Online Safety Policy 2023-24

Reviewed by:	Owen Perkins (Online Safety Coordinator)
Designated Safeguarding Lead (DSL) is:	Mike Pooley
Governor Responsible for Online Safety:	Mark Evans
Approved & Ratified by:	Headteacher – Caroline Barlow
Next review:	September 2024

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures

Signed..... Richard Karn, Chair of Governors

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

Contents

Page 3: 1. Our aims
2. What is Online Safety?
3. Our Philosophy
Page 4: 4. Scope of the Policy
4.1. Relationship with other policies
4.2. Monitoring and Review
4.3. What constitutes unsafe / unacceptable use of New Technologies
5. Curriculum Entitlements (all subjects/Computing, Digital Literacy, PSHEE)
Page 5: 6. Responsibilities
6.1. Governors'
6.2. Head Teacher / Leadership Team
Page 6: 6.3. DSL
6.4. Network Managers
Page 7: 6.5. Curriculum Leaders
6.6. All staff
6.7. Classroom teachers
Page 8: 6.8. Students
6.9. Parents' & carers
Page 9: 6.10. Community Users responsibilities
7. Education & Engagement Approaches
7.1. Engagement & Education of Students
7.2. Engagement & Education of Students (vulnerable)
7.3. Engagement and Education of Staff
Page 10: 7.4. Engagement & education of Parents and Carers
8. Reducing Online Risks
Page 11: 9. Safer Use of Technology
9.1. Classroom Use
9.2. Managing & Authorising Internet Access
Page 13: 9.3. Managing personal data online
9.4. Security and Management of Information Systems
9.5. Password Policy
9.6. Managing the Safety of our website
9.7. Publishing Images, Videos & Other Recordings Online
9.8. Managing Electronic Communications, especially Email
Page 14: 9.9 Live Stream Lessons for Remote Learning
Page 16: 10. Use of Video Conferencing or Similar Technologies
Page 16: 11. The College Learning Platform
Page 17: 12. Management of Apps Used to record Children's Progress
13. Social Media
Page 22: 14. iPads, Personal Devices and Mobile Phones
Page 25: 15. Responding to Online Incidents and Concerns
16. Procedures for Responding to Specific Online Incidents or Concerns
Page 26: 16.1 Online Sexual Violence and Sexual Harassment between Children
Page 27: 16.2. Youth Produced Sexual Imagery ("Sexting")
Page 28: 16.3. Online Child Sexual Abuse and Exploitation)
Page 29: 16.4. Indecent Images of Children (IIOC)
Page 30: 16.5. Cyberbullying
16.6. Online Hate
Page 31: 16.7. Radicalisation, Online Extremism and Online Hate
Page 32: Appendix A: The types of Online Safety Risks
Page 33: Appendix B: What is and what is not allowed in college and when
Page 34: Appendix C: The legal framework
Page 38: Appendix D: What constitutes unsafe / acceptable use of new technology
Page 39: Appendix E: Reporting flow diagrams
Page 42: Appendix F: Requesting changes to the filtering system
Page 43: Appendix G: Online Safety Code of Conduct
Page 44: Appendix H: Electronic Communication & "Netiquette"
Page 45: Appendix I: Social Media Application Form

1. Our Aims

This online safety policy has been written by Heathfield Community College, involving staff, students and parents/carers, building on the East Sussex County Council/The Education People online safety policy template, with specialist advice and input as required. It takes into account the DfE statutory guidance "Keeping Children Safe in Education" (KCSiE) 2021 and the East Sussex Safeguarding Children Partnership procedures.

The purpose of this document is to:

- safeguard and protect all members of our community whilst online.
- identify approaches and to educate and raise awareness of online safety with all members of our community
- enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- identify clear procedures to use when responding to online safety concerns that are known by all members of the community.
- ensure that all changes to the use of Electronic Communications Technologies in College are examined to take into account BOTH the potential risks and benefits BEFORE a change of use in College is promoted.

2. What is Online Safety?

Online safety is what was formerly known as e-safety. A summary of the generally accepted range of risks faced by children can be found In Appendix A. This is by no means a comprehensive list as new risks emerge and others evolve all of the time.

Online 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 other pieces of hardware that facilitate digital communication and collaboration. Online safety is about personal responsibility and managing the personal risks of using such technologies. Online safety requires education on risks AND responsibilities and is part of the 'duty of care' to both children and those that work with children. It is about making sure that the College effectively raises awareness to enable all users, including students, parents /carers and staff, to be responsible and minimise the risks created by their own use of these technologies.

3. Our Philosophy

We believe that:

- online safety is an essential part of safeguarding and acknowledge our duty to ensure that all students and staff are protected from potential harm online.
- the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life and can bring great benefits to students, the College and other College stakeholders.
- students should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- the use of electronic communications technologies in our College is an entitlement in addition to our statutory curriculum commitments.
- this access should be withdrawn if the privilege is abused or the safeguarding of an individual member of our community is judged to require such action.
- the benefits of using these technologies should not be allowed to compromise the physical, psychological or data security of any of the members of our community. A table that summarises what is and what is not allowed in College and when can be found in Appendix B.

4. Scope of the Policy

This policy has been benchmarked against best practice and government guidance. The legal framework can be found in Appendix C. This policy applies to:

- all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the College (collectively referred to as "staff" in this policy) as well as students, parents and carers
- all access to the internet and uses of technology, including personal devices, or where students, staff or other individuals have been provided with setting issued devices for use off-site, such as work laptops, tablets or mobile phones.
- any incidents of cyber-bullying, or other online safety incidents which may take place either inside or outside of the College (but is linked to membership of the College).
- all related issues covered by the published Behaviour for Learning policy and the staff Code of Conduct.

4.1. Relationship to Other Policies

What follows should be read in conjunction with other College policies on (but not limited to) Safeguarding, Anti-Bullying, Network Acceptable Use Agreement, Behaviour, Staff Code of Conduct, Data Protection, Equalities, Copyright, Discrimination, Computing, Personal Social and Health Education (PSHE), Sex and Relationships Education (SRE).

4.2. Monitoring and Review

This document will be reviewed by the Online Safety Co-ordinator in conjunction with the Network Manager, the Designated Safeguarding Lead (DSL) and the Senior Leadership Team. The revisions will be endorsed by the governing body.

- Technology in this area evolves and changes rapidly. As a result, we will review this policy **at least annually**
- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Head Teacher will be informed of online safety concerns, as appropriate.
- The DSL / named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

4.3. What Constitutes Unsafe / Unacceptable Usage of New Technologies?

A detailed but NOT definitive list can be found in Appendix D.

5. Curriculum Entitlements

5.1 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

5.2 ICT, Computing, Digital Literacy & 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 be 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
5. develop skills in appraising the reliability of data found on the internet

6. Responsibilities

The Designated Safeguarding Lead (Mike Pooley) has lead responsibility for online safety and some aspects of this role are delegated to an Online Safety Co-ordinator (Owen Perkins). However, we recognise that all members of the community have important roles and responsibilities to play with regards to online safety.

6.1. The **Governors** will:

- At least annually review the effectiveness of the Online Safety Policy
- Appoint a governor with responsibility for online safety.
- Regularly monitor online safety incident logs
- Regularly monitor filtering control logs

6.2. The **Head Teacher / Leadership Team** will:

- Recognise that a one size fits all approach may not be appropriate for all children and a more personalised or contextualised approach to online safety is used for more vulnerable children and children with SEND
- ensure that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture
- ensure there are appropriate and up-to-date policies regarding online safety; this includes our Behaviour for Learning policy and our Network Acceptable Use Agreements
- ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks; as schools increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material (including when they are online at home)
- ensure that online safety is embedded within a progressive curriculum, which enables all students to develop an age-appropriate understanding of online safety both at school and at home
- supporting the DSL / Online Safety Co-ordinator by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities
- ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support
- ensure that appropriate risk assessments are undertaken regarding the safe use of technology
- audit and evaluate online safety practice to identify strengths and areas for improvement
- provide staff that manage filtering systems and monitor ICT use with appropriate supervision and monitoring
- ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety
- explain the importance to all staff of adhering to the College Policy, up to and including the risk of dismissal

