Callington Community College

DIGITAL TECHNOLOGY USE & ONLINE SAFETY POLICY

September 2022

Version	Date	Review Date
September 2022	September 2022	September 2023
Originator: R Taylor	Authorised by CCC Governors:	

Callington Community College
Digital Technology Use & Online Safety Policy

Development / Monitoring / Review of this Policy

This Online Safety policy and associated AUAs has been developed by a working group made up of:

- *Senior Leaders*
- *Online Safety Officer*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors*
- *Students*

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Local Governing Board on:	5 October 2022
The implementation of this Online safety policy will be monitored by the:	*Online Safety lead (Rob Taylor), Designated Safeguarding Lead (Gemma Parker) and the Leadership Team.*
Monitoring will take place at regular intervals:	*Half-termly as part of the Safeguarding concern analysis on a block-by-block basis.*
The Safeguarding Governor will receive a report on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Termly*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:	*Next review date September 2023*
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	*MARU, Police, LADO (as appropriate)*

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the College site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place outside of the College, but is linked to membership of the College. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Overview of policy

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including: web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole.

This policy has been written taking into consideration all statutory guidance with particular reference to:

DfE guidance – Searching, Screening and Confiscation (July 2022)
DfE guidance - Behaviour in Schools (July 2022)
DfE guidance – Teaching Online Safety in Schools (2019)
DfE guidance – Sharing nudes and semi-nudes: advice for education settings working with children and young people (2020)
SWGfL – Online Safety Policy for Schools (Sept 2022)
Keeping Children Safe in Education 2022

This policy is in keeping with the College's Right Respecting ethos. It incorporates a number of aspects of using ICT within and outside the College including:

1. **Online Safety in the curriculum**
2. **The code of conduct for the responsible use of digital technology**
   - 2.1. Using our College network
   - 2.2. Bringing own devices
   - 2.3. Acceptable use of all digital devices
   - 2.4. Data protection when using digital technology
   - 2.5. Use of social networking sites and chatrooms
   - 2.6. Communication between Staff, Students and Parents and carers
   - 2.7. Distance learning – Safeguarding in online lessons
3. Using Images of Children Policy
4. Technical Infrastructure/equipment

The use of technology has become integral to many of our lives and has certainly become part of the way we communicate and access information. Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in Online Safety is therefore an essential part of the College's Online Safety provision. Children and young people need the help and support of the College to recognise and avoid Online Safety risks and build their resilience.

Appendix 5.2 outlines the roles and responsibilities of students and staff concerning Online Safety and the use of digital technology. Appendix 5.1 outlines the consequences and sanctions associated with breaches of this policy. All staff, students, parents and volunteers or visitors using our ICT systems are required to sign Acceptable Use Policies (AUAs) in order to use digital technologies.

Online Safety team

Online Safety developments and the Online Safety policies will be reviewed and monitored by our College Online Safety team. This team includes the College Online Safety Officer, Designated Safeguarding lead, Safeguarding Governor, Safeguarding team members and members of the College leadership team. There is also significant consultation and input from the PSHE Subject Leader, the Computing Department subject leader and Network manager.

Monitoring and Review

The policy is to be reviewed annually, but also in response to new technologies being introduced or incidents that have taken place as part of an Online Safety review cycle. The safeguarding committee monitor the impact of the policy using evidence from self-evaluation as identified below.

Online Safety Self-evaluation

In order to understand the issues within our school community we will gather and use a range of evidence to inform development of our practice, planning for the curriculum and planned professional development. Self-evaluation is conducted through many channels which can include:

- Logs of reported incidents
- Network monitoring data from our IT technical team
- Consultation with pupils, parents / carers, and staff including non-teaching staff
- The South West Grid for Learning "360° safe" online tool will also be used as a benchmark to enable us to monitor our development towards more effective practice.

1 Online Safety and the Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of ICT across the curriculum.

KCSIE suggests that Online Safety issues can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit. Students should be reminded of the AUA they have signed.

- It is accepted that from time-to-time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need, giving 24 hour's notice.

