E-Safety & Electronic Communications Policy 2017

Reviewed by: Owen Perkins (E-Safety Co-ordinator)
Ratified by:
Next review:

Signed.. Richard Karn, Chair of Governors

Our mission statement: "*Outstanding learning and personal development for the future*"

Background

The use of mobile communication enabled devices is now so widespread amongst our community and so potentially useful in enhancing learning that we have to embrace their usefulness whilst preparing the members of our community for the potential dangers of using them: "We need to empower young people with the skills, knowledge and confidence that they need to embrace new technology to make the decisions that will protect themselves and their family." (Byron Report 2008).

Relationship to Other Policies

This Policy has been benchmarked against identified best practice and government guidance. What follows in this document should be read in conjunction with other College policies on Safeguarding, Anti-Bullying, Behaviour, Data Protection, Communications, Social Networking, Media, Equalities, Copyright and Discrimination.

Scope of the Policy

This policy applies to all members of the College community (including staff, students, volunteers, parents / carers, visitors & community users) who have access to and are users of College ICT systems, both in and out of the College. The Education and Inspections Acts 2006 & 2011 empowers the Headteacher, to such extent as is reasonable, to regulate the behaviour of students when they are off the College site and it empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety related incidents covered by this policy, which may take place outside of the College, but is linked to membership of the College. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

What is E-safety?

E-safety is much more than just use of the Internet on a computer. It also includes use of mobile phones, tablets, PDAs, games consoles, portable games devices and many other pieces of hardware that facilitate digital communication and collaboration. E-safety covers issues relating to children, young people and adults when using all electronic communications technologies, both in and out of College. It is about personal responsibility towards others people and managing the personal risks of using electronic communications technologies. E-safety requires education on risks AND responsibilities and is part of the 'duty of care' which applies to everyone working with children but especially those who use electronic communications technologies in their work with children. It is about making sure that the College effectively raises awareness to enable all users, including students, parents and staff, to be responsible and minimise the risks created by their own use of electronic communications technologies.

Our Philosophy

Heathfield Community College believes that the use of electronic communications technologies in our College is an entitlement in addition to our statutory curriculum commitments. We allow access to some internet based technologies to allow students to develop their education and learning about e-safety, whilst ensuring that the risks are minimised. For example, we follow government advice and best practice on filtering of access to social media and other parts of the internet. We also only allow managed access to the internet for those students who show a developing, mature, safe and responsible approach to its use. This entitlement can be withdrawn, temporarily or otherwise, if the privilege is abused or the safeguarding of an individual member of our community is judged by the Head Teacher (or delegated responsibility holder, for example, a Head of Year) to require such action.

We believe that Electronic Communications Technologies bring great benefits for the efficient management of the College, the exchange of ideas, social interaction, the improvement of educational standards and other learning opportunities. We believe that students and other College community users should be able to bring their own devices into college and use them for the benefit of the College community but with clear guidance as to when and under which circumstances this would be appropriate. We wish to use existing and emerging technologies to enhance the organisation and management of the College as well as to improve the learning experiences of our students without compromising the physical, psychological or data security of any of the members of our community. The following table summarises our approach to the use of communication technologies.

	Staff & other			Students / Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	wed with staff permission	Not allowed
Mobile phones may be brought to school	√				√			
Use of mobile phones in lessons		√					√	
Use of mobile phones in social time	√							√
Taking photos on mobile phones / cameras		√				√		
Use of tablets in lessons	√						√	
Use of tablets in social time	√							√
Use of mobile gaming devices		√				√		
Use of personal email addresses in school, or on school		√		√				
Use of school email for personal emails		√					√	
Use of messaging apps		√					√	
Use of social media		√						√[1]
Use of blogs		√					√	

[1] Individual teachers can apply to use social media with specific students where there is a clear learning benefit that can be justified to the leadership team.

Our Aims

The purpose of this document is to present guidelines for the responsible, safe and secure use of electronic communications technologies both within Heathfield Community College and outside of the College by members of its community. We wish to do so in such a way that is flexible enough to allow the College to adapt to technologies that we do not yet know about, whilst helping students, staff and the wider College community **to protect themselves** from the sometimes unanticipated risks and dangers that may be posed by the use of such technologies.

The Senior Leadership Team, supported by the Child Protection Officer, the E-safety Co-ordinator and the Network Manager, will continually review the use of Electronic Communications Technologies to examine it for its educational, organisational and management benefits, taking into account the potential risks BEFORE a change of use in College is promoted. This document will be reviewed and **updated at least every year** by the E-safety Co-ordinator in conjunction with the Network Manager, the Child Protection Officer and the Senior Leadership Team. The revisions will be endorsed by the governing body.

What Constitutes “Un” E-Safe / Unacceptable Usage of New Technologies?

The following applies equally to staff use as it does to students’ use of new technologies. It is **NOT an exhaustive list** and is presented purely for guidance:

- Using a mobile digital device in a lesson for anything other than the teacher’s intended use ie “off task” behaviour
- Seeking and /or viewing inappropriate content, including content related to “radicalisation”, even if found by other people
- Publishing, sharing or distributing personal information or other inappropriate content
- Leaving a device unlocked, including iPads & personal mobile phones, whilst unsupervised, that allows direct access to sensitive data or other data protected information.
- Predation and grooming
- Requests for personal information not pertinent to achieving the aims of the College.
- Publicly (defined as making available more widely than the core College community AND without the need for a password to be able access it) publishing, sharing or distributing digital images or digital video of another person without consent
- Bullying e.g. defamatory statements, creating defamatory images or threats
- Gambling
- Misuse of computer systems, both hardware and software
- Hacking and other security breaches
- Corruption or misuse of data
- Identity theft
- Running a private business from the College network
- Sending soliciting communications
- Connecting to proxy servers whilst on the College network
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Unfair usage (downloading / uploading large files that hinders others in their use of the internet)

- File sharing of other people's intellectual property
- Excessive use of screen based technologies (impacting on social and emotional development)
- Using school systems to run a private business
- Accessing, publishing, sharing, distributing & playing of unsuitable video / Internet games
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Inappropriate use of social media / networking sites for any of the above
- Making unreasonable expectations about when a community member should respond to electronic communication. (It is accepted by the College that a period of between 24-36 hours is a reasonable expectation for a response. It would also be unreasonable to expect staff to respond in their own private time but they may choose to do so anyway.)
- Allowing "vulnerable" students (as defined on a case by case basis by Social services, the Head Teacher, the Head of Learning Support and / or the Head of Year) unrestricted access to the internet

