E-SAFETY POLICY

Introduction
This policy applies to the Queen Ethelburga's Collegiate - Queen's Kindergarten, Chapter House Preparatory School, King's Magna Middle School, Queen Ethelburga's College and The Faculty of Queen Ethelburga's - hereafter referred to as "the Collegiate".

The E-safety Policy applies to all members of the Collegiate community who have access to, and are users of, Collegiate ICT systems both in and out of school, together with use of mobile electronic devices. The policy applies to any use which affects the welfare of other members of the Collegiate community or where the culture or reputation of the Collegiate are put at risk. This includes any misuse of the internet or social media.

The staff and student Acceptable Use Policies (AUPs) are central to the E-safety Policy and should be consulted alongside this policy. The E-safety Policy will be reviewed annually by the E-safety Committee who will provide recommendations for updating the policy in the light of experience and changes in legislation or technologies. The Student Council will be consulted regarding any changes to the Student AUP and the Staff body regarding any changes to the Staff AUP.

Aim
The Collegiate is committed to safeguarding the welfare of all students and recognises that an effective e-safety strategy is paramount to this. The aim of this policy is to ensure a safe, beneficial and acceptable environment for all students and staff using the extensive ICT facilities provided by the Collegiate and, together with the AUPs, to:

- safeguard and promote the welfare of students, in particular by anticipating and preventing the risks arising from:
    - exposure to inappropriate material (such as pornographic, racist, extremist or offensive materials);
    - the sharing of personal data, including images and sexting;
    - inappropriate online contact; and
    - cyberbullying and other forms of abuse;
- to minimise the risk of harm to the assets and reputation of the Collegiate;
- to minimise excessive use of their devices;
- to help students take responsibility for their own ICT safety (i.e. limiting the risks that children and young people are exposed to when using ICT);
- to ensure that students use ICT safely and securely and are aware of both external and peer to peer risks when using ICT;
- to prevent the unnecessary criminalisation of students.

Teaching and Learning
Internet use is part of the curriculum and a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction. Students use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their

own safety and security. E-safety is a focus in all areas of the curriculum and key e-safety messages are reinforced regularly, teaching students about the risks of internet use, how to protect themselves and their peers from potential risks, how to recognise suspicious, bullying or extremist behaviour and the consequences of negative online behaviour.

Staff should be vigilant in lessons where students use the internet. If staff allow the use of mobile devices in their lessons, they must ensure that they are used in line with Collegiate policy. Staff will be provided with sufficient e-safety training to protect students and themselves from online risks and to deal appropriately with e-safety incidents when they occur. Ongoing staff development training includes training on online safety together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements.

The Collegiate's Internet access is designed to enhance and extend education. Students will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use. The Collegiate will ensure that staff are aware of copyright law regarding the copying and subsequent use of Internet derived materials. Access levels reflect the curriculum requirements and age of students.

Staff should guide students to on-line activities that will support the learning outcomes planned for the students' age and maturity. Students are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy (for example, valid research about the Holocaust is likely to find information about Holocaust denial). The evaluation of on-line materials is a part of teaching/learning in every subject.

Internet use
The internet is a powerful tool which opens up new opportunities for students and staff. They can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Students are given clear guidelines for what internet and email use is acceptable through the AUP and in lessons which use such technologies, as part of the curriculum in Personal Development (PSHE), General Studies and ICT lessons, and in special presentations. Key e-safety messages are also reinforced in assemblies and form activities. Where appropriate, students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Management of website content
The Principal takes overall editorial responsibility and ensures that content is accurate and appropriate.

QENET Wi-Fi and personal dongles
Students and staff may not use dongles purchased from mobile phone providers.

Mobile Devices cannot be used as hotspots. QENET is the only authorised WIFI network. Mobile Devices must not be used at inappropriate times or to access inappropriate material for the time of day, for example social networking sites or personal e-mail during prep).

Failure to follow these guidelines will lead to a minimum sanction of confiscation of the device, although repeated breaches of this policy will lead to the student being prohibited from using any device which has been used inappropriately.

Mobile electronic devices (phones, laptops, i-pads and tablets)

Mobile telephones are permitted both in boarding houses and in academic school. During the school day phones are only to be used by students during break time and lunch time, unless in the boarding houses (see below). Head phones must not be used while moving around the grounds.