- ensure that relevant and regularly updated, training and support to all staff about the dangers to themselves in managing their own ICT use and the dangers faced by the students for whom they are responsible. This will be integrated, aligned and considered as part of the whole school or college safeguarding approach
- require **all staff**, on appointment and annually, to read and sign an acceptable use document and thereby acknowledge the College can monitor network and Internet use to help ensure staff and student safety, before providing or continuing to provide access to the College facilities
- require that **all students** agree to comply with the online safety and acceptable use rules when signing an acceptable use letter
- require that **parents / carers** sign and return a consent form for student access to the College facilities

6.3. The **Designated Safeguarding Lead** will:

- act as a named point of contact on all online safeguarding issues and liaising with other members of staff (especially pastoral support staff, school nurses, IT technicians, senior mental health leads and SENCOs) and other agencies on matters of safeguarding that include online and digital safety
- ensure that Online Safety is recognised as art of the College's safeguarding responsibilities and that a co-ordinated approach is implemented
- access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep students safe online
- access regular and appropriate training and support to ensure they recognise the additional risks that students with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation.
- keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate
- work with staff to promote positive online behaviour, e.g. Safer Internet Day. Eg the use of representatives from the Police form in assemblies
- ensure that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches
- maintain records of online safety concerns, as well as actions taken, as part of the College's safeguarding recording mechanisms
- monitor reports of online safety incidents to identify gaps/trends and use this data to update the College response to reflect need
- report to the school leadership team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures
- work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input
- meet regularly with the governor with a lead responsibility for Safeguarding, which includes Online Safety as part of their remit

6.4. The Network Manager will:

- provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures
- implement the College's agreed security measures to ensure that the settings of our IT infrastructure are secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised
- ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team

- report any identified filtering breaches that present the potential for harm to the DSL (or deputy DSLs) and leadership team, as well as, our Internet Service Provider or other services, as appropriate to the circumstances
- ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL (or deputy DSLs), in accordance with the safeguarding procedures
- keep up to date with the relevant legislation as it relates to the security and safety of the technical infrastructure
- use the agreed process for dealing with requests for filtering changes (see Appendix F for more details)

6.5. Curriculum Leaders will (or delegate to responsibility holders as appropriate)**:**

- ensure that students' entitlement to learn, where it is most efficient way to do so, in a digitally literate way is planned into their curriculum
- ensure that classroom teachers, where appropriate to the topic being taught, take advantage of the benefits for learning of using the Internet and mobile devices as a normal approach to teaching and learning
- ensure the prominent display of safe use guidelines, including online 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

6.6. All staff will:

- ensure that they have an up to date awareness of online safety matters and of the current College Online Safety Policy so that they are aware that technology is a significant component of many safeguarding and wellbeing issues and that children are at risk of abuse online as well as face to face and that in many cases abuse will take place concurrently via online channels and in daily life
- ensure that they have read, understood and signed the Network Acceptable Use Agreement
- contribute to the development of online safety policies
- take responsibility for the security of school systems and data to which they have access
- have an awareness of a range of online safety issues and how they may be experienced by the children they interact with
- follow the safeguarding policy and procedures for identifying & reporting any online safety issues
- ensure that all digital communications with students are on a professional level in line with the staff code of conduct
- take personal responsibility for professional development in this area

6.7. Classroom teachers will:

- be aware that they cannot rely on filtering alone to safeguard children. Supervision, classroom management and including reference to safe and responsible use is essential in all teaching
- ensure that the use of all Internet-derived materials by colleagues and students complies with copyright law and acknowledge the source of that material
- ensure that they take advantage of the benefits for learning of using the Internet and mobile devices, where it is the best way to teach a topic

- plan lessons, using the available technology, eg JAMF and Google Classroom, that are organised to prevent behaviour issues arising from digitally facilitated activities that are unrelated to the learning outcomes of lessons
- treat any off task use of technologies as an issue to be followed up, using the College Behaviour for Learning 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 electronic sources of information before accepting its accuracy for inclusion 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. eg their address, phone numbers, College attended, instant messaging / e-mail addresses, full names of friends, full face photographs on social networking sites, photographs taken in an easily identifiable location eg outside an identifiable building or whilst wearing the College logo on clothing
- remind students about safe passwords
- 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 record a digital image or sound recording of another person if it achieves the learning objectives of the lesson AND to check the digital imaging exemptions list, to make sure that we have permission to record digital images of that person, before publishing any images

6.8. Students will:

- be asked to contribute to the development of online safety policies
- follow the College **Online Safety Code of Conduct** (Appendix G)
- read the school acceptable use / Network User agreement / code of conduct and adhere to them
- respect the feelings and rights of others both on and offline, inside and outside of College
- seek help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues
- help keep other students stay safe by reporting the risky online behaviours that they know about

6.9. Parents and carers should support the College by:

- reading the school Online safety and Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate
- supporting our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home
- role modelling safe and appropriate uses of technology and social media for their children
- abiding by the home-school agreement and Acceptable use / network user agreement

- identifying changes in behaviour that could indicate that their child is at risk of harm online
- seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns
- contributing to the development of the school online safety policy.
- using school systems, such as our learning platform, and other network resources, safely and appropriately
- taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- following College guidance on sound recordings, digital and video images taken at school events

6.10. Community Users who access College systems / website as part of the wider College provision will be expected to sign a Community Acceptable use / network user agreement before being provided with access to school systems.

7. Education & Engagement Approaches

7.1. Engagement and Education of Students

- we will establish & embed a progressive online safety curriculum through both dedicated lessons and through the main curriculum to raise awareness regarding the importance of safe and responsible internet use amongst students
- online safety will be included in the PSHEE and Computing programmes of study, covering both safe school and home use
- we will educate students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
- we will teach students to be critically aware of the materials they read and they will be shown how to validate information before accepting its accuracy
- we will use support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches
- students will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability
    - providing support for students and families that have difficulty in accessing written text
    - Displaying the Code of Conduct in all rooms with internet access.
    - Informing students that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Rewarding positive use of technology
- we will provide online safety education and training as part of our transition programmes, including use of Digital Geniuses to support younger students.
- students' input, through our Digital Geniuses, will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation, including the operation of the filtering system and the classroom management software (JAMF, Google Classroom).

7.2. Engagement and Education of Vulnerable Students

- We are aware that some children may be considered to be more vulnerable online due to a range of factors.
- We will ensure that differentiated and ability appropriate online safety education is given, with input from specialist staff as appropriate (e.g. SENCO, Looked after Child Coordinator).

- When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate.

7.3. Engagement and Education of Staff

- The online safety policy will be formally provided to all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- All members of staff will be made aware through the staff code of conduct about the importance and potential consequences of bringing the profession or College into disrepute, or of something that is felt to have undermined confidence in their professional abilities.
- We will recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- We will make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- We will make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- We will highlight useful educational resources and tools which staff should use, according to the age and ability of the students.
- We will ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting students, colleagues or other members of the community.

7.4. Engagement and Education of Parents and Carers

- We recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- We will build a partnership approach to online safety at home and at school. This will include:
    - drawing parents' / carers' attention to the online safety policy and expectations in newsletters, letters and on the College website
    - offering consultation evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. consultation evenings, transition events and sports days
    - parents / carers will be encouraged to role model positive behaviour for their children online
    - requesting that parents / carers read the Online Safety Policy (or a summary of it) and the Network Acceptable Use Agreement, discussing the implications with their children and signing them to state their understanding

8. Reducing Online Risks

- We recognise that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:

    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
    - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the College community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, sound recordings, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

9. Safer Use of Technology

The college is aware that the emergence of machine learning models (commonly known as AI) is an issue that will affect the efficient and safe running of the College as well as the lives and safety of all of our community members. As a result, we are exploring an AI Innovation Team which will work to explore opportunities and threats of AI so that this policy can be updated to reflect the issues that AI represents for us and our community members.

9.1. Classroom Use

- We use a wide range of technology. This includes access to:
    - Computers, laptops and other digital devices
    - Internet which may include search engines and educational websites
        - Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
        - The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
    - Learning platform/intranet
    - Email
    - Digital cameras, web cams and video cameras
- All College owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place. College owned iPads and iPads bought on the College iPad scheme will be protected by device management software (unless, for the iPad purchase scheme, the parent / carer opts out and signs a notice indicating that they are aware of the increased risks whilst their child is at home)
- We use normal search tools, supported by
    - The advance lesson planning of teachers
    - Recommended websites for students to use
    - Lessons on how to use search engines efficiently and safely
- We will ensure that the use of internet-derived materials, by staff and students complies with copyright law and acknowledge the source of information.
- Supervision of students will be appropriate to their age, ability & understanding.

