ROBERTSBRIDGE

COMMUNITY COLLEGE

E-Safety Policy

Co-ordinator – Business Manager

Updated – November 2016

Ratified by Governors – November 2016

Review Date – November 2017

INTRODUCTION

1.1. The Byron Review "Safer Children in a Digital World" stressed the role of colleges:
"One of the strongest messages I have received during my Review was about the role that colleges and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Colleges and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."

1.2. The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in colleges in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Colleges have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, colleges must, through their e-Safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside College. The policy will also form part of the College's protection from legal challenge, relating to the use of ICT.

BACKGROUND / RATIONALE

1.3. New technologies have become integral to the lives of children and young people in today's society, both within Robertsbridge Community College and in their lives outside College.

1.4. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

1.5. The requirement to ensure that young people are able to use the internet and related communications technologies appropriately and safely, is addressed as part of the wider duty of care to which all who work in Robertsbridge Community College, are bound. Robertsbridge Community College e-Safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

1.6. The use of these exciting and innovative tools in Robertsbridge Community College and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the College. Some of the dangers they may face include:

a. Access to illegal, harmful or inappropriate images or other content
b. Unauthorized access to / loss of / sharing of personal information
c. The risk of being subject to grooming by those with whom they make contact on the internet.
d. The sharing / distribution of personal images without an individual's consent or knowledge
e. Inappropriate communication / contact with others, including strangers
f. Cyber-bullying
g. Access to unsuitable video / internet games
h. An inability to evaluate the quality, accuracy and relevance of information on the internet
i. Plagiarism and copyright infringement
j. Illegal downloading of music or video files
k. The potential for excessive use which may impact on the social and emotional development and learning of the young person.

1.7. Many of these risks reflect situations in the off-line world and it is essential that this e-Safety policy is used in conjunction with other Robertsbridge Community College policies (eg behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' 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.

1.8. The College must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

DEVELOPMENT / MONITORING / REVIEW OF THIS POLICY

1.9. This E-Safety policy has been developed by the E-Safety committee made up of:

a. Robertsbridge Community College E-Safety Coordinator David Evans
b. Senior Leaders
c. Teachers
d. Support Staff
e. ICT Technical staff

1.10. Consultation with the whole Robertsbridge Community College community has taken place through the following:

a. Staff meetings
b. Robertsbridge Community College / Student Council
c. INSET Day
d. Governors meeting
e. Parents evening
f. Robertsbridge Community College website / newsletters

SCHEDULE FOR DEVELOPMENT / MONITORING/ REVIEW

This e-Safety policy was approved by the Governing Body on:	
The implementation of this e-Safety policy will be monitored by the:	David Evans – e-Safety Coordinator / e-Safety committee
Monitoring will take place at regular intervals:	Yearly
The Governing Body Committee will receive a report on the implementation of the e-Safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Annually
The e-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	September 2016
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager, LA Safeguarding Officer, Police Commissioner's Office

1.11. The College will monitor the impact of the policy using

a. Logs of reported incidents
b. Monitoring logs of internet activity (including sites visited)
c. Internal monitoring data for network activity
d. Surveys / questionnaires of:
   i. students (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey)
   ii. parents / carers
   iii. staff

SCOPE OF THE POLICY

1.12. This policy applies to all members of the Robertsbridge Community College community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of Robertsbridge Community College ICT systems, both in and out of College.

1.13. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the Robertsbridge Community College site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of Robertsbridge Community College, but is linked to membership of the College.