<u>Curriculum Entitlements</u>

In all subjects, use of electronic communications technologies should be:

1. designed to enhance the learning of students
2. clearly focused on learning outcomes
3. used for engaging students in their learning
4. used for enriching and extending learning activities
5. used for accelerating the learning of all students

ICT, Computing, Digital Literacy and PSHEE curriculum time will be used to:

1. educate all students about the of using new technologies, including how to use them responsibly, how to safe whilst online and how to react if they come across inappropriate material, making links with the themes of bullying, grooming, identity theft, copyright, data protection, radicalisation etc
2. educate all students about the accepted rules of electronic communication etiquette (AKA "Netiquette"). See section on "Netiquette" for further detail
3. emphasise the importance of personal responsibility on behalf of the students when using electronic communications
4. develop skills in quick and efficient data searching

<u>Responsibilities</u>

The Governors will:

- At least annually, review the effectiveness of the E-safety Policy
- Appoint a governor with responsibility for E-safety, separate to the ICT / Computing Link Governor
- Regularly monitor E-safety incident logs
- Regularly monitor filtering control logs

The **Headteacher** will:

- Take final responsibility for overseeing the coordination of the College's E-safety activities and procedures

- Ensure that both s/he and **at least** one 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
- Ensure an up to date E-safety policy (AKA the College E-safety & Electronic Communications Policy) is in place and make it easily accessible to all staff, governors, parents and visitors to the College, through the College website
- Enable the Network Manager & E-safety Co-ordinator to take all reasonable actions and measures, that are consistent with the College policy, to protect the users of the technologies that are provided by / used by members of the College community, including appropriate CPL
- Provide appropriate supervision for staff that manage filtering systems and monitor ICT use
- Explain the importance to all staff of adhering to the College Policy, as well as warning all staff that a member of staff who ignores security advice, or uses electronic communication technologies for inappropriate reasons risks dismissal
- Provide relevant and regularly updated (bi-annually or more regularly, if issues need to be urgently addressed) training and support to all staff about the dangers to themselves in managing their own ICT use, for instance in viewing inappropriate images to investigate their source, and where appropriate about the dangers faced by the students for whom they are responsible. This training should also be about best practice in managing E-safety and how to discuss E-safety issues with students
- Ensure that appropriate means are used to communicate clearly to students, staff and visitors that the use of College electronic communications hardware and software for inappropriate reasons is “unauthorised” and that the privilege of using the College’s facilities can be removed if a good reason arises e.g. for the safety of the individual, other individuals or for the safety of personal data. This will involve making it clear that e-mail, network and Internet use can be monitored
- Ensure that appropriate means are used to communicate clearly to all students and staff about how inappropriate or illegal ICT use is reported to senior management
- Ensure that acceptable use documents for students and staff, include reference to both the expected use of, and the appropriate use of, digital video in lessons
- Require **new staff**, on appointment, to read and sign an acceptable use document and thereby acknowledge that the College can monitor network and Internet use to help ensure staff and student safety, before providing access to the College facilities
- Require **all staff** to bi-annually read and sign an acceptable use document and thereby acknowledge any changes to the policy and E-safety procedures put in place by the College
- Require that **all students** apply for Internet access individually by agreeing to comply with the E-safety and acceptable use rules when signing an acceptable use letter, before providing access to the College facilities
- Require that **parents** sign and return a consent form for student access to the College facilities
- Draw parents’ attention to E-safety issues in newsletters, the College brochure and on the College website, offering the web site addresses where parents can get advice on filtering systems and educational and leisure activities that include responsible use of the Internet

- Insist that Teachers' official blogs, wikis or other social networking teaching tools should be run from sites in a way consistent with the College Social Networking / Communications policy
- Advise teachers that when running social network spaces for non-publishing learning purposes with students, that they should apply restrictions to who can view the space
- Advise teachers that when the purpose of a learning activity is about publishing to the world that student work should be moderated before it is published
- Remind teachers that their private blogs, wikis or other social networking tools could potentially undermine their professional role and status if appropriate privacy settings are not being used
- Remind staff of the College policy regarding the use of social media as a learning or communication tool and the potential consequences of the abuse of such media
- Remind staff that all work related devices, including iPads, which are used for accessing data or apps which can access network drives such as "Department Shares" or "Staff Shared", should be password protected and never left unlocked if not being used by their owner
- Remind staff that no personal data should be physically taken off the College premises unless it is encrypted AND that such data should NOT be shared outside of the College network unless the owner of the personal data has given express permission to do so (clauses in the network agreement cover most instances in which this occurs for the day to day running of the college for example: Exams and student progress data to the LA / DfE; Microsoft 360; virtual learning environments)
- Ensure that staff are issued with a College phone and /or College email account where direct contact with students is required outside of the College environment

The **Child Protection** / **E-safety co-ordinator** will (or delegate as required):

- Take day to day responsibility for E-safety issues
- Liaise with the Local Authority
- Liaise with College ICT technical staff
- Ensure that E-safety issues are seen within the College as safeguarding issues
- Receive reports of E-safety incidents and create a log of incidents to inform future E-safety developments
- Attend relevant meetings / committees of Governors
- Give reports, as required, to the Senior Leadership Team & governors
- Ensure that appropriate procedures are in place to protect those students for whom a less filtered internet environment creates a very high risk
- Ensure that the College provides regular up to date training in E-Safety issues for all staff
- Ensure that parents that are new to the College have the opportunity to attend E-Safety training provided by the College within a reasonable time period
- Ensure that all Network Acceptable Use Agreements are up to date and revalidated with an agreement from staff, parents and students on a regular basis

The Network Manager will:

- Discuss security strategies with the Local Authority (LA) and adopt recommended minimum procedures