9.2 Managing & Authorising Internet Access

- The school will maintain a current record of all staff and students who are granted access to the school's devices and systems.
- All staff, students and visitors will read and sign the Network Acceptable Use Agreement in order to maintain access to school resources.
- Parents / carers will be asked to read the Network Acceptable Use Agreement for student access and discuss it with their child.
- When considering access for vulnerable members of the community the College will make decisions based on the specific needs and understanding of the student(s).

9.2.1 Filtering & Monitoring

We maintain internet access using appropriate filtering and monitoring systems

9.2.1.1 Decision Making

- Our Senior Leadership Team and Network Manager have ensured that we have age and ability appropriate filtering and monitoring in place, to limit student's exposure to online risks.
- We are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be decided in accordance with the procedure detailed in Appendix F.
- Regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential

9.2.1.2. Filtering

- Education broadband is provided through "TalkStraight".
- We use "Smoothwall", which blocks sites in categories such as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- Our system blocks all sites on the Internet Watch Foundation (IWF) list. Additionally, we block all illegal content, social media and categories such as: gaming; pornography; weapons and violence.
- We work with "TalkStraight" & "Smoothwall" to ensure that our filtering procedure is continually reviewed.
- If students discover unsuitable sites, they will be required to:
  - report the concern immediately to a member of staff & the member of staff will report the concern (including the URL of the site if possible) to the Network Manager and / or DSL
  - the breach will be recorded and escalated as appropriate.
  - depending on the circumstances, parents/carers will be informed of filtering breaches involving their child
- In addition, we provide the following support for our iPad purchase scheme:
  - 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 / carers online safety evening
  - all parents / carers purchasing an iPad through the college scheme are auto enrolled in the college managed internet access service for those devices when outside of College and then given the opportunity to opt out if they so wish. When opting out parents / carers are required to sign a declaration recognising the risks involved in doing so

- Heads of Year / Pastoral Managers regularly monitor suspicious search criteria reports and follow up with the student, in the first instance, and then follow the College Behaviour, Safeguarding and SEND policies as appropriate
- Heads of Year / Pastoral Managers follow the guidance in Appendix E should they have a suspicion that a student could be at particular risk

9.2.1.3. Monitoring

- We will appropriately monitor internet use on all college owned or provided internet enabled devices. This is achieved by:
  - physical monitoring in lessons by teachers
  - electronically recording all internet and web access records on the college network
  - sending weekly reports of suspicious activity to the Head of Year
- If a concern is identified via monitoring approaches we will:
  - investigate via the Head of Year to establish the facts
  - escalate the concern in line with our Behaviour, Safeguarding and SEND policies as appropriate
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

9.3. Managing Personal Data Online

Please see our Data Protection Policy
http://www.heathfieldcc.co.uk/?page_id=1595711

9.4. Security and Management of Information Systems

- The steps we take to ensure the security of our systems, include:
  - Virus protection being updated regularly.
  - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - Not using portable media without specific encryption
  - Portable media will be checked by an anti-virus /malware scan before use.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Regularly checking files held on our network,
  - The appropriate use of unique user logins and strong passwords to access our network.
  - All users are expected to log off or lock their screens/devices if systems are unattended.
  - Further information about technical environment safety and security can be found in our Data Protection & Records management Policies.

9.5. Password Policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- All students are provided with their own unique username and private passwords to access our systems; students are responsible for keeping their password private.
- We require all users to:
  - use strong passwords for access into our system
  - change their passwords immediately if they suspect there has been a security breach

- always keep their password private; users must not share it with others or leave it where others can find it
- not to login as another user at any time

9.6. Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or student's personal information will not be published on our website
- The contact details on the website will be the address, email and telephone number of the College & the work email addresses of members of staff
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.
- We will not publish student / staff photographic images, including videos, or sound recordings without prior permission

9.7. Publishing Images, Videos & Other Recordings Online

- We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) data protection, our Network Acceptable Use Agreement, our code of conduct.

9.8. Managing Electronic Communications, especially email

- Access to our email systems will always take place in accordance with data protection legislation and in line with our Network Acceptable Use Agreement and the code of conduct.
- Excessive social email use can interfere with teaching and learning and will be restricted in response to misuse
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Procedures are in place to ensure that the correct addresses for the intended recipients of bulk E-mails are accurate and up to date at the beginning of each new academic year and whenever College staffing changes

9.8.1. Staff Email

- All members of staff are provided with a specific school email address to use for any official communication.
  - The use of personal email addresses by staff for any official school business is not permitted.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, students and parents / carers
- Any external electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
  - Staff MUST NOT send any emails with attachments that contain student or staff data unless it meets the requirements specified in the data protection policy section 22.2

- College email addresses and other official contact details will not be used for setting up personal social media accounts. They may be used for professional social media accounts.
- 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.
- Staff should never have MS Outlook open on a computer that is connected to a projector or TV, which is turned on.

9.8.2. Student Email

- Students will sign a acceptable use / network user agreement and will receive education regarding safe and appropriate email etiquette before access is permitted
- Students will follow the online safety code of conduct

9.9 Live Stream / Recorded Lessons for Remote Learning

- Live stream is a broad term and can refer to:
    - a platform where the teacher and the children are all linked into a video call/conference and see one another.
    - where only the teacher, or whoever is providing the content, is visible and the children are viewing the content, without being seen themselves.
    - A platform based on wither of the above with the added ability to interact through a live chat function.
- When live streaming lesson or recording them for students to use, all staff will follow the published whole college remote learning protocol. The College will:
    - Consider whether the technology is available to children/families and make alternative arrangements for provision where necessary.
    - Ensure that staff are trained to use the technology.
    - Ensure that children's behaviour/interactions are managed in line with the expectations of the college behaviour policy.
    - Risk assess the platform being used, considering the data protection implications & whether functions, such as live chat, pupil's use of video camera, or the recording of the session, should be disabled or used with further measures to support appropriate use.
    - Only live streaming platforms approved by SLT / the Data Protection Lead will be used.
    - Staff will dress professionally and choose a background that maintains their personal privacy.
    - Pupils should be dressed appropriately e.g. clothes they might wear for a non-uniform day, not pyjamas.
    - Pupils participate in a live stream from a suitable location within their household, choosing a space that avoids interruptions and protects their personal privacy, preferably not their bedroom.
    - Staff behaviour and language will be in line with the staff code of conduct.
    - All other school policies/practices will be followed, especially the safeguarding policy, so that there is no delay in highlighting concerns to the DSL.
- Where the College allows live streams from other providers, the College / College staff will:

- check in advance its suitability and appropriateness, with reference to Data Protection as well as Online Safety.
- consider the safeguarding aspect of how content is being delivered e.g. how children are able to interact, how is content and interactions being monitored/moderated etc.
- ensure that a member of staff will monitor one-off live events along with the interactions/behaviour of the learners taking part.
- check that we are satisfied with the safeguarding policy of the provider(s) if multiple sessions are being run at various times during the college day and, then, monitor some sessions to check they are in accordance with the policy.

- Using video calls for 1:1 sessions with children
  - The school may consider using 1:1 video call sessions to support interventions with children such as mental health support or counselling.
  - These sessions will only be provided where they have been risk assessed and approved by SLT and parental consent given.
  - Where the communication with an individual child does not require the confidentiality of a counselling session, there will be two adults involved; this will provide a safeguard for the adults and the children.
  - These two adults will either be physically in the same room, with the second member of staff being referenced to the child so that they are aware, or, where staff are working remotely, they will both be within the virtual room of the meeting.
  - In either case both adults will be present before the child is admitted to the online session

10. Use of Video Conferencing, Webcam or Similar Technologies (eg Skype)

The school acknowledges that video conferencing is a challenging activity with a wide range of learning benefits. We do not use dedicated video conferencing equipment; we only use generic commercial software such as Skype and FaceTime. We will ensure that external video conference opportunities are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure by consulting Network Services, the Online Safety Co-ordinator or the Data Protection Lead in advance of using them with students.