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

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

2 The code of conduct for the responsible use of digital technology

Digital Mobile devices include mobile phones, iPods, mp3 players, iPads, tablets and all similar devices

The College recognises the advantages of digital technology for staff and students as a means of communication and as a learning tool. However, this technology is open to abuse leading to the invasion of privacy and, in its most serious form, cyber-bullying. This code of conduct sets out appropriate use of digital technology while protecting the individual and maintaining a productive, working environment. We expect all students and Staff to use digital technology responsibly.

Misuse of digital technology that results in an invasion of privacy or personal distress is CYBER-BULLYING and this will not be tolerated at the College. Cyberbullying is a criminal offense. The College will investigate any suspected cyber-bullying where there is evidence that it is causing distress to one or more students or staff of the College. Where there is proof of cyber-bullying the bullies will be dealt with in line with our Anti-Bullying Policy, whether or not the cyber-bullying took place on the College site.

Cyberbullying

- During any investigation of suspected invasion of privacy or bullying the student concerned will be requested to show senior members of staff the contents of text messages or photos/videos contained on their phones. Full co-operation is expected and parents and carers will be involved in the investigation if the student refuses to co-operate.

- Bullying which impacts on students at the College will not be tolerated, no matter where the bullying began. Students should not assume that once they leave College they can partake in bullying and be beyond punishment.

- Students found guilty of bullying or invasion of personal privacy will not be allowed to bring a mobile phone to College at all. There will also be an additional sanction depending on the severity of the incident.

2.1 Using our College network

- All users must not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.

- All users must not try to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

- All users must not try (unless they have prior permission from the Network Manager) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- All users must not disable or cause any damage to College equipment, or the equipment belonging to others.

- All users must immediately report any damage or faults involving equipment or software to the IT administrators, however this may have happened.

- When using ICT rooms all users must use equipment appropriately and Staff must recognise it is their responsibility to ensure equipment is used appropriately and is not damaged. I will abide by the rules of use of these rooms (see Appendix 6 – Advice and guidance).

2.2 Bringing own devices:

- Students and Staff are allowed to carry digital mobile devices, but do so at their own risk.

- When connecting to the Wi-Fi all users will abide by the Acceptable Use Policies and will be required to securely login.

- Users will ensure that to the best of their knowledge, any devices that are connected to our network or Wi-Fi are protected by up to date anti-virus software and are free from viruses.

- Staff should be mindful that many children will have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G) and that this access is not monitored by Smoothwall filtering as with access via the College Wi-Fi network. As such the College does not allow the use of mobile phones by students on the College site between the hours of 8:30am and 3:00pm.

2.3 Acceptable use of all digital devices (including mobile phones)

- Digital mobile devices should be switched off and in bags at all times during the college day, if not being used for a taught activity at the discretion of individual teaching staff.

- Students and staff must not use digital mobile devices to communicate in any form during lessons, unless it is part of the learning activity.

- Students must seek permission from the class teacher to use digital mobile devices, including phones during the lesson. Use will always be at the teachers' discretion and clear expectations of terms of use will be given.

- In some lessons teachers may feel it is beneficial for students to use digital mobile devices. The teacher should make clear what acceptable use is in this case and students should use them in a respectful and appropriate way.

- Students must not use digital mobile devices when travelling between lessons, Staff will challenge such behaviour.

- Digital mobile devices must not be used to take a photograph, voice recording or video of anyone without their permission.

- Mobile phones are banned from use in public examinations. They must not be taken into the examination room at all. The consequences of a mobile phone ringing or being found on a student in an examination are very severe and could include disqualification from that examination.

- Staff must not give out personal mobile phone numbers or personal email addresses to students or parents and carers.

- The College reserves the right to ban the possession of digital mobile devices on site if they are persistently misused.

2.4 Data Protection when using digital technology

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR) and other relevant data protection legislation such as the Data Protection Act 2018 (DPA 2018) to ensure data is:

- Processed fairly, lawfully and in a transparent manner.
- Used for specified, explicit and legitimate purposes.
- Used in a way that is adequate, relevant and limited.
- Accurate, kept up to date.
- Kept no longer than is necessary.
- Processed in a manner that ensures appropriate security of the personal data.