Chapter House students are only allowed to have mobile electronic devices in school with advance permission from parents. All devices will be kept in a secure place by the form teacher during the day and handed back to the students at the end of the day. No mobile phones are to be used in the EYFS setting. (See Child Protection policy).

In school, mobile phones should be turned off and kept in a bag or pocket during lessons (i.e. not visible and silent) unless permission has been given by the classroom teacher. In the event of a mobile phone being used in a lesson without permission from the teacher, the phone should be confiscated and given to the Pastoral Team when in the main school building or the Wimbledon Centre, the Faculty Team in Genesis or the Head of Department in Woodlands.

In boarding, mobile phones are permitted during free time, although their use is prohibited after lights out. Phones are collected in from younger students (up to Year 8) and this provision can be extended to students who persistently use their phones at inappropriate times. Further guidelines for mobile phones can be found in boarding policies.

Mobile devices must not be used to directly take photographs, video or sound clips of any person who is unaware of the action and who has not given their permission. Students and staff are informed about the statutory framework regarding the sharing and publishing of photographs and videos, regardless of the media chosen. Staff must adhere to the Child Protection Policy and Staff Code of Conduct.

Any use of mobile technology to intimidate, bully, harass, threaten or attempt to radicalise others or breach copyright laws will be counted as an infringement of network use and breach of discipline and will be dealt with in accordance with the Collegiate's behaviour and discipline policies. This may result in disconnection from the network, confiscation of the mobile technology and/or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission and if in doing so, Collegiate and statutory guidelines are not breached.

Students are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the Collegiate and may constitute a criminal offence. The Collegiate will treat incidences of sexting (both sending and receiving) as a safeguarding issue and students concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

The Collegiate has the right to confiscate and search any mobile electronic device if it suspects that a student or staff member is in danger or has misused a device. This will be done in accordance with the Collegiate's policy on searching and confiscation as set out in the Behaviour and Discipline Policy.

Cyberbullying

Cyberbullying is the use of ICT, particularly mobile electronic devices and the internet, deliberately to upset someone else. Cyberbullying (along with all forms of bullying) will not be tolerated and incidents of cyberbullying should be reported and will be dealt with in accordance with the Collegiate's Anti-Bullying Policy. Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

Students should remember the following:

- Always respect others - be careful what you say online and what images you send.
- Think before you send - whatever you send can be made public very quickly and could stay online forever.
- Don't retaliate or reply online.
- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the Collegiate to investigate the matter.
- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly.
- Don't do nothing - if you see cyberbullying going on, support the victim and report the bullying.

The Collegiate has clear procedures in place to support anyone affected by cyberbullying and if a student thinks that they, or another person, is being bullied, they should talk to a teacher or any trusted adult about it as soon as possible. The following websites are useful resources for advice on internet use:

http://www.saferinternet.org.uk/

http://www.kidsmart.org.uk

http://www.safetynetkids.org.uk/

http://www.safekids.com/

http://www.thinkuknow.co.uk

The Leadership Team and staff will monitor the usage of shared areas of the intranet by students and staff regularly in all areas, in particular message and communication tools and publishing facilities. Students and staff will be advised on acceptable conduct and use when using the shared areas of the intranet. Only members of the current student, parent/carers and staff community will have access to the shared areas of the intranet. When staff, students and other users leave the Collegiate their account or rights to specific school areas will be disabled.

Any concerns with content may be recorded and dealt with as follows:

- Confiscation and searching the device in accordance with the procedures in the Collegiate's Behaviour and Discipline Policy.
- The user will be asked to remove any material deemed to be inappropriate or offensive.
- In some cases the material may have to be removed by the site administrator, the Designated Safeguarding Lead or external agencies.
- Viruses may be wiped from software on student and staff devices by the Head of IT.
- Access to shared areas of the intranet for the user may be suspended.
- The user will need to discuss the issues with a member of the Leadership Team before reinstatement.
- A student's parent/carer may be informed.
- Sanctions will be applied appropriate to the offence in line with the Collegiate's Behaviour and Discipline Policy.

- Staff concerns will be reported to the Principal following the referral process outlined in the Whistleblowing Policy. More information can be found in the Staff Code of Conduct and staff Acceptable Use Policy.

If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the Collegiate's child protection procedures (see the Collegiate's Child Protection Policy).

Guidance for parents
The role of parents in ensuring that students understand how to stay safe online is crucial. The Collegiate expects parents to promote e-safety and to:

- support the Collegiate in the implementation of this policy and report any concerns in line with the Collegiate's policies and procedures;
- talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and
- encourage their child to speak to someone if they are being bullied or need support.