10.1. Guidance regarding users

- We will ensure that parents and carers have given express consent for their children to take part in video conferences
- Students will ask permission from a teacher before making or answering a video conference call or message.
- Video conferencing will be supervised appropriately for the students' age and ability

10.2. Content

- When recording a video conference lesson, written consent is required from all participants.
- Recorded material will be stored securely.
- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site, the school will check that they are delivering material that is appropriate for the class.

11. The College Learning Platform

- The Senior Leadership Team will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular message and communication tools and publishing facilities.

- Only current members of staff, students and parents / carers will have access to the LP.
- When staff and/or students leave the setting, their account will be disabled or transferred to their new establishment.
- Students/staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, students' etc. leave the school their account or rights to specific school areas will be disabled or (if appropriate) transferred to their new establishment.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - If the user does not comply, the material will be removed by the site administrator.
  - Access to the LP for the user may be suspended.
  - The user will need to discuss the issues with a member of leadership before reinstatement.
  - A student's parents/carers may be informed.
  - If the content is illegal, we will respond in line with existing child protection procedures.
- A visitor may be invited onto the LP by a member of the leadership. In this instance there may be an agreed focus or a limited time slot.
- Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

12. Management of Applications (apps) Used to Record Children's Progress

- We use SIMS (our School Information Management System) to track students' progress and share appropriate information with parents and carers.
- The Head Teacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard student's data:
  - Only College approved devices will be used for apps that record and store students' personal details, attainment or photographs.
  - Staff owned mobile phones will not be used to access or upload content to any apps which record and store students' personal details, attainment or images
  - Staff owned tablet and other computers can be used to access and edit data only if:
    - They are using the security protected SIMS teacher app (the iPad app version of our School Information Management System)
    - They are using card reader devices, when accessing the College Network, to ensure that there is increased security on the device
  - Portable storage devices can only be used on devices connected to the College network if they are appropriately encrypted, to reduce the risk of a data security breach, in the event of loss or theft.
  - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.

- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access to parent apps; for example, not sharing passwords, sound recordings, videos or images.

13. Social Media

- Safe and responsible use of social media applies to all members of the Heathfield Community College community
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messaging services.
- All members of Heathfield Community College are:
  - expected to engage in social media positively, safely and responsibly
  - advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- We will control learner and staff access to social media. Access will be blocked by default to all students.

13.1 Staff Personal Use of Social Media

- Access for staff is as follows:
  - use during directed time is permitted for professional uses.
  - use during directed time for personal use *is not* permitted.
  - inappropriate or excessive use of social media during working hours or whilst using college devices may result in disciplinary or legal action.
- Staff members participating in social media for work purposes are expected to demonstrate the same high standards of behaviour as when using other media or giving public presentations on behalf of Heathfield Community College
- Concerns regarding the online conduct of any member of Heathfield Community College on social media, should be reported as per the flow charts in Appendix E.
- The safe and responsible use of social networking, social media and personal publishing sites will be raised as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy and as part of our acceptable use policy.
- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
  - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will include (but is not limited to):
  - Setting the privacy levels of their personal sites.
  - Being aware of location sharing services.
  - Opting out of public listings on social networking sites.
  - Logging out of accounts after use.
  - Keeping passwords safe and confidential.
  - Ensuring staff do not represent their personal views as that of posts that relate to the College
- Members of staff are encouraged not to identify themselves as employees of Heathfield Community College on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.

- All members of staff are encouraged to carefully consider the information, including text sound recordings, videos and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Senior Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

13.2. Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this, will be discussed with the DSL (or deputies) and/or the headteacher.
    - If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.
- Staff will not use personal social media accounts to contact learners or parents / carers, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the headteacher.
- Any communication from learners and parents / carers received on personal social media accounts will be reported to the DSL (or deputies).

13.3 Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.
- Any concerns regarding learners use of social media will be dealt with in accordance with this and other policies, including anti-bullying and behaviour.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications.
    - How to report concerns both within the setting and externally.

13.4 College Official Use of Social Media

- Heathfield Community College official social media channels are:
    - Twitter: @heathfield_cc
    - Youtube: HeathfieldCollege (https://www.youtube.com/channel/UCXkS4nHVjPRsHOuuJJx2sjQ)
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.

    - The official use of social media as a communication tool has been formally risk assessed and approved by the head teacher.
    - Designated leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
    - Staff use College provided email addresses to register for and manage any official social media channels.
    - Official social media sites are suitably protected and, where possible, linked from our website (for example, HeathfieldTV is hosted as a website page but the films are stored on YouTube).
- Official social media use will be conducted in line with existing policies, including: anti-bullying, image/camera use, data protection, confidentiality and child protection.
    - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
    - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
    - Any official social media activity involving learners will be moderated in line with the College procedures.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

13.5 Staff Professional Use of Social Media on behalf of the College

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Sign our Acceptable Use Agreement.
    - Always be professional and aware they are an ambassador for the setting.
    - Disclose their official role and position but make it clear that they do not necessarily speak on behalf of the setting.
    - Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Ensure that they have appropriate consent before sharing images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, learners, parents and carers.

13.6 Creation of accounts on behalf of Heathfield Community College

- Prior to creating a site, careful consideration must be given to the purposes for using social media and whether the overall investment is likely to be worthwhile for achieving the proposed pedagogical outcome.

- The proposed audience and level of interactive engagement with the site, for example whether pupils, school staff or members of the public will be able to contribute content to the site, must be discussed with the staff members Line Manager and agreed by the designated member of the Senior Leadership Team.
- There must be a careful exit strategy and a clear plan from the outset about how long the site will last. It must not be neglected, creating a potential risk to the school's brand and image.
- Staff members must ensure that the sites they create or contribute to for work purposes conform to the *Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services* (Home Office Task Force on Child Protection on the Internet, updated 2010) (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251456/industry_guidance_social_networking.pdf)
- Staff members must also ensure that the webspace they create on third party sites comply with the site owner's minimum age requirements (this is often set at 13 years). Staff members must also consider the ramifications and possibilities of children under the minimum age gaining access to the site.
- Care must be taken to ensure that content is suitable for the target age group and contributors or 'friends' to the site are vetted.
- Heathfield Community College social media sites can be created only by or on behalf of the school. Site administrators and moderators must be Heathfield Community College employees or other authorised people.
- Approval for creation of sites for work purposes, whether hosted by the school or hosted by a third party such as a social networking site, must be obtained from the staff member's line manager and the member of Senior Leadership Team responsible.
- Staff members must complete the Social Media Site Creation Approval Form (Appendix I) and forward it to the member of Senior Leadership Team responsible before site creation.
- Be aware that the content or site may attract media attention. All media enquiries must be forwarded to the head teacher immediately. Staff members must not communicate with the media without the advice or approval of the head teacher.
- Staff members must not disclose information, make commitments or engage in activities on behalf of Heathfield Community College or the County Council without authorisation.
- Information provided must be worthwhile and accurate; remember what is published on the site will reflect on the school's or County Council's image, reputation and services.
- Stay within the law and be aware that child protection, privacy, data protection, libel, defamation, harassment and copyright law apply to the content of social media.
- Staff members must respect their audience and be sensitive in the tone of language used and when discussing topics that others may find controversial or objectionable.
- Permission must be sought from the relevant people before citing or referencing their work or referencing service providers, partners or other agencies.
- Personal opinions should not be expressed on official sites.
- Any images and/or naming of students must only be published with agreement from parents/carers. Permission is sought annually as part of the whole

College Data Collection. In order to check the list staff should contact the Data Office.