Staff must ensure that they:

- Take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Store personal data only on secure school encrypted or otherwise secured devices, ensuring that
    - all devices are password protected
    - all devices must offer approved virus and malware checking software.
    - the data must be securely deleted from the device, once it has been transferred or its use is complete (see Appendix 6 for Advice and Guidance).
    - The device will be properly logged off at the end of any session

- Transfer personal data using the College network or email system. If using USBs these must be encrypted.

There is also a whole College Data Protection Policy that covers all aspects of data protection in addition to the digital technology aspects outlined here (See Data Protection policy).

2.5 Use of social networking sites and chatrooms

- **Chatrooms** are **not to be used** at the College.

- Some **social networking sites**, such as Facebook and Twitter may be used in College for education purposes. These sites should **only** be used for educational purposes and not for personal social networking by students or staff at any time in the working day.

- Any staff member wishing to carry out a social networking activity with students needs to complete a Social Networking use Proforma, seek relevant training and will have authorization to continue from the Curriculum leader, Trainer and then the Online Safety Officer before starting the activity.

- Staff or students must not use any social networking sites or other web-based methods to

    - post inappropriate comments about students, their parents or staff.
    - post comments that could bring the College or its staff or students into disrepute.
    - send inappropriate messages about students, their parents or teachers
    - send inappropriate messages that could bring the College or its staff or students into disrepute

- Staff must not have students or parents as online friends using their personal Social Networking Sites (See Code of Conduct Section 11 and 12).

2.6 Digital communication between Staff, Students and Parents

- Any digital communication between staff and students or parents and carers must be professional in tone and content.

- These communications may only take place on official (monitored) College systems (College E-mail/Show my homework/Google classroom), unless setting up an agreed Social Networking Activity.

- If setting up a social networking activity, then the appropriate permission needs to be sought by staff and all guidance followed (see Use of Social Networking above).

- Staff **must not** use personal Social Networking accounts to communicate with students.

- We recommend and strongly advise colleagues to avoid having parents/carers as "friends" on social media.

- Staff must not give out personal mobile phone numbers or personal email addresses to students or parents and carers.

- The content of any e-mails to other students or teachers and the content of any messages posted on any sites on the internet should not be offensive, abusive or cause another person distress.

- The official College e-mail service may be regarded as safe and secure and is monitored.

- Users must immediately report to their Head of Year (in the case of students) or the Online Safety Officer (in the case of Staff) any email that they receive that makes them feel

uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such e-mail.

- When staff are emailing students they must use students' College email addresses and copy in a colleague if the email is to an individual student rather than a group.

- Students should be taught about e-mail safety issues, such as the risks attached to the use of personal details and not clicking on unknown links. They should also be taught strategies to deal with inappropriate email and be reminded of the need to write e-mails clearly and correctly and without unsuitable or abusive material.

- All users must not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs.

2.7 Distance learning – Safeguarding in online lessons

- All live online lessons using platforms such as Zoom/Microsoft Teams/Google Meet should be password protected and/or make use of the waiting room facility.

- Links to online lessons should only be shared with invitees using secure platforms such as College email or Show My Homework and not on social media or public websites.

- Students should be reminded not to share the link with anyone outside of the College community or is not intended to be invited to the session.

- A new link should be generated for each session to avoid it becoming known to persons who are not staff or students at the College.

- Students and staff should use their College email addresses and logins only.

- Online tutoring or lessons on a 1-2-1 basis should be recorded and saved in the shared drive which is accessible by the Network Manager, Online Safety officer, Designated Safeguarding lead and Vice-Principal/Principal to safeguard both staff and students. These recordings should not be shared beyond those staff who are authorised to view them without consent of the Principal.

- If pastoral support is to be offered online on a 1-2-1 basis, consider whether it is appropriate to record the session or whether detailed notes should be kept instead. Seek advice from the DSL as appropriate if you are unsure.

