist behaviours.

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 e-safety policies.

I agree to abide by all the points above.

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:
I approve this user to be set-up.

Signature ……................ Date……………………………….

Assistant Headteacher

FAILURE TO ADHERE TO THE ICT ACCEPTABLE USAGE POLICY MAY LEAD TO DISCIPLINARY ACTION.

Appendix 5

PUPIL ACCEPTABLE USER AGREEMENT

These rules will keep everyone safe and help us to be fair to others;

- I will only use the school's computers for schoolwork, homework and as directed;
- I will not bring files into school (on removable media or online) without permission or upload inappropriate material to my workspace;
- I will only edit or delete my own files and not view, or change, other people's files without their permission;
- I will keep my logins, IDs and passwords secret and will change them when requested;
- I will use the Internet responsibly and will not visit web sites I know to be banned by the school. I am also aware that during lessons I should visit web sites that are appropriate for my studies;
- I will only e-mail people I know, or those approved by my teachers;
- The messages I send, or information I upload, will always be polite and sensible;
- I will not open attachments, or download a file, unless I have permission or I know and trust the person that has sent them;
- I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission;

- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me;
- 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 save it and talk to a teacher / trusted adult;
- I am aware that some websites and social networks have age restrictions and I should respect this;
- I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk;
- I will respect that others need to use the computers. I will log off when I have finished using them and not interfere with their proper operation;
- I agree that the use of computers is monitored for the protection of both others and myself and that my internet usage will be checked from time to time.
- I will not access any information via the internet or store information that promotes radicalisation or extremist behaviours.
- I will not access social media during school hours or on school equipment.
- I am aware that my online activity is accessible to parents/carers if requested
- I will not use a teacher or another students account and or falsely set up an account

I have read and understand these rules and agree to them.

Name: …………………………….……………………………….. (Please PRINT name)

Signed: ……………………………………………………………….. Form…………………………….….Date…………………..