The online resources above provide useful information together with the DfE guidance Advice for Parents and Carers on Cyberbullying. Parents and Guardians should take note of any guidance on radicalisation given by North Yorkshire Safeguarding Children Board.

If parents have any concerns or require any information about online safety, they should contact the Head of Pastoral Care.

Visitors Access

Visitors are able to access the schools WIFI on request with a visitor password and username. This provides limited access to the network and would run through 'Smoothwall' the schools filter to allow the school to monitor any inappropriate use.

Policy Decisions
The Collegiate maintains a current record of all staff and students who are granted access to the Collegiate's electronic communications. All staff, parent/guardians and students must sign that they have read and understand the relevant AUP before using any Collegiate ICT resource.

The Collegiate will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a Collegiate computer.

If students access inappropriate material from their personal devices the Collegiate takes no responsibility. This action can, however, be subject to investigation and sanction in line with Collegiate policy. Students can report any incident of misuse or concern to any member of staff they trust. The Collegiate also has an online virtual bully box which students can report bullying and attach any relevant information.

Any user who accidentally comes across inappropriate or offensive material should do the following:

1. Inform the Collegiate's Child Protection Team of the incident and give the website address. (This must be handwritten, not sent as an e-mail or forwarded).
2. Ask the Child Protection Team to log the web address, time and username.

3. The Child Protection Team will initiate an investigation. The categorisation of the material will be checked.
4. The outcome of the investigation will be relayed back to the e-safety committee and logged.
5. Incidents will be reviewed by the e-safety committee at each meeting.

In the event of accidental access to illegal material:

1. Inform the Collegiate's Child Protection Team of the incident and give the website address (this must be handwritten, not sent as an e-mail or forwarded).
2. Do not show anyone the content or make public the URL
3. Make sure a reference is made of the incident.
4. The Child Protection Team may then go to the IWF website at www.iwf.org.uk and click the report
5. If reporting a URL do not use copy and paste, type the URL. In the event of unsolicited illegal material received by e-mail, the Child Protection Team should report to Easynet on abuse@uk.easynet.net or contact the Easynet helpdesk on: 0845 333 4568.

Any person suspecting another of deliberate misuse or abuse of technology should take the following action:

1. Report in confidence to the Collegiate's Child Protection Team.
2. If the misuse is by a member of staff this should be reported to the Principal.
3. The Head of Pastoral Care should investigate the incident.
4. If this investigation results in confirmation of access to illegal material, the committing of illegal acts, or transgression of collegiate rules, appropriate sanction will be enforced.
5. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the CEOP or the police will be informed.
6. No student or member of staff should attempt to access or view the material, whether online or stored on internal or external storage devices. If this step is necessary, CEOP and/or police will be contacted.

The school audits ICT use annually to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate. Methods to identify, assess and minimise risks will be reviewed every term and following any major incident. Complaints of Internet misuse, including the misuse of social media, will be dealt with under the relevant complaints procedure. Any complaint about staff misuse must be referred to the Principal. All e–Safety complaints and incidents will be recorded by the Head of Pastoral Care or E-safety coordinator, including any actions taken. Any issues (including sanctions) will be dealt with according to the Collegiate's disciplinary and child protection procedures.

The e-safety committee will consult with the student council to discuss issues and any concerns or ideas the students may have. The Collegiate will endeavour to draw from the whole Collegiate community, although this may require questionnaires rather than meetings with parents due to the distance most parents live from the school.

Responsibilities

The Collegiate Board are responsible for the approval of the e-safety policy and reviewing its effectiveness. The Collegiate Board will undertake an annual review of the Collegiate's safeguarding procedures and their implementation, which will include consideration of how students may be taught about safeguarding, including online safety, through the Collegiate's curricular provision, ensuring relevance, breadth and progression.