- Work with the LA and the Internet Service Provider to ensure that external systems to protect students are reviewed and improved
- Ensure that the "master / administrator" passwords for the College ICT system, are also available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
- Ensure that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Discuss with the Senior Leadership Team the implications and resource requirements of implementing and maintaining a lightly managed Internet access environment
- Ensure that users may only access the College's networks through a properly enforced and appropriate password protection policy, even when using their own devices
- Securely locate servers and restrict physical access to them
- Ensure that the server operating system is secured and kept up to date
- Ensure that the virus protection for the whole network is fully installed and current.
- Ensure that firewalls, switches and the wireless network are configured to prevent unauthorised access between members of any educational Wide Area Network used by the College
- Ensure that access to the network by wireless devices is pro-actively managed
- Review system capacity regularly
- Regularly review the security of the College information systems, including ensuring that all unauthorised portable electronic and wireless devices do not have access to the College network or its files
- Ensure that files held on the College's network will be regularly checked for viruses or other malicious software
- On request, provide an up to date record of access levels granted to all network users
- Ensure, wherever practicable, workstations are secured against both user mistakes and deliberate actions
- Block / filter only those websites / website categories that the Senior Leadership Team decides should be restricted as part of a lightly managed Internet environment. This will include ensuring that Illegal content (eg child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.
- Implement an enhanced / differentiated user-level filtering system (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc) in line with recommendations made by the College SLT.
- Restrict access to the internet, using a blocking / filtering system, for all students regarded as "vulnerable" and "at risk"
- Use the agreed process for dealing with requests for filtering changes (see Appendix D for more details)
- Provide regular reports to the E-Safety Officer on E-safety related incidents that are highlighted by the network monitoring systems

Heads of Department will:

- Ensure that classroom teachers take advantage of the benefits for learning of using the Internet and mobile devices as a normal approach to teaching and learning
- Ensure that students' entitlement to learn in a digitally literate way is planned into their curriculum
- Ensure the prominent display of safe use guidelines, including E-safety rules in all rooms with Internet access or where mobile devices will be used
- Support classroom teachers in planning and organising their lessons to prevent behaviour issues from arising as a result of digitally facilitated time wasting that is unrelated to the learning outcomes of lessons
- Monitor and evaluate the implementation of this E-safety policy within their subject area for those lessons that incorporate ICT and related electronic communications technologies
- Remind their staff about the E-safety issues around using the Internet and social media in both their private and professional lives

All staff will:

- Ensure that they have an up to date awareness of E-safety matters and of the current College E-safety policy and practices
- Encourage responsible use of all internet enabled devices
- Report any suspected misuse or problem to the E-safety Co-ordinator / Child Protection Officer / Headteacher / Network Manager / Head of Department as appropriate to the situation for investigation / action / sanction
- Ensure that all digital communications with students (email / Virtual Learning Environment / audio files etc..) should be on a professional level and only carried out using official College systems or otherwise approved by the College in line with its other policies eg the policy for Social Networking / Communications
- Ensure that all work related devices, including iPads & personal mobile phones, which are used for accessing data or apps that can access network drives such as "Department Shares" or "Staff Shared", should be password protected and never left unlocked if not being used by their owner
- Ensure that no personal data is physically taken off the College premises unless it is encrypted AND that such data should NOT be shared outside of the College network unless the owner of the personal data has given express permission to do so (clauses in the network agreement cover most instances in which this occurs for the day to day running of the college for example: Exams and student progress data to the LA / DfE; Microsoft 360; virtual learning environments).

Classroom teachers will:

- Ensure that they take advantage of the benefits for learning of using the Internet and mobile devices when it is appropriate to do so to improve learning
- Ensure that they have an up to date awareness of e-safety matters and of the current College e-safety policy
- Ensure that they have read, understood and signed the Staff Acceptable Use Agreement
- Plan lessons that are organised to prevent behaviour issues arising from digitally facilitated time wasting activities that are unrelated to the learning outcomes of lessons

- Monitor the use of electronic communications devices in their lessons and treat any off-task use of these technologies as an issue to be followed up, using the College behaviour policy
- Remind students about what Internet use is acceptable, giving clear objectives for the use of those technologies in lesson where they are used
- Remind students about safe Internet searching techniques
- Remind students to be critically aware of the materials they read and how to validate and evaluate electronic sources of information before accepting its accuracy and including it in their work
- Remind students to evaluate the electronic sources of information in their work
- Remind students to never to give out personal details of any kind which may identify them and / or their location. This should include, but is not restricted to: their address, mobile or landline phone numbers, College attended, instant messaging and e-mail addresses, full names of friends, specific interests and clubs attended, posting full face photographs on social networking sites, posting photographs taken in an easily identifiable location on social networking sites eg outside an identifiable building, whilst wearing the College logo on clothing
- Remind students about personal and network security and encourage them to set safe passwords, deny access to unknown individuals and how to block unwanted communications
- Remind students to reject "friend" invitations or similar from people that they do not know personally when using social networking spaces
- Remind students about how to electronically publish specific and detailed private thoughts in a way that does not put them at risk
- Remind students to only publish material that is not harmful to other individuals or to the reputation of the College
- Only allow the recording by a student of any digital image of another person if it helps to achieve the learning objectives of that lesson AND, if it is to be published in the public domain that they have previously checked the digital imaging exemptions list to make sure that we have permission to record digital images of that person
- Remind students, using electronic communications technology for research purposes, about the potential copyright implications of using materials sourced electronically, and how to reference the sources of their information appropriately
- Never leave a work related device, including iPads & personal mobile phones, which are used for accessing data or apps that can access network drives such as "Department Shares" or "Staff Shared", without password protection and never leave them unlocked if not being used by their owner

Students will follow the College **E-Safety code of conduct (see Appendix E)**, including:

- Take responsibility for the proper care of any mobile digital device that they are asked to use as part of a lesson
- Only use mobile digital devices in lessons as instructed by their teacher to aid the intended learning
- Fully reference the sources of any research information that they use in their formally assessed work
- Ask permission BEFORE taking photographs or video images of another member of the community
- Not share passwords with anyone else

- Not share personal details, that may identify them or their location, with anyone via a digital device
- Not automatically trust information researched on a digital device unless they have use validation techniques to check that information
- Not publish any material that is or could potentially be harmful to another person

Parents will support the College in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website and e-Lockers
- Their children's personal devices both inside and outside of the College

Community Users who access school systems / website as part of the wider College provision will be expected to sign a Community User Agreement (AUA) before being provided with access to school systems.

<u>Responding To Evidence of Inappropriate Use</u>

Students should:

- Report instances of inappropriate use to a trusted member of staff, usually their form teacher or the class teacher in which the instance occurred

Class teachers should:

- Inform the Designated Child Protection Officer for cases involving potential issues related to the safeguarding of, a child
- Follow the College behaviour policy for instances of digitally enabled "off task" behaviour
- Follow the College behaviour policy for instances of misuse of the College facilities AND inform the Network Manager
- Not allow students with internet bans to use another person's login details / device to access a lesson unless supervised and monitored for 100% of the time.