- Should an individual join a lesson who was not invited, the teacher/tutor should remove them immediately.

- Screen sharing should only be enabled for the host to prevent inappropriate material being shared.

- Staff should ensure that any tabs/windows containing personal or confidential information are closed and not visible to students prior to screen sharing commencing.

- If cameras are being used, staff need to ensure they are professionally dressed and the are against a plain background. If this is not possible, they should blur their background or use an appropriate virtual background.

- Staff should conduct online lessons/tutoring in an area that is away from distractions and minimises the risk of family members appearing on camera or within earshot.

3 Use of Digital and Video Images Policy - Photographic, Video

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

- Staff will follow the WeST Code of Conduct when using digital images of students.

WeST Code of Conduct (Section 11)

> *"Photographs/still images or video footage of students should only be taken using Trust equipment, for purposes authorised by the school/Trust. Any such use should always be transparent and only occur where parental consent has been given. The resultant files from such recording or taking of photographs must be stored in accordance with the Trust's procedures on Trust equipment"*

4 Technical – infrastructure/equipment, filtering and monitoring

4.1 Infrastructure/equipment

The College will be responsible for ensuring that the College infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- College ICT systems will be managed in ways that ensure that the College meets the Online Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of College ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to College ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Online Safety Committee.

4.2 Bring Your Own Devices

As a College, we understand that the world is changing fast and that more and more students and staff have personal mobile equipment that they can use to enhance their learning and teaching. Although we do not yet have the wireless infrastructure to enable high volumes of mobile devices we have allowed students and staff to make use of our Wi-Fi for internet access through our filtered service.

- As with mobile phones, these devices are expensive items and the College will not take any responsibility for them if one happens to be stolen, lost, or damaged whilst in College.

Students bring devices to College at their own risk. During PE lessons, phones and other valuable items should be handed in by the student to the valuables box.

- When connecting to the Wi-Fi, users will be asked to agree to our Acceptable Use Policies and will be required to securely login
- This enables complete filtering and logging of all access to internet sites.
- Students and staff can access their network files securely through our VLE/Google drive.
- If it is felt that it would be beneficial for a student to use their own laptop/chromebook or similar device in lessons, they will need to seek the approval of the SENDCo who will liaise with the network manager in reaching their decision. The device will need to be presented to the network manager so that it can be safely configured for use on the network and be checked for suitable anti-virus provision.

As our infrastructure develops, we will consider enabling further access to the network and adaptations to this policy and acceptable use forms will follow.

4.3 Filtering Policy

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context.

- The College maintains and supports the managed filtering service provided by SWGfL, supplemented by Smoothwall.
- Student Smoothwall alerts will be monitored by Heads of Year who will investigate any concerns and report them to the safeguarding team as appropriate.
- Staff Smoothwall alerts are monitored by the College Principal who will liaise with the Network manager and DSL as appropriate.
- The responsibility for the management of the College's filtering policy will be held by the Network Manager.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged. Any filtering issues should be reported immediately to the Network manager and SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and the Online Safety Officer. All users have a responsibility to report immediately to the Network Manager any infringements of the College's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
- Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.
- Students will be made aware of the importance of filtering systems through the Online Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.
- Staff users will be made aware of the filtering systems through: signing the AUA, induction training, staff meetings, briefings, INSET.
- Parents will be informed of the College's filtering policy through the Acceptable Use agreement and through Online Safety awareness sessions and the College website.
- Users who gain access to, or have knowledge of others being able to access, sites, which they feel should be filtered (or unfiltered), should report this in the first instance to the Network Manager who will decide whether to make College level changes (as above). If it is felt that

the site should be filtered (or unfiltered) at SWGfL level, the Network Manager will contact SWGfL.

No filtering system can guarantee 100% protection against access to unsuitable sites. The College will therefore monitor the activities of users on the College network and on College equipment as indicated in the College Online Safety Policy and the Acceptable Use agreement. Monitoring will take place and logs of filtering change controls and of filtering incidents will be made available to the Principal, Online Safety