The Principal is responsible for ensuring the safety (including e-safety) of members of the collegiate community, though the day to day responsibility will be delegated to members of the e-safety committee which consists of:

Chair of the Collegiate Board - Amy Martin
Chair/Head of Pastoral Care – Erica Papaglimis
SLT/Deputy Head of College - Lauren Blakeley
Head of IT - Dave Millington
SLT/ Head of Chapter House - Karen Kilkenny
SLT/Deputy Head of Boarding/Assistant Head of Pastoral Care - Tracy Holt
SLT/Deputy Head of Boarding - Mike Dawson
SLT/Head of Teaching and Learning - Vic Adams
Pastoral Coordinator i/c Focus Weeks - Helen Weeds
Assistant Head of Pastoral Care Welfare - Rebecca Thackray
Personal Development - Victoria Allen
Chapter House Representative - Damien Campbell

The e-safety coordinator organises regular meetings of the e-safety committee and reports to the Strategic Leadership Team. The e-safety committee takes day to day responsibility for e-safety issues in school and out of school hours. The team consists of members of the Collegiate Board, Strategic Leadership Team, Senior Leadership Team, IT Team, Safeguarding and Welfare teams and a representative from Teaching and Learning. The minutes from the esafety minutes are sent to the Student Council meetings for their input and support. Meeting minutes are maintained to inform future e-safety.

The Network Manager is responsible for ensuring that the Collegiate's ICT infrastructure is secure and that users may only access the Collegiate's networks through a username and password. Servers, wireless systems and cabling are securely located and physical access is restricted. The school Local Area Network (LAN) is protected by an active firewall. In addition to this there is a web filter (Smoothwall) that dictates the level of access given to the internet and is operated to ensure that students are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the Collegiate's network. Smoothwall reports are sent daily to the Network Manager and Safeguarding Team and acted on in line with the safeguarding and acceptable use policies. Https traffic will be decrypted and inspected as part of our filtering process using Smoothwall software.

Careful consideration is also given to the use of 3G and 4G connection on site and the use of hotspots (further information is provided in the policy and the acceptable use policies). The Collegiate aims to educate students in the safe use of the internet and social media and continually offers guidance and support. If the Collegiate suspects that a student is accessing inappropriate material through their own 3G or 4G network, then all devices are confiscated and searches carried out in line with the Collegiate's Behaviour and Discipline Policy.

There is restricted wireless access to the school LAN. The Wide Area Network (WAN) is managed off-site and security is ensured through a separate VLAN, with virus protection updated daily. The Collegiate Sharepoint site enables users to access relevant file storage areas, as well as enabling users to report online issues electronically. Students are not allowed to download executable files and workstations are secured against user mistakes and deliberate actions. The Network Manager monitors the use of the internet and email of all users, reporting any misuse to the e-safety committee.

Virtual Private Networks

The use of VPN's is not permitted by staff or student and this is reflected in the Acceptable Use Policies. Any use of a is dealt with in line with the Collegiate intervention and sanctions systems.

Teaching and support staff must accept and comply with the Staff AUP which is detailed in the Staff Handbook and must report any suspected misuse as detailed above. New members of staff receive e-safety training as part of their induction programme and all members of staff are kept up to date with e-safety issues though INSET and staff briefings. Digital communications with students should be on a professional level and only through their Collegiate e-mail account. Teaching staff are responsible for monitoring ICT activity in lessons, and in extracurricular and extended school activities. They should provide the necessary support for students and embed internet safety messages within lessons as appropriate. Students are taught as part of SMSC to use ICT and the internet safely and we aim to build resilience in students and develop their ability to protect themselves online and make the right choices. Students also receive support as part of THRIVE@QE. Staff must be aware of e-safety issues related to the use of mobile phones, cameras and other hand held devices, and ensure they are used according to policy. All members of staff are expected to maintain an appropriate level of professional conduct in their own internet use, including the use of social media, both within and outside school. Any complaint about staff misuse must be referred to the Principal.

Collegiate i-pads will only be distributed once the member of staff has read, and signed, the staff acceptable use policy. I-pads can be checked at any time by the e-safety committee and supporting safeguarding staff. Staff should not use school iPad's or electronic devices to conduct personal business/enterprise which would lead to personal gain. Information such as media, photos, files and any other personal information must not be accessed or stored on the device. Staff are welcome to use their own devices for personal use, in line with collegiate e-safety policy, but may not allow students to access staff members' personal devices at any time.

The Child Protection Team and e-safety committee are responsible for keeping up to date with e-safety issues in the use of internet and related technologies, and how these relate to children and young people.