- Careful consideration must be given to the level of engagement of contributors – for example whether users will be able to add their own text or comments or upload images. When other contributors wish to add content approval from the moderator must be sought to ensure all content meets the Online Safety Policy.
- Sites created for and contributed to by pupils must have the strongest privacy settings to prevent breaches of confidentiality. Pupils and other participants in sites must not be able to be identified.
- The content and postings in Heathfield Community College-hosted sites must be moderated. Moderation is the responsibility of the team that sets up or initiates the site.
- The team must designate at least two approved Administrators whose role it is to review and moderate the content, including not posting or removal of comments which breach the Terms of Use and House Rules. It is important that there are enough approved moderators to provide cover during leave and absences so that the site continues to be moderated.
- For third-party-hosted sites such as social networking sites used for work purposes, the responsibility for protection and intervention lies first with the host site itself. However, different sites may have different models of intervention and it is ultimately the responsibility of the staff member creating the site to plan for and implement additional intervention, for example in the case of content raising child safeguarding concerns or comments likely to cause offence. At Heathfield Community College an internal Moderator must be agreed to manage the content of the social networking site and ensure all content abides by the College Online Safety Policy.
- Sites that are viewed and followed but not contributed to are more likely to be agreed.
- Where possible contribution forums should take place on the College Learning Platform, which is accessible by logged in users only.
- Moderation and management of external accounts is a time consuming job. Ensuring that the impact of the account is worthwhile is vital to allow for success and to ensure that the methods of communication remain safe.
- It is the responsibility of the administrators of the site to update the relevant member of the Senior Leadership Team to any changes that are made to the moderation, or if the site is to be closed.

14. iPads, Personal Devices and Mobile Phones

We recognise that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but technologies need to be used safely and appropriately.

14.1 General:

- All use of iPads, other personal devices and mobile phones will take place in accordance with the law and other appropriate college policies, eg Safeguarding, Behaviour, Data Protection.
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. We accept no responsibility for the loss, theft or damage of such items. Nor will we accept responsibility for any adverse health effects caused by any such devices either potential or actual.

    - All members of our community are advised to take steps to protect their mobile phones or devices from loss, theft or damage.
    - All members of our community are advised to use strong passwords/pin numbers to ensure that unauthorised usage of their device is prevented; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones, iPads and other personal devices are not permitted to be used in certain areas within the school site or particular school activities such as changing rooms & toilets.
- The sending of abusive or inappropriate messages or content via iPads, mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the Behaviour for Learning policy.
- Members of staff will be issued with a school/work phone number and email address where contact with students or parents/carers is required.
- All members of our community are advised to take the recommended steps to protect their mobile phones or devices from loss, theft or damage, for example:
    - secure passwords / PIN numbers
    - passwords and pin numbers should be kept confidential
    - lock the screen when using the device
    - not sharing devices
- All members of our community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene College policies.
- College issued mobile phones and devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies (for example the anti-bullying and social media polices).
    - College issued mobile phones and devices used for communication with parents / carers and students are protected via a passcode/password/pin and must only be accessed and used by members of staff.

14.2 Students:

- Students will be educated regarding the safe and appropriate use of personal devices (eg smart watches) and mobile phones and will be made aware of boundaries and consequences.
- All use of mobile phones, iPads and personal devices by children will take place in accordance with the acceptable use agreement and only at the approved hours.
    - Mobile phones, iPads and other personal devices are not allowed to be used by students in their free time at College between 8.37am and 3.05pm.
    - Mobile phones will not be used by students during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
    - Student's iPads & phones that are being used as part of a curriculum based activity with consent from a member of staff will be placed on their desk with the screen facing down unless they have been told otherwise by the member of staff.
    - Student's personal mobile phones, and other personal devices, unless otherwise directed by a member of staff, will be switched to silent and kept out of sight during lessons and while moving between lessons.
- Mobile phones and personal devices (eg smart watches) must not be taken into examinations.
    - Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in

the withdrawal from either that examination or all examinations as directed by the awarding body

- If a student needs to contact his/her parents/carers they will be allowed:
  - to do so if the member of staff judges that the reason for doing so & to use a College telephone only
- If a student breaches the College policy, then the phone or device will be confiscated and will be held in a secure place.
  - School staff may confiscate a student's mobile phone or device if they believe it is being used in contravention of the College's policies: https://www.gov.uk/government/publications/searching-screening-and-confiscation
  - Mobile phones and devices will only be released in accordance with the College policy. This depends on the reason for the confiscation. In most cases the device will be released to the student at the end of the College day. (In escalated cases confiscation can be for longer periods and the device may only be released to a parent or carer).
  - Students mobile phones or devices may be searched by a Head of Year or a member of the leadership team, EITHER with the consent of the student or a parent / carer OR in line with the government guidance on searching. Content may be deleted or requested to be deleted, if it contravenes our policies. In some cases copies of content may be taken as evidence or handed to the police.

14.3 Staff:

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.
- Staff will be advised to:
  - Keep mobile phones and personal devices in a safe and secure place.
  - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
  - Ensure that Bluetooth or other forms of communication (such as 'airdrop'), which identify the owner of the device to students, are hidden or disabled during lesson times on their own personal devices.
  - Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting students or parents and carers.
  - Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputies) and/or Head Teacher.
- Staff use of personal devices:
  - Staff will only take photos or videos of students when it is necessary for the functioning of the College or necessary for a learning purpose.
  - Where possible staff will only use college-provided equipment for taking photos or videos of students, not their own personal devices
  - Where it is not possible to avoid using a personal device for taking photos or videos of students, staff should transfer the images to the College Network within 24 hours, permanently deleting copies from the personal device AND any cloud service where they may have automatically been backed up.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy. See Appendix E for the escalation procedure for illegal activity by members of staff.

14.4 Visitors:

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the Acceptable use / network user agreement and other associated policies, such as: anti-bullying, behaviour, child protection & data protection.
- We will ensure appropriate signage and information is displayed and provided to inform all visitors to not take digital images or videos whilst on the College site.
- All daytime visitors are asked to consent to not taking digital images, unless they have the express consent of the Head Teacher, before being allowed further into the College buildings than the main reception.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputies) or Head Teacher of any breaches of our policy.

14.5 Officially provided mobile phones and devices:

- Members of staff will be issued with a work phone number and email address, where contact with students or parents/ carers is required.
- Mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- Mobile phones and devices will always be used in accordance with the Acceptable use / network user agreement and other relevant policies eg Safeguarding, Data Protection.

15. Responding to Online Safety Incidents and Concerns

15.1 General:

- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, sound recordings, images or videos online which cause harm, distress or offence to any other members of the school community.
- All members of the community will be made aware that online safety concerns are safeguarding concerns
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing nudes and semi nudes (or sexting) by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting / sharing nudes and semi nudes), cyberbullying and illegal content (see Appendix E).
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
- Students, parents / carers and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and students to work in partnership to resolve online safety issues.
- When investigating online safety incidents, we will NOT:
    - View any images suspected of being youth produced sexual imagery, unless there is a clear need or reason to do so in order to safeguard the child or young person. If it is necessary to view the image(s) in order to safeguard the child or young person, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.

        - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- Safeguarding concerns and incidents should be reported to Single Point of Access, in line with East Sussex Safeguarding and Child Protection model policy.
    - If we are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice from the Standards and Learning Effectiveness Service Safeguarding Team.
    - Where there is suspicion that illegal activity has taken place, we will contact the Standards and Learning Effectiveness Service or Sussex Police using 101, or 999 if there is immediate danger or risk of harm.
    - If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or Head Teacher will speak with Sussex Police and/or the Standards and Learning Effectiveness Service first to ensure that potential investigations are not compromised.
- Complaints will be dealt with in line with the College's complaints policy or the safeguarding reporting procedures, as appropriate (See Appendix E).

15.2 Concerns about Students' Welfare

- See flow chart in Appendix E for our reporting procedures

15.3 Staff Misuse

- See flow chart in Appendix E

16. Procedures for Responding to Specific Online Incidents or Concerns

We will follow the advice as set out in the non-statutory UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people. Flow charts containing guidance on how to respond to an online safety incident can be found in **Appendix E.** This includes contains flow charts for guidance on:

- how we will respond to issues relating to illegal activity, material and content;
- 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.

16.1. Online Sexual Violence and Sexual Harassment between Children

- We have accessed and understood the "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' (KCSiE) 2021.
- We recognise that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
- Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Safeguarding policy.
- We recognise that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local

community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

- We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our Computing, PSHE and PRE curriculums.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our Safeguarding policy.
    - If content is contained on students' electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all students involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour for learning policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police.
    - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
    - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Sussex Police first to ensure that investigations are not compromised.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate

16.2. Youth Produced Sexual Imagery ("Sexting") or "Sharing Nudes and semi nudes"

- We recognise youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on/off site or using setting provided or personal equipment.