Heads of Department will:

- Follow the College behaviour policy for instances of misuse of the College facilities by students that have been referred to them
- Follow the College policy on staff disciplinary procedures for instances of misuse of the College ICT facilities by their staff. This includes informing the Head Teacher

The **Network Manager** will:

- Restrict individual student access to the Internet and/or other ICT equipment in College as appropriate to the situation. Eg in terms of both misuse of the College facilities AND for the protection of the individual
- Immediately inform the appropriate Head of Year & relevant teaching staff when individual student access to the Internet and/or other ICT equipment in College has been restricted
- Inform parents, as appropriate to the situation, and as agreed with a senior member of staff, for example the Head of Year
- Refer any evidence about **staff misuse** directly to the Head Teacher

- Refer any material that is believed to be illegal to the Head Teacher
- Organise the investigation of inappropriate websites so that there is more than one member of staff present in the room when inappropriate material is likely to be displayed on screen

The **Designated Child Protection Officer** will:

- Co-ordinate, in accordance with the College policy on Safeguarding, action on any reports involving potential abuse of a child or an issue that affects the safety of a child
- Report any material that the College believes is illegal to the appropriate agencies, eg the Police
- Ensure that there is a procedure in place to record E-Safety incidents
- Provide copies of the E-safety incident log to the Governor's committee overseeing Child Protection issues at each meeting of the committee

The **Headteacher** will:

- Consider the **full range of disciplinary proceedings** where a member of staff who uses electronic communication technologies, including social media, for inappropriate reasons, as appropriate to the situation. In the most serious instances this could potentially lead to **dismissal**. Such proceedings will be started in response to any misuse that appears to include any of the following, that is an illegal activity, but is not limited to this list:
    1. child sexual abuse images
    2. adult material which potentially breaches the Obscene Publications Act
    3. criminally racist material
    4. breaches of copyright eg illegal downloading of music or video files
    5. other criminal conduct, activity or materials

A flow chart containing East Sussex guidance on how to respond to an E-safety incident can be found in **Appendix B. Appendix C contains flow charts** for guidance on: how we will respond to issues relating to illegal activity, material and content; for how we respond to students accessing inappropriate but legal materials; and for how we consider whether or not students should be denied less filtered internet access. Flow charts, showing the agreed lines of action for potential breaches of this policy, especially with regard to the use of Social Media sites, can also be found within the Social Media policy.

<u>Control Measures for a Managed Filtering Internet Environment / Ipad for all Environment</u>

In order to be sure that we are providing adequate support for students in a managed filtering environment, all of the actions described above should be adequate. However, in addition to this:

- All parents /carers are given the opportunity to take advice on the safe management of the use of mobile devices, including screen time addiction through the new Parents E-Safety evening
- All parents purchasing an iPad through the college recommended scheme are offered the opportunity to join the college managed internet access service for those devices when outside of College
- Heads of Year regularly monitor suspicious search criteria reports and follow up with the student, in the first instance, should anything worrying emerge

- Heads of Year follow the guidance in Appendix C should they have a suspicion that a student could be at particular risk, possibly leading to the re-imposition of filtered protection for individuals up to and including removing internet access altogether, as appropriate to the circumstances.
- Heads of Year follow the guidance in Appendix C for all students already identified as being at risk.

Electronic Communication, including Email

The College sees the potential benefits of a range of electronic communication methods between staff, students and parents, in enhancing the work and effectiveness of the College. It also believes that it is easy to for the users of such communication methods, particularly E-mail but also including official use of Social Networking, to forget the needs of the potential receivers of such electronic communication. As such the College believes that guidance in the use of electronic communication is an important way of ensuring that the work and effectiveness of the College is enhanced by its use.

All senders of electronic communications, including email and other messaging facilities, should remember that:

- The communication creates an impression, in the eyes of the receiver, about the College and should, where applicable to the audience, **be treated as a formal piece of written communication** and so should be constructed with-the general rules of formal written communication in mind
- The "subject field" in E-mails should be used to convey information that would allow the receiver to decide how urgent it is to answer or act upon that E-mail
- They should not send personal data, including student records, over the Internet. (Please refer to the Data Protection policy for further guidance)
- E-mails should only be sent to the people who need to receive the information contained within it and **not to all staff or to all teaching staff** unless this is absolutely necessary
- They should not use College facilities to send non-College related messages to all staff or large groups of staff. This represents a form of unwanted electronic communication called SPAM
- Electronic communication that requires urgent action may not be read in time for that action to be taken. (It is accepted by the College that a period of between 24-36 hours is a reasonable expectation to receive a response to a piece of urgent electronic communication)
- It is unreasonable, and in some cases impossible, for E-mails sent in the afternoon of a working day to require action by a time before the end of the next working day. The College believes that it would be unreasonable to expect staff to respond to electronic communication in their own private time
- Chain letters sent via E-mail should not be forwarded

The Leadership Team should ensure that:

- Facilities are in place to allow staff to send bulk E-mails to specific staff. For example, all teachers of Y10, Y10 form tutors etc. Consultation may be necessary to decide the make-up of these groups
- Procedures are in place to ensure that the intended recipients of the bulk E-mail addresses are accurate and up to date at the beginning of each new academic year and whenever College staffing changes

- This policy is communicated to all new staff

Staff Should:

- Use electronic communications facilities to communicate with students only using facilities approved by the College eg College email, approved social networking pages
- Only communicate with students electronically for direct College related reasons, for example, to set work, give feedback on work that has been marked, notify students of the location of learning materials, to organise other College related activities etc.