Students are responsible for using the collegiate ICT systems in accordance with the Student AUP, which parents must sign online before students are given access to Collegiate systems. Students are taken through the AUP in assembly and sign this in their planners in Personal Development lessons and General Studies where the AUP is discussed further. They must have a good understanding of research skills and the need to avoid plagiarism, as well as understanding the importance of reporting abuse, misuse or access to inappropriate materials. The AUP makes it clear that failure to comply with its terms may lead to withdrawal of access, close monitoring of network activity, investigation into past network activity or, in more serious cases, criminal prosecution.

Parents or guardians indicate their support for the e-safety Policy by endorsing the Student AUP through the Parent Portal and by signing the e-safety policy online. The Collegiate helps parents to understand e-safety issues through presentations and information made available on the website.

Risk assessment is in place and regularly reviewed with regards to CCTV, mobile phones and camera usage (See Child Protection Policy and CCTV Policy). ***Visitors and parents*** are asked not to post photographs of other people's children on social media sites without the express permission of those children's parents.

Personal data is managed in line with Collegiate's Data Protection Policy which gives further details about the management, storage and release of personal data in line with the Data Protection Act.

Related Policies

The staff and student Acceptable Use Policies (AUPs)
Child Protection Policy
Anti-bullying Policy
Staff Code of Conduct
Behaviour and Discipline Policy
Data Protection Policy
Esafety Committee Remit

Updated EPA – October 2015
Reviewed October 2015 SJa
Review due June 2015. Reviewed October 2015 EPA/JHa.
To be reviewed by August 2016
Reviewed June 2016 EPA
To be reviewed June 2017
Reviewed July 2016 EPA
To be reviewed July 2017
Reviewed September 2016 EPA
To be reviewed September 2017

Student Acceptable Use Policy (AUP)

E Ensure that I do not create, send or post anything which is offensive to other people or brings the school into disrepute. I will not use any language or images which could offend any minority group. I understand that sending or receiving inappropriate images, including sexting, via social media or private message is criminal activity and must be reported immediately.

S Secure all my passwords and not share them with others. I understand I must not reveal or use anyone else's login details or access a device someone else is logged onto. I will change my password immediately if it becomes known to someone else and ensure I log out after every network session.

A Access only appropriate material. I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that school can monitor my use of the internet if any poor conduct is suspected. I will report any accidental access to other people's information, unsuitable websites or receipt of any inappropriate material as well as any security risk or suspicious behaviour that I become aware of. Offensive materials includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity.

F Facebook, social media and email use. I will not publish my own and others' personal details, information or location over any social networking site. I am aware that email is not guaranteed to be private. Messages or any communication via social media or email supporting illegal activities will be reported to the authorities.

E Exercise caution when downloading material. I understand that the illegal download and/or copyright of any material, including receiving, sending or publishing, is forbidden and may be passed to the relevant authorities. I will not download any unapproved software, system utilities or resources from the internet.

T Turn off mobile hot spots and not use the network in any way that will disrupt its use for other people. This includes any attempt to harm, destroy or remove any equipment, work of another user, or website connected to the system. The use of VPN's (Virtual Private Networks) are not allowed under any circumstances.

Y Your device, your responsibility. I understand that the Collegiate has the right to confiscate and search any device if it suspects that a student is in danger or has misused a device or the school network. I understand that any activity from a device I own is my responsibility, including all portable devices and their content or viruses. Devices which have detected viruses on them will have to be handed over to the IT department to have the virus cleared.

Student Acceptable Use Policy

All students must follow the rules outlined in this policy when using Collegiate ICT resources and equipment, including all internet access and the Virtual Learning Environment (VLE), accessed from both in and outside of school, and their own mobile devices and electronic equipment. Breaking these conditions may lead to: **confiscation of any electronic devices, close monitoring of the student's network activity, investigation of the student's past network activity, withdrawal of the student's access and, in some cases, permanent removal from the Collegiate and even criminal prosecution.** Misuse of the internet will be dealt with in accordance with the Collegiate's Behaviour and Discipline Policy and, where there is a safeguarding risk, the Child Protection and Safeguarding Policy.

The Collegiate is not responsible for any loss of data on the network, computers connected to the network or data storage used on the network (including USB memory sticks). Data held on the network will be backed up for a limited period. Students are responsible for backups of any other data held. Use of any information obtained via the network is at the student's own risk.

Student access to networked resources is a privilege, not a right. Students will be expected to use the resources for the educational purposes for which they are provided.

Students are expected to use the network systems in a responsible manner. It is not possible to compile a complete set of rules about what is, and what is not, acceptable however the above should be a guide and in cases of dispute, the decision of Principal will be final.