1.14. The College will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of College.

ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the College

1.15. Governors:

a. Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of e-Safety Governor. The role of the e-Safety Governor will include:

   i. regular meetings with the e-Safety Co-ordinator
   ii. regular monitoring of e-safety incident logs
   iii. regular monitoring of filtering / change control logs
   iv. reporting to relevant Governors committee

1.16. Headteacher and Senior Leaders:

a. The Headteacher is responsible for ensuring the safety (including e-safety) of members of the College community, though the day to day responsibility for e-safety will be delegated to the e-Safety Co-ordinator David Evans.

b. The Headteacher / Senior Leaders are responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant

c. The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in College who carry out the

internal
e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

d. The Senior Leadership Team will receive regular monitoring reports from the e-Safety Co-ordinator
e. The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

1.17. e-Safety Coordinator

a. leads the e-safety committee
b. takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the College e-Safety policies / documents
c. ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
d. provides training and advice for staff
e. liaises with the Local Authority
f. liaises with college ICT technical staff
g. receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
h. meets regularly with e-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
i. attends relevant meeting / committee of Governors
j. reports regularly to Senior Leadership Team

1.18. Network Manager / Technical staff:

a. The Network Manager:
   i. that the College's ICT infrastructure is secure and is not open to misuse or malicious attack
   ii. that the College meets the e-safety technical requirements outlined in the LA Security Policy and Acceptable Usage Policy and any relevant Local Authority e-Safety Policy and guidance
   iii. that users may only access the College's networks through a properly enforced password protection policy, in which passwords are regularly changed
   iv. the College's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
   v. will keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
   vi. that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the e-Safety Co-ordinator /Headteacher / SLT / Head of ICT / Class teacher / Head of Year investigation / action / sanction

vii. that monitoring software / systems are implemented and updated as agreed in college policies

1.19. Teaching and Support Staff

a. Are responsible for ensuring that:

i. they have an up to date awareness of e-safety matters and of the current College e-Safety policy and practices

ii. they have read, understood and signed the College Staff Acceptable Use Policy / Agreement (AUP)

iii. they report any suspected misuse or problem to the e-Safety Co-ordinator /Headteacher / SLT / Head of ICT / Class teacher / Head of House(as in the section above) for investigation / action / sanction

iv. digital communications with students email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official College systems

v. e-safety issues are embedded in all aspects of the curriculum and other College activities

vi. students understand and follow the College e-safety and acceptable use policy

vii. students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

viii. they monitor ICT activity in lessons, extra-curricular and extended College activities

ix. they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current College policies with regard to these devices

x. in lessons where internet use is pre-planned students 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

1.20. Designated person for child protection / Child Protection Officer

a. is trained in e-safety issues and aware of the potential for serious child protection issues to arise from:

i. sharing of personal data

ii. access to illegal / inappropriate materials

iii. inappropriate on-line contact with adults / strangers

iv. potential or actual incidents of grooming

v. cyber-bullying

1.21. e-Safety Committee

a. Members of the e-Safety Committee will assist the e-Safety Coordinator with:

i. the production / review / monitoring of the College e-Safety policy / documents.

ii. the production / review / monitoring of the College filtering policy (if the College chooses to have one)

1.22. Students:

a. are responsible for using the College ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to College systems.

b. have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

c. need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

d. will be expected to know and understand College policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand College policies on the taking / use of images and on cyber-bullying.

e. should understand the importance of adopting good e-safety practice when using digital technologies out of College and realise that the College's e-Safety Policy covers their actions out of College, if related to their membership of the College

1.23. Parents / Carers

a. Parents / Carers 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 College will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

i. endorsing (by signature) the Student Acceptable Use Policy

ii. accessing the College website / VLE / on-line student records in accordance with the relevant College Acceptable Use Policy.

1.24. Community Users

a. Community Users who access College ICT systems / website / VLE as part of the Extended College provision will be expected to sign a Community User AUP before being provided with access to College systems.