- We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
        - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request students to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - Act in accordance with our Safeguarding policy and the relevant East Sussex Safeguarding Child Board's procedures.
    - Store the device securely.
        - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
    - Carry out a risk assessment which considers any vulnerability of students involved; including carrying out relevant checks with other agencies.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - Make a referral to Children's Social Care and/or the Police, as appropriate.
    - Provide the necessary safeguards and support for students, such as offering counselling or pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour for learning policy but taking care not to further traumatise victims where possible.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
    - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

16.3. Online Child Sexual Abuse and Exploitation (including child criminal exploitation and County Lines)

- We will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- We recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for students, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

- We will ensure that the 'Click CEOP' report button is visible and available to students and other members of our community on our online safety website page.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our Safeguarding policy and the relevant East Sussex Safeguarding Child Board's procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Children's Social Care (if required/ appropriate) and immediately inform the police via 101 (or 999 if a child is at immediate risk)
    - Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for students, such as, offering pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible, students will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Standards and Learning Effectiveness Service and/or Police.
- If students at other settings are believed to have been targeted, the DSL (or deputy) will seek support from the Police and/or the Standards and Learning Effectiveness Service first to ensure that potential investigations are not compromised.

16.4. Indecent Images of Children (IIOC)

- We will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police and/or the Standards and Learning Effectiveness Service.
- If made aware of IIOC, we will:
    - Act in accordance with our Safeguarding policy and the relevant East Sussex Safeguarding Child Boards procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Sussex police or the LADO.

- If made aware that a member of staff or a student has been inadvertently exposed to indecent images of children, we will:
    - Ensure that the DSL (or deputy DSL) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
    - Ensure that the DSL (or deputy DSL) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
    - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
    - Ensure that the Head Teacher is informed in line with our managing allegations against staff policy.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
    - Quarantine any devices until police advice has been sought.

16.5. Cyberbullying & Cybercrime

- All staff understand that children are capable of abusing their peers online. Cyberbullying, along with all other forms of bullying, will not be tolerated.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy, which can be found on the policies page of the college website: http://www.heathfieldcc.co.uk/?page_id=410816
- We will ensure that all members of the community are aware that children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.
- If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), will consider referring into the Cyber Choices programme.
- We will seek advice from Cyber Choices, 'NPCC- When to call the Police' and National Cyber Security Centre.

16.6. Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated and will be responded to in line with existing policies, including anti-bullying and behaviour for learning.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.

- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy DSL) will obtain advice through the Standards and Learning Effectiveness Service and/or Sussex Police.

16.7. Radicalisation, Online Extremism and Online Hate

- Please see separate "Prevent" policy
- We will ensure that all members of the community are made aware of the role of the internet as a tool for radicalisation
- We will take all reasonable precautions to ensure that students and staff are safe from terrorist and extremist material when accessing the internet on site. Please the section 10.2.1 on how we filter and monitor internet usage at the College
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) will be informed immediately, and action will be taken in line with our Safeguarding and Prevent policies.
- If we are concerned that member of staff may be at risk of radicalisation online, the Head Teacher will be informed immediately, and action will be taken in line with the Safeguarding, Prevent and managing allegations policies.

Appendix A

	Commercial	Aggressive	Sexual	Values
Content Child as recipient	Advertising Spam Copyright Sponsorship	Violent content Hateful Content	Pornographic content Unwelcome sexual comments	Bias Racist and extremist content Misleading information/advice Body image and self esteem Distressing or offensive content
Contact Child as participant	Tracking Phishing Harvesting Sharing personal information	Being bullied, harassed or stalked	Meeting strangers Grooming Online Child Sexual Exploitation	Self-harm and suicide Unwelcome persuasions Grooming for extremism
Conduct Child as actor	Illegal downloading Hacking Privacy Copyright	Bullying, harassing or stalking others	Creating and uploading inappropriate or illegal content (including "sexting") Unhealthy/inappropriate sexual relationships Child on child sexualised or harmful behaviour	Providing misleading information and advice Encouraging others to take risks online Sharing extremist views Problematic Internet Use or Plagiarism
Commerce Child as actor	Gambling Financial scams Inappropriate advertising	Bullying, harassing or stalking others	Financially benefitting from pornographic or other illegal content	"Addiction" Encouraging others to take risks online

Appendix B

What is and what is not allowed in College and when

Communication Technologies	Staff & other adults			Students			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with permission
Mobile phones may be brought to school	✓				✓		
Use of mobile phones in lessons		✓					✓
Use of mobile phones in social time[1]	✓			✓			
Taking photos on mobile phones / cameras		✓				✓	
Use of tablets	✓					✓	
Use of mobile gaming devices		✓		✓			
Use of personal email addresses in school, or on school network		✓		✓			
Use of school email for personal emails		✓		✓			
Use of messaging apps		✓		✓			
Use of social media		✓		✓[2]			
Use of blogs		✓					✓

[1] Social time for students is any time out of lessons between 8:37pm and 3:05pm

[2] 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.

Appendix C

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 l 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 & now GDPR & the Data Protection Act 2018**. 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 enacted to 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 own gratification. 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 Criminal Justice Act 2003**. Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.
- **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 & Education Act 2011**. Empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the College site and empowers the head teacher to impose disciplinary penalties on members of staff for inappropriate behaviour. E.g. online bullying or online safety incidents which may take place outside of the school/academy but is linked to member of the school/academy. The 2011 Act gives powers with regard to the searching for and of electronic devices and the deletion of data. 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. Actions that can be taken are restricted to issues covered by this policy, the behaviour policy and the antibullying policy and to such extent as is reasonable. We will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that has taken place out of school. http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted.
- **The Criminal Justice & Immigration Act 2008**. Section 63 makes it an offence to possess "extreme pornographic images". 63 (6) identifies that such images must be considered to be "grossly offensive, disgusting or otherwise obscene". Section 63 (7) includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties for possession of extreme pornographic images can be up to 3 years imprisonment.
- **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
- **Criminal Justice and Courts Bill 2015 (section 33) - Revenge Pornography.** Section 33 makes it an offence to share private, sexual materials, either photos or videos, of another person without their consent and with the purpose of causing embarrassment

or distress, often referred to as “revenge porn”. The offence applies both online and offline and to images which are shared electronically or in a more traditional way so includes the uploading of images on the internet, sharing by text and e-mail, or showing someone a physical or electronic image. This offence can result in imprisonment for up to 2 years. Sending images of this kind may, depending on the circumstances, also be an offence under the Communications Act 2003 or the Malicious Communications Act 1988. Repeated behaviour may be an offence under the Protection from Harassment Act 1997. This law and the term “revenge porn” only applies to images or videos of those over 18. For more information, access: Revenge Porn Helpline

- **Serious Crimes Act 2015.** Part 5 (Protection of Children) section 67 makes it a criminal offence for an adult (person aged over 18) to send a child (under 16) sexualised communications or sends communications intended to elicit a sexual communications. The offence is committed whether or not the child communicates with the adult. Penalties for sexual communication with a child can be up to 2 years imprisonment. Section 69 makes it an offence to be in possession of paedophile manuals, information or guides (physically or electronically) which provide advice or guidance on sexually abusing children. Penalties for possession of such content can be up to 3 years imprisonment. This law also removed references in existing legislation to terms such as child prostitution and child pornography and identified that this should be viewed to be child sexual exploitation
- **‘Keeping Children Safe in Education (KCSiE)’ 2021.** This is statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014 and the Non-Maintained Special Schools (England) Regulations 2015.