Students will:

- Only use approved E-mail accounts in College, for example their own College web based E-mail account
- Not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission from a relevant adult
- Immediately tell a teacher if they receive offensive E-mail or E-mail that breaks any part of the College E-safety policy
- Never forward chain letters by E-mail

The Accepted Rules Of Electronic Communication Etiquette AKA Netiquette

These include but are **not limited to** the following:

- Be polite
- Use appropriate language
- Do not use abusive language in your messages to others
- Do not expect a reply to electronic communication within an unreasonable time period eg 24-36 hours
- Do not expect a reply to electronic communication during a member of staff's non-contracted working time
- Unless circumstances require it and appropriate permissions have been obtained, e.g. staff communications with suppliers or outside organisations, do not reveal the address, phone number, photographic image or other personal details of yourself or other users
- Not using the network in such a way that would disrupt the use of the network by other users
- Not engaging in any Illegal activities
- Remembering that e-mail is not guaranteed to be private
- Not engaging in messages relating to or in support of illegal activities

Rules Regarding Video Conferencing Or Similar Interactive Learning Technologies (eg Skype)

- Ensure all video recording equipment in classrooms is switched off when not in use and not set to auto answer
- Ensure that video conferencing contact information is not put on the College Website.
- Secure the equipment when not in use
- Ensure that College video conferencing equipment is not taken off site without permission

- Ensure that students ask permission from the supervising teacher before making or answering a video conference type call
- Ensure that parents and carers have given express consent for their children to take part in video conferences
- Ensure that all participants have given written permission in advance when recording a video conference lesson. The reason for the recording must be given and the recording of a video conference should be clear to all parties before the start of the conference
- Ensure that recorded material is stored securely
- Ensure that, if third-party materials are included in the lesson, it is acceptable to do so to avoid infringing the third party intellectual property rights eg Copyright law

Electronically Published Information by the College or College staff

- The Head Teacher will take overall editorial responsibility or delegate this to an appropriate person to ensure that content is accurate and appropriate
- We will not publish staff or students' personal data, including first names, or their photographic image, without prior permission
- We will only publish digital images of students, whose parents have given their permission in advance
- We will take measures to avoid spam harvesting in the way that we publish E-mail addresses
- We will ensure that the College website complies with the College's guidelines for publications, including respect for personal privacy, intellectual property rights, including copyright

Appendix A

Legal Framework

The following is accurate as of the time of the most recent review of this policy.

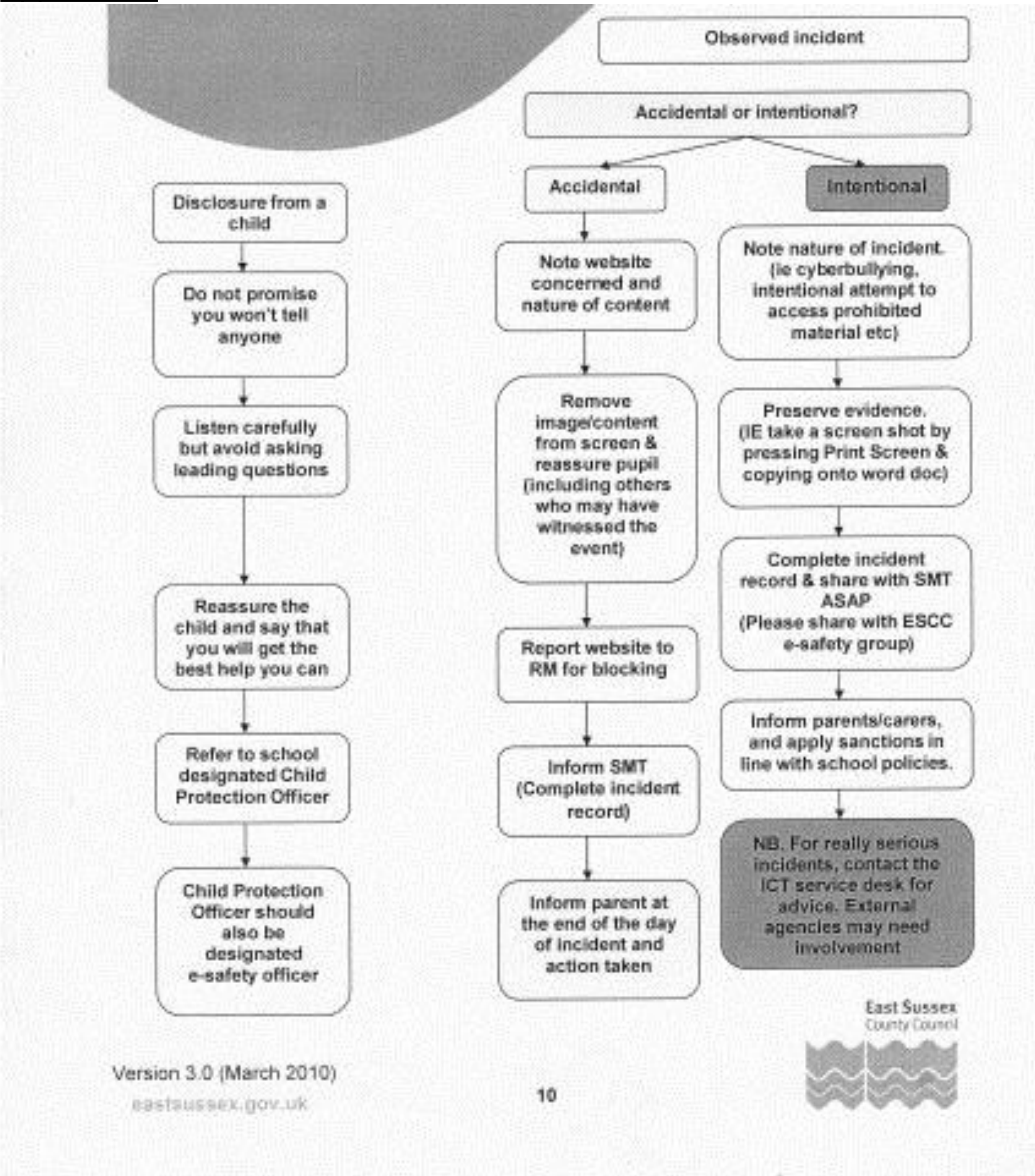
- **Obscene Publications Act 1959 and 1964**. Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.
- **Protection of Children Act 1978 (Section 1**). It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.
- **Telecommunications Act 1984**. It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.
- **Public Order Act 1986 (sections 17 – 29**). This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.
- **Malicious Communications Act 1988 (section 1)**. This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.
- **Copyright, Design and Patents Act 1988**. Copyright is the right of a person to prevent others from copying or using his or her "work" without permission. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film, theatre, poetry, dance, mime, architecture, databases and software all qualify for copyright protection, although not until they are recorded by some means, in writing or otherwise. The author of the work is usually the copyright owner, but if it was created during the course of employment it usually belongs to the employer. It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author(s) permission. Sometimes a licence associated with the work will allow a user to copy or use it for limited purposes (eg. Creative Commons Licence, Colleges license agreements). You must obtain permission from the copyright holder before you copy or use someone else's material, unless the terms of such a license permit it. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.
- **The Computer Misuse Act 1990 (sections 1 – 3).** Regardless of an individual's motivation, the Act makes it a criminal offence to: gain access to computer files or software without permission (for example using someone else's password to access files); gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or impair the operation of a computer or program (for example caused by viruses or denial of service attacks). UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

- **Trade Marks Act 1994.** This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.
- **Criminal Justice & Public Order Act 1994**. This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress.
- **Protection from Harassment Act 1997**. A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.
- **Data Protection Act 1998**. The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.
- **Human Rights Act 1998.** This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. The college is aware that all of its policies ned to be put in the context of:
    - The right to a fair trial
    - The right to respect for private and family life, home and correspondence
    - Freedom of thought, conscience and religion
    - Freedom of expression
    - Freedom of assembly
    - Prohibition of discrimination
    - The right to education
- **Freedom of Information Act 2000.** The act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures
- **Regulation of Investigatory Powers Act 2000. The Regulation of Investigatory Powers Act 2000 (RIPA)** regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enactedto comply with the Human Rights Act 1998.
- **The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000** permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to College activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
- **The Sexual Offences Act 2003,** which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of the

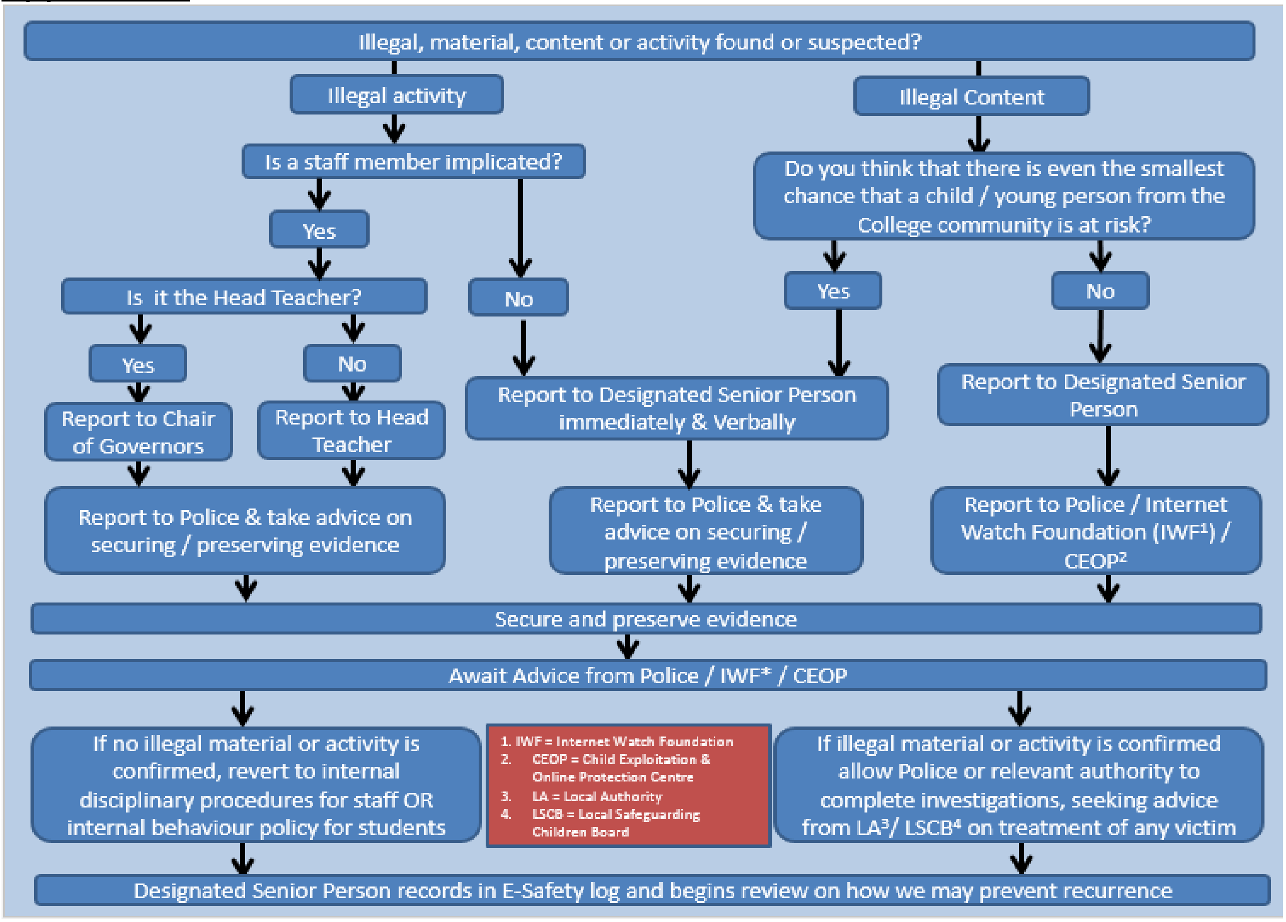
child to 18 years old.The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your owngratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust.