<u>POLICY STATEMENTS</u>

1.25. Education – students

a. Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the College's e-safety provision. Children and young people need the help and support of the College to recognise and avoid e-safety risks and build their resilience. e-Safety education will be provided in the following ways:

  i. A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in College and outside College

  ii. Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities

  iii. Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

  iv. Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside college

  v. Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

  vi. Staff should act as good role models in their use of ICT, the internet and mobile devices

  vii. Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens

1.26. Education – parents / carers

a. Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report). The College will therefore seek to provide information and awareness to parents and carers through:

  i. Letters, newsletters, web site, VLE

  ii. Parents evenings

1.27. Education - Extended Colleges

a. The College will offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

1.28. Education & Training – Staff

a. It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
   i. A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
   ii. All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the College E-Safety policy and Acceptable Use Policies
   iii. The e-Safety Coordinator will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by the LA and others.
   iv. This e-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
   v. The e-Safety Coordinator will provide advice / guidance / training as required to individuals as required

1.29. Training – Governors

a. Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:
   i. Attendance at training provided by the Local Authority / National Governors Association / LA or other relevant organisation.
   ii. Participation in College training / information sessions for staff or parents

1.30. Technical – infrastructure / equipment, filtering and monitoring

a. The College will be responsible for ensuring that the College infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:
   i. College ICT systems will be managed in ways that ensure that the College meets the e-safety technical requirements outlined in the LA Security Policy and Acceptable Usage Policy and any relevant Local Authority e-Safety Policy and guidance
   ii. There will be regular reviews and audits of the safety and security of College ICT systems
   iii. Servers, wireless systems and cabling must be securely located and physical access restricted

iv. All users will have clearly defined access rights to College ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E-Safety Committee.

v. All users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames. Users will be required to change their password every 3 months.

vi. The “master / administrator” passwords for the College ICT system, used by the Network Manager must also be available to the Headteacher and kept in a secure place (eg College safe)

vii. Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

b. The College maintains and supports the managed filtering service provided by:

i. The College has provided enhanced user-level filtering through the use of the School Guardian filtering programme.

ii. In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).

iii. Any filtering issues should be reported immediately to LA.

iv. Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and E-Safety co-ordinator. f the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee

v. College ICT technical staff regularly monitor and record the activity of users on the College ICT systems and users are made aware of this in the Acceptable Use Policy.

c. Remote management tools are used by staff to control workstations and view users activity

i. An appropriate system is in place using the ICT work order system for users to report any actual / potential e-safety incident to the Network Manager (or other relevant person).

ii. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the College systems and data.

iii. An agreed policy (AUP) is in place for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the College system.

iv. An agreed policy (AUP) is in place regarding the downloading of executable files by users

v. An agreed policy (AUP) is in place regarding the extent of personal use that users (staff / students community users) and their family members are allowed on laptops and other portable devices that may be used out of College.

vi. An agreed policy (AUP) is in place that forbids staff from installing programmes on College workstations / portable devices.

vii. An agreed policy (AUP) is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on College workstations / portable devices.

viii. The College infrastructure and individual workstations are protected by up to date virus software.

ix. Personal data cannot be sent over the internet or taken off the College site unless safely encrypted or otherwise secured (AUP)

1.31. Curriculum

a. e-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

i. in lessons where internet use is pre-planned, it is best practice that students 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

ii. where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit

iii. it is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study.. Any request to do so, should be auditable, with clear reasons for the need

iv. students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

v. students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

1.32. Use of digital and video images - Photographic, Video

a. The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The college will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

i. When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

ii. Staff are allowed to take digital / video images to support educational aims, but must follow College policies concerning the sharing, distribution and publication of those images. Those images should only be taken on College equipment; the personal equipment of staff should not be used for such purposes.

iii. Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute.

iv. Students' must not take, use, share, publish or distribute images of others without their permission

v. Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

vi. Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

vii. Written permission from parents or carers will be obtained before photographs of students are published on the College website (may be covered as part of the AUP signed by parents or carers at the start of the year see Parents / Carers AUP Agreement in the appendix)

viii. Student's work can only be published with the permission of the student and parents or carers.