Appendix D

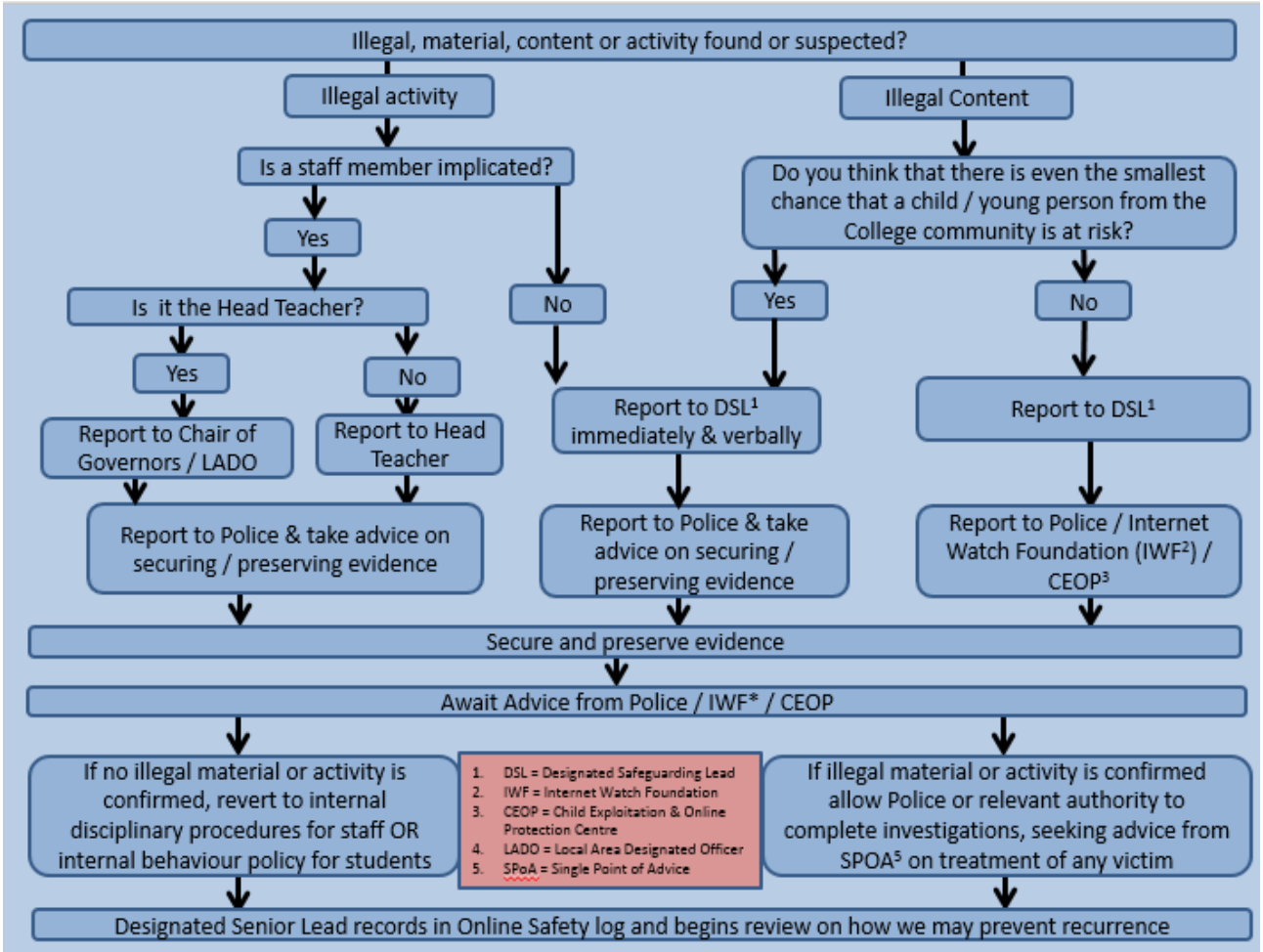
What Constitutes Unsafe / Unacceptable Usage of New Technologies?

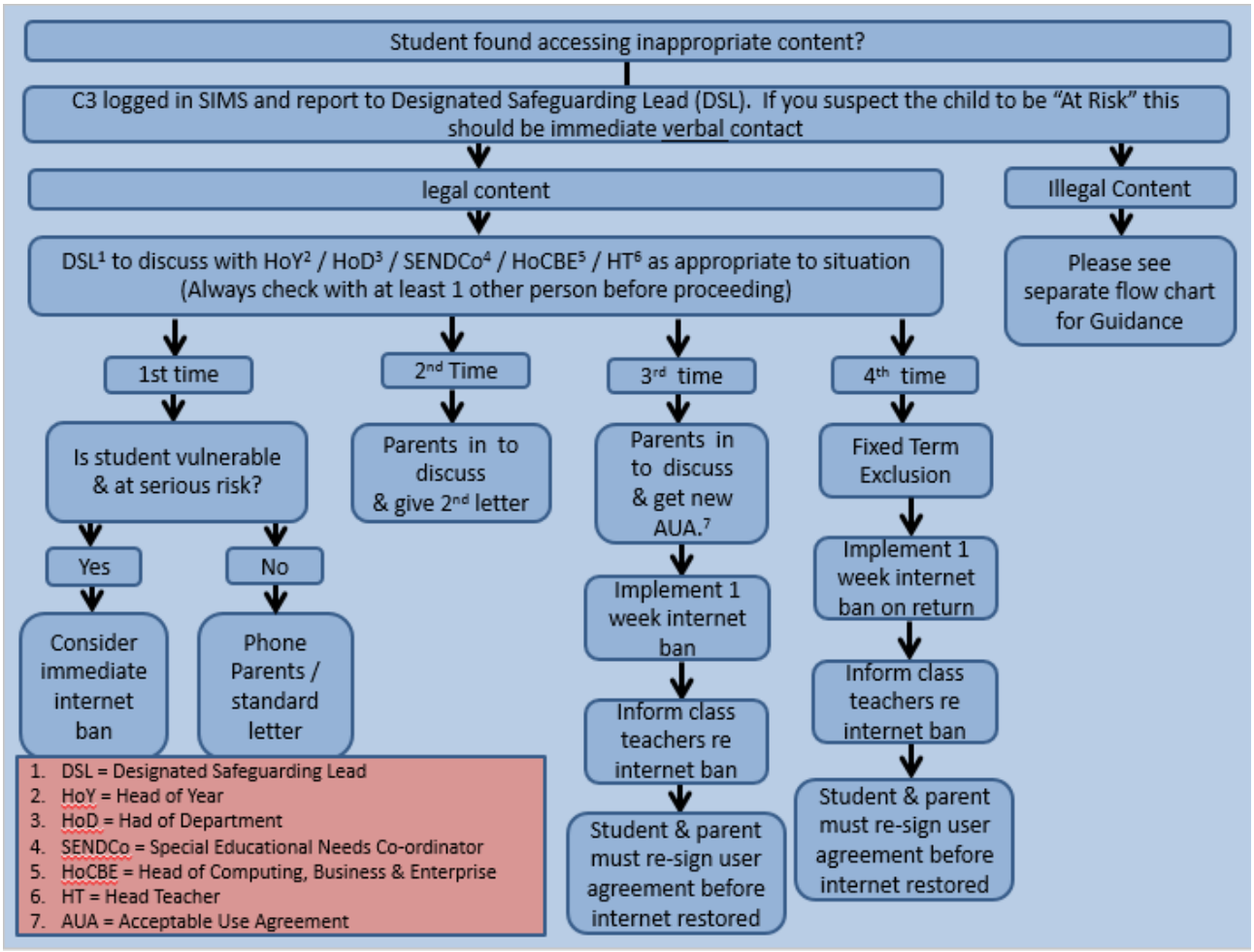
The following applies equally to staff use as it does to students' use of new technologies. It is **NOT an exhaustive list** and is presented purely for guidance:

- 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 data or other inappropriate content
- 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 sound recordings, 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
- Downloading / uploading large files that hinders others' use of the internet)
- File sharing of other people's intellectual property
- Excessive use of "screen time" (impacting on social and emotional development)
- Accessing, publishing, sharing, distributing & playing of unsuitable video / games
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Inappropriate use of social 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 TWO working days 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