Student agreement:

I agree to follow the Collegiate rules on the use of Collegiate network resources and mobile electronic devices. I will use the network and all mobile electronic devices in a responsible way and observe all of the conditions explained in both the E-Safety Policy and this Acceptable Use Policy. I understand and accept the consequences of breaking these rules.

Print student name……

Student Signature…….Date……..

Parent/Guardian agreement:

I understand that my child has agreed to accept the terms of the E-safety and Student AUP Policy and I confirm that I accept the terms of the agreement.

I have read and understood the E-Safety Policy and agree to check any updates which are made available on the Parent Portal.

Print Parent/Guardian name……..

Parent/Guardian Signature…… Date…….

Queen Ethelburga's Collegiate

Chapter House Student Acceptable Use Policy

All students must follow the conditions described in this policy when using school ICT networked resources including: Internet access, the school Virtual Learning Environment (VLE) both in and outside of school.

Breaking these conditions may lead to:

- Withdrawal of the student's access,
- Close monitoring of the student's network activity,
- Investigation of the student's past network activity,
- In some cases, criminal prosecution.

Students will be provided with guidance by staff in the use of the resources available through the schools network. School staff will regularly monitor the network to make sure that it is being used responsibly.

The school will not be responsible for any loss of data as a result of the system or student mistakes in using the system. Use of any information obtained via the network is at the student's own risk.

Conditions of Use

Student access to the networked resources is a privilege, not a right. Students will be expected to use the resources for the educational purposes for which they are provided.

It is the personal responsibility of every student to take all reasonable steps to make sure they follow the conditions set out in this Policy. Students must also accept personal responsibility for reporting any misuse of the network to the relevant Head of Year.

Acceptable Use

Students are expected to use the network systems in a responsible manner. It is not possible to compile a complete set of rules about what is, and what is not, acceptable. All use however should be consistent with the spirit of the school Code of Conduct. The following list does provide some examples that must be followed:

1	I will not create, send or post any material that is likely to cause offence or needless anxiety to other people or bring the school into disrepute. Remember: "What goes on the internet stays on the internet".
2	I will use appropriate language at all times.
3	I will not use language that could stir up hatred against any ethnic, religious or other minority group.
4	I understand work saved on the school network can be checked by staff.
5	I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network.
6	I will not trespass into other users' files or folders.
7	I will not share my login details (including passwords) with anyone else. Likewise, I will never use other people's username and password.

8	I will ensure that I log off after my network session has finished.
9	I will not attempt to visit websites that might be considered inappropriate or illegal.
10	I will not download and/or install any software.
11	I understand that breaking these rules will result in removal of access to internet or computers.

Key Stage 1 Student User Agreement Form for the Student Acceptable Use Policy

I agree to follow the school rules on the use of the school computers and only go on websites my teacher tells me to go on.
If I do not follow the rules, I understand that this may result in me not being allowed to use the computers or internet within school.

Student Name: _____

Key Stage 2 Student User Agreement Form for the Student Acceptable Use Policy

I agree to follow the school rules on the use of the school network resources. I will use the network in a responsible way and observe all the conditions explained in the school acceptable use policy in the spirit of the school code of conduct.
I agree to report any misuse of the network to my class teacher.
I also agree to report any websites that are available on the school Internet that contain inappropriate material to my class teacher.
If I do not follow the rules, I understand that this may result in me not being allowed to use the computers or internet within school.

Student Name: _____

Chapter House Parent/Guardian Agreement Form for the Student Acceptable Use Policy

Copy of Key Stage 1 Student Agreement

I agree to follow the school rules on the use of the school computers and only go on websites my teacher tells me to go on.

If I do not follow the rules, I understand that this may result in me not being allowed to use the computers or internet within school.

Copy of Key Stage 2 Student Agreement

I agree to follow the school rules on the use of the school network resources. I will use the network in a responsible way and observe all the conditions explained in the school acceptable use policy in the spirit of the school code of conduct.

I agree to report any misuse of the network to my class teacher.

I also agree to report any websites that are available on the school Internet that contain inappropriate material to my class teacher.

If I do not follow the rules, I understand that this may result in me not being allowed to use the computers or internet within school.

Parent/Guardian Agreement

I understand that my son/daughter has agreed to accept the terms of the Student AUP and I confirm that I accept the terms of the agreement.

Parent / Guardian's Name: _____

Date: __/__ /_____