1.33. Data Protection

a. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

i. Fairly and lawfully processed

ii. Processed for limited purposes

iii. Adequate, relevant and not excessive

iv. Accurate

v. Kept no longer than is necessary

vi. Processed in accordance with the data subject's rights

vii. Secure

viii. Only transferred to others with adequate protection.

b. Staff must ensure that they:
   i. At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
   ii. Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
   iii. Transfer data using encryption and secure password protected devices.

c. When personal data is stored on any portable computer system, USB stick or any other removable media:
   i. the data must be encrypted and password protected
   ii. the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
   iii. the device must offer approved virus and malware checking software
   iv. the data must be securely deleted from the device, in line with College policy (below) once it has been transferred or its use is complete

1.34. Communications

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

	Staff & other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to College	X				X			
Use of mobile phones in lessons		X	X				X	
Use of mobile phones in social time	X					X		
Taking photos on mobile phones or other camera devices	X						X	

Use of hand held devices eg PDAs, PSPs	X						X	
Use of personal email addresses in College, or on College network	X						X	
Use of College email for personal emails	X							X
Use of chat rooms / facilities	X						X	
Use of instant messaging	X						X	
Use of social networking sites		X					X	
Use of blogs	X						X	

b. When using communication technologies the College considers the following as good practice:

i. The official College email service may be regarded as safe and secure and is monitored.

ii. Users need to be aware that email communications may be monitored

iii. Users must immediately report, to the nominated person – in accordance with the College 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.

iv. Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) College systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

v. Students will be provided with individual College email addresses for educational use.

vi. 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.

vii. Personal information should not be posted on the College website and only official email addresses should be used to identify members of staff.

1.35. Unsuitable / inappropriate activities

a. The College believes that the activities referred to in the following section would be inappropriate in a College context and that users, as defined below, should not engage in these activities in College or outside College when using College equipment or systems. The College policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
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:	child sexual abuse images					X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X
	pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	

	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the College or brings the College into disrepute				X	
Using College systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by LA and / or the College					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
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					X	
On-line gaming (educational)			X			
On-line gaming (non educational)				X		
On-line gambling					X	
On-line shopping / commerce			X			
File sharing				X		
Use of social networking sites			X			
Use of video broadcasting eg Youtube			X			

1.36. Responding to incidents of misuse

a. It is hoped that all members of the College 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 below are the responses that will be made to any apparent or actual incidents of misuse:

b. If any apparent or actual misuse appears to involve illegal activity ie.

   i. child sexual abuse images

   ii. adult material which potentially breaches the Obscene Publications Act

   iii. criminally racist material

   iv. other criminal conduct, activity or materials

c. The LA flow chart – below and should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

d. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the LA "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the LA Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

e. It is more likely that the College 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 College 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 as follows:

Students **Actions / Sanctions**

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of	Refer to Headteacher	Refer to Police	Refer to technical support staff for action	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X			X
Unauthorised use of non-								X	X

educational sites during lessons									
Unauthorised use of mobile phone / digital camera / other handheld device		X				X		X	X
Unauthorised use of social networking / instant messaging / personal email		X				X		X	X
Unauthorised downloading or uploading of files								X	X
Allowing others to access College network by sharing username and passwords		X			X	X		X	X
Attempting to access or accessing the College network, using another student’s account		X			X	X		X	X
Attempting to access or accessing the College network, using the account of a member of staff		X			X	X		X	X
Corrupting or destroying the data of other users		X			X	X		X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X	X	X	X
Actions which could bring the College into disrepute or breach the integrity of the ethos of the College	X	X	X		X	X	X	X	X
Using proxy sites or other means to subvert the College’s filtering system	X	X			X	X	X	X	X

Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X			X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act								X	

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X	X				X		
Unauthorised downloading or uploading of files	X	X				X		
Allowing others to access College network by sharing username and passwords or attempting to access or accessing the College network, using another person's account	X	X				X		X
Careless use of personal data eg holding or transferring data in an insecure manner	X	X				X		

Deliberate actions to breach data protection or network security rules	X	X			X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X				X	X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X					X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students	X	X				X		
Actions which could compromise the staff member's professional standing	X	X				X	X	X
Actions which could bring the College into disrepute or breach the integrity of the ethos of the College	X	X				X		
Using proxy sites or other means to subvert the College's filtering system	X					X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X					X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X				X	X
Breaching copyright or licensing regulations	X					X		
Continued infringements of the above, following previous warnings or sanctions		X					X	X