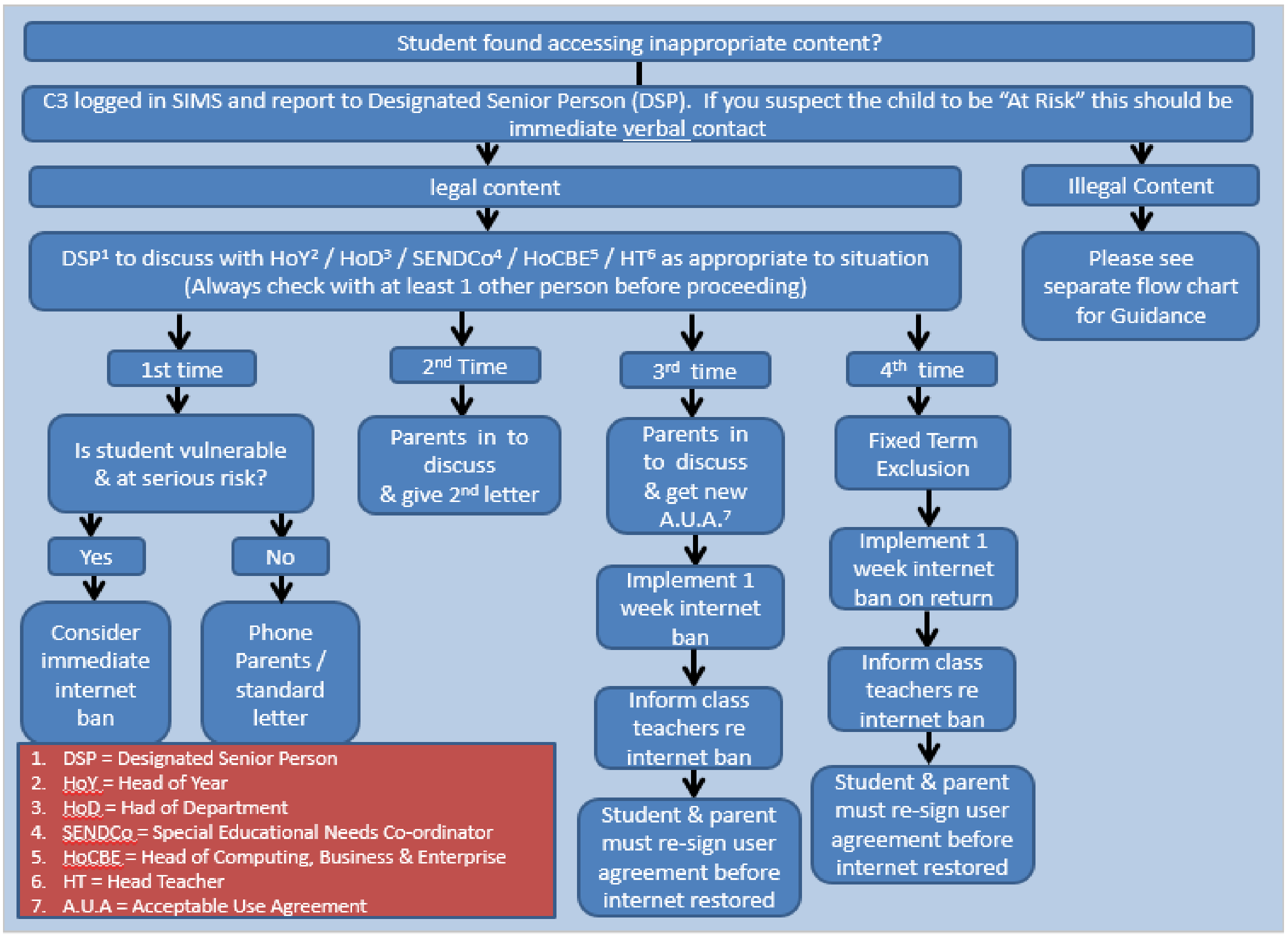
- **Communications Act 2003 (section 127).**Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent : there is no need to prove any intent or purpose.
- **Communications Act 2003 (section 127).**Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent : there is no need to prove any intent or purpose.
- **The Racial and Religious Hatred Act 2006**. This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.
- **The Police and Justice Act 2006**, which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.
- **The Education and Inspections Act 2006 & 2011**. Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the College site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. Please refer to the following website for the detail of this act which changes the legal responsibilities of various bodies in respect of the welfare of children in the care of Colleges. http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted.
- **The Protection of Freedoms Act 2012.** Requires schools to seek permission from a parent / carer to use Biometric systems.
- **The School Information Regulations 2012.** Requires schools to publish certain information on its website: http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations

Appendix B

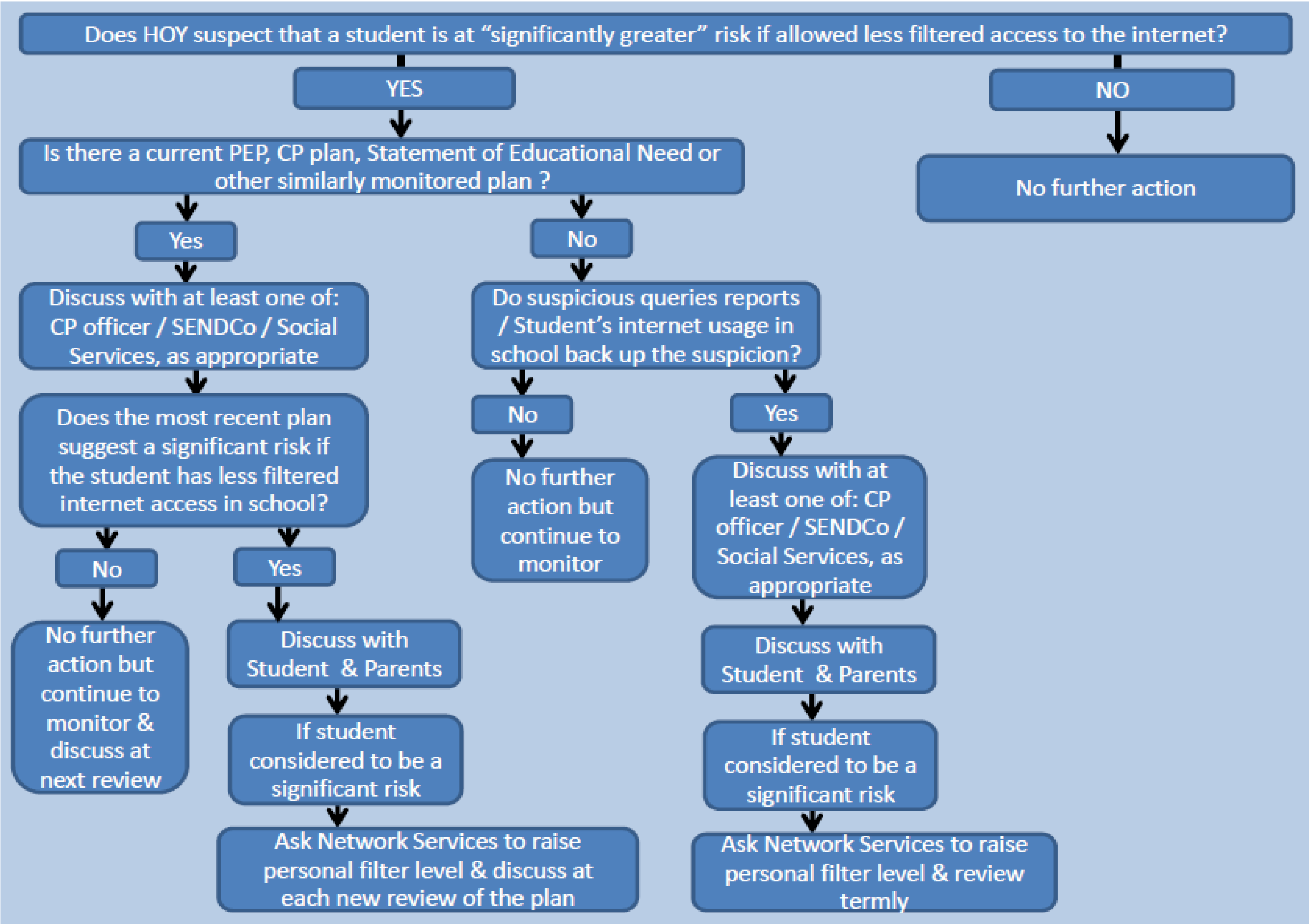

Observed incident
Accidental or intentional?
Accidental
Intentional
Disclosure from a child
Do not promise you won't tell anyone
Listen carefully but avoid asking leading questions
Reassure the child and say that you will get the best help you can
Refer to school designated Child Protection Officer
Child Protection Officer should also be designated e-safety officer
Note website concerned and nature of content
Remove image/content from screen & reassure pupil (including others who may have witnessed the event)
Report website to RM for blocking
Inform SMT (Complete incident record)
Inform parent at the end of the day of incident and action taken
Note nature of incident. (ie cyberbullying, intentional attempt to access prohibited material etc)
Preserve evidence. (IE take a screen shot by pressing Print Screen & copying onto word doc)
Complete incident record & share with SMT ASAP (Please share with ESCC e-safety group)
Inform parents/carers, and apply sanctions in line with school policies.
NB. For really serious incidents, contact the ICT service desk for advice. External agencies may need involvement
East Sussex County Council
Version 3.0 (March 2010)
eastsussex.gov.uk
10

Appendix C


Illegal, material, content or activity found or suspected?
Illegal activity
Illegal Content
Is a staff member implicated?
Do you think that there is even the smallest chance that a child / young person from the College community is at risk?
Yes
Is it the Head Teacher?
No
Yes
No
Yes
No
Report to Chair of Governors
Report to Head Teacher
Report to Designated Senior Person immediately & Verbally
Report to Designated Senior Person
Report to Police & take advice on securing / preserving evidence
Report to Police & take advice on securing / preserving evidence
Report to Police / Internet Watch Foundation (IWF¹) / CEOP²
Secure and preserve evidence
Await Advice from Police / IWF* / CEOP
If no illegal material or activity is confirmed, revert to internal disciplinary procedures for staff OR internal behaviour policy for students
1. IWF = Internet Watch Foundation
2. CEOP = Child Exploitation & Online Protection Centre
3. LA = Local Authority
4. LSCB = Local Safeguarding Children Board
If illegal material or activity is confirmed allow Police or relevant authority to complete investigations, seeking advice from LA³/ LSCB⁴ on treatment of any victim
Designated Senior Person records in E-Safety log and begins review on how we may prevent recurrence


Student found accessing inappropriate content?
C3 logged in SIMS and report to Designated Senior Person (DSP). If you suspect the child to be "At Risk" this should be immediate verbal contact
legal content
Illegal Content
DSP¹ to discuss with HoY² / HoD³ / SENDCo⁴ / HoCBE⁵ / HT⁶ as appropriate to situation (Always check with at least 1 other person before proceeding)
Please see separate flow chart for Guidance
1st time
2nd Time
3rd time
4th time
Is student vulnerable & at serious risk?
Parents in to discuss & give 2nd letter
Parents in to discuss & get new A.U.A.⁷
Fixed Term Exclusion
Yes
No
Implement 1 week internet ban
Implement 1 week internet ban on return
Consider immediate internet ban
Phone Parents / standard letter
Inform class teachers re internet ban
Inform class teachers re internet ban
Student & parent must re-sign user agreement before internet restored
Student & parent must re-sign user agreement before internet restored
1. DSP = Designated Senior Person
2. HoY = Head of Year
3. HoD = Had of Department
4. SENDCo = Special Educational Needs Co-ordinator
5. HoCBE = Head of Computing, Business & Enterprise
6. HT = Head Teacher
7. A.U.A = Acceptable Use Agreement

Appendix C Cont'd



Appendix D

The process for requesting changes to the agreed filtering system.

1. Staff finding that a website that they would like to use for learning purposes is still filtered / blocked can request that this site be unblocked.

   In the first instance this should be submitted, using the online form linked to from the screen which appears when trying to access the site. This will ask for a reason and you will receive a response as soon as possible.

2. Staff finding that sites that are not filtered are causing negative consequences for learning and believe that it should be blocked.

   In the first instance this should be submitted in writing / email to the deputy Headteacher responsible for line managing the implementation of the College Digital strategy with an explanation.

   On approval, this can then be submitted to Network Services for implementation.

Appendix E

The E-Safety Student Code of Conduct

HCC Internet and E-Safety Code of Conduct

Students Will:

Keep ALL passwords private
Immediately change your password if anyone finds it out
Respect other people's work
Respect other people's opinions and beliefs, even if you disagree
Respect the College's and other people's equipment
Tell a teacher or use the "report abuse" button if you are ever made to feel scared or uncomfortable
Always keep your own and other people's information private eg name, address, school, pets, close up photos
Only reply to messages from people you know or who have been approved by an adult you know
Always give credit to the source of other people's work if you have used it in your own work

Students will NOT:

Tell anyone your network password
Reply to nasty messages. (Tell an adult or use the "report abuse" button AND keep it as evidence)
Show other people photos of yourself, friends or family without asking an adult first
Agree to meet an online friend without checking with an adult first
Be rude, offensive, bully or harass other people eg on facebook
Use a mobile / portable device in a lesson for anything other than a learning activity set by the teacher
Electronically publish personal details or identifying photos eg name, address, school, pets, close up photos
Access, read, alter or delete the work of other people
Search for, create, transmit, view or share inappropriate material
Play non educational games over the college network
Attempt to install executable files, programs or viruses on the network
Attempt to access the operational files of the network