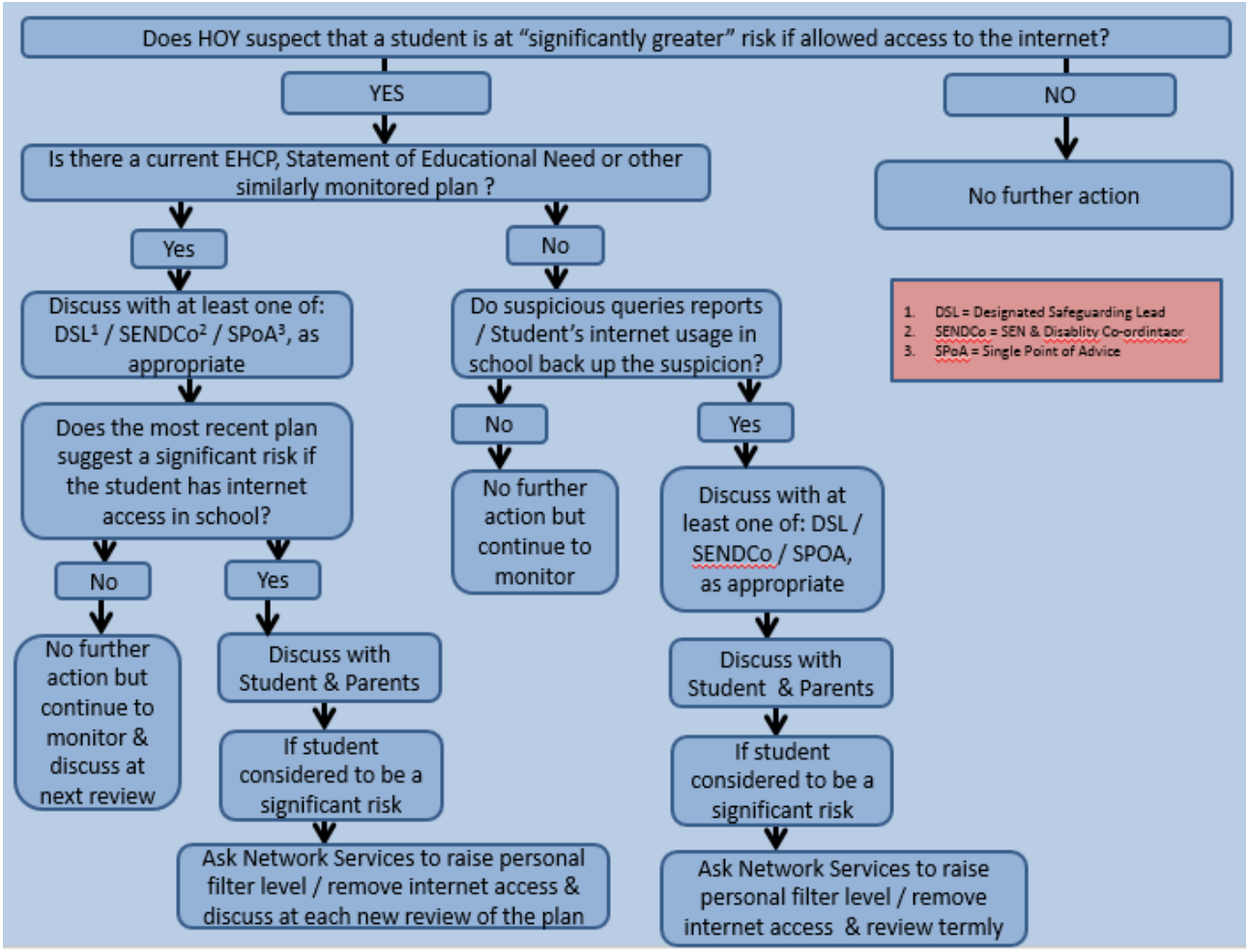
Appendix E: Procedures for:

- Reporting illegal activity
- Reporting illegal content
- Students found accessing inappropriate content
- Protecting more vulnerable students from the dangers of the internet




Student found accessing inappropriate content?
C3 logged in SIMS and report to Designated Safeguarding Lead (DSL). If you suspect the child to be "At Risk" this should be immediate verbal contact
legal content
Illegal Content
DSL[1] to discuss with HoY[2] / HoD[3] / SENDCo[4] / HoCBE[5] / HT[6] 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 AUA.[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. DSL = Designated Safeguarding Lead
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. AUA = Acceptable Use Agreement

Appendix E Cont'd



Appendix F

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.
    a. All requests will be considered after reviewing the site for potential risks
    b. Any sites about which there is uncertainty with regards to the risks that they posed will be discussed with the DSL before agreeing to unblock them.

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 Head of Network Services for implementation.

Appendix G

The Online Safety Student Code of Conduct

Online Safety Code of Conduct

Students Will:

☺	Keep ALL passwords private & change it immediately if anyone else finds out	
☺	Respect other people's opinions and beliefs, even if you disagree	
☺	Respect other people's work and devices, keeping to your own device / computer	
☺	Respect other people's learning in both classroom & remote learning Lessons	
☺	Respect the College's and other people's equipment	
☺	If you are ever made to feel scared or uncomfortable: use the online reporting method for the website you are using; tell a teacher; AND use the "report abuse" button on the College Online Safety website page	
☺	Always keep your own and other people's information private eg name, address, telephone numbers, school, pets, close up photos or videos	
☺	Only reply to messages from people you know	
☺	Always credit the source of other people's work when you use it in your own work	

Students will:

✗	NOT tell anyone your network password	
✗	NOT reply to nasty messages. (Instead: keep a copy of it as evidence; tell a teacher; use the online reporting for the website you are on; AND use the "report abuse" button on the College website.)	
✗	NOT show or upload online photos or videos of other people without asking for their permission first	
✗	NOT show other people photos or videos of yourself, including "live streaming", without asking an adult first	
✗	NOT publish personal details or photos or videos that identify other people eg no names, addresses, phone numbers, school name, pets, portrait photos with a name	
✗	NOT agree to meet an online friend without checking with an adult first	
✗	NOT be rude, offensive, bully or harass other people eg in a message, eg on an online service, eg in a remote "live" lesson	
✗	NOT use a computer / mobile or portable device in a lesson for anything other than a learning activity set by the teacher	
✗	NOT access, read, alter or delete the work of other people	
✗	NOT search for, create, share or view inappropriate material	
✗	NOT play electronic / online games whilst in College, especially not in lessons, unless asked to do so by a teacher	
✗	NOT attempt to install or attempt to use non network executable files, programs or viruses on the network	
✗	NOT attempt to access the operational files of the network, classroom workstations or iPads	
✗	NOT attempt to install, attempt to use or create your own network executable files, programs, viruses or other malicious files on the college network	
✗	NOT use VPN, proxies or similar tools to evade the protections provided by the College Network, Wifi and iPad management system.	

Appendix H

Examples of how students can take responsibility for keeping themselves and others safe whilst online include but cannot be restricted to:

- 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 sound recordings, 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
- increasingly take responsibility for keeping themselves and others safe online
- increasingly take responsibility for their own awareness and learning about the opportunities and risks posed by new and emerging technologies
- increasingly assess the personal risks of using any particular technology, and behave safely and responsibly to limit those risks.

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 less than 2 working days
- 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

Appendix I

Social Media Application Form

Please complete this form after reading the College Social Media Policy and in discussion with your line manager.

Responsible Team & Personnel	
Department / Team	
Author of Site	
Authors Line Manager	
Purpose of the Social Media Site	
What are the aims of this site?	
What is the proposed content of the site?	
Why is the chosen Social Media method appropriate to the aims and content?	
Proposed Audience of the Site	
☐ Students of Heathfield Community College **[age range]** ☐ Heathfield Community College staff ☐ Students family members ☐ Members of the public ☐ External organisations ☐ Others **[add details]**	
Proposed Contributors to the Site	
☐ Students of Heathfield Community College **[age range]** ☐ Heathfield Community College staff ☐ Students family members ☐ Members of the public ☐ External organisations ☐ Others **[add details]**	
Administration of the Site	
Name of administrator	
Name of 2nd administrator	
Name of moderator	
Name of 2nd moderator	
Where will the site be hosted?	☐ On the school network ☐ Externally **[Specify]**
Proposed date going live	
Proposed date for closure	
Permissions & Security	

If contributors include students how do you propose to inform and obtain consent of parents / carers or responsible adults?		
What security measures will you take to prevent unwanted individuals from contributing to the site?		
Approval & Recognition		
Moderator ***I will take responsibility for checking the content of the website and have read the Social Media Policy and e-safety policy and I understand the flow charts on what I have to do if I find illegal or inappropriate materials.***	***Name***	
	Signature	
	Date	
Line Manager ***I approved this application form and are happy that the proposed site meets the College Social Media Policy.***	***Name***	
	Signature	
	Date	
SLT Line Manager ***I approved this application and considered the aims and content and that the site can use the College branding.***	***Name***	
	Signature	
	Date	
Copy to SLT Link (Digital Pedagogy) ***Online Safety Co-ordinator***	***Name***	
	Signature	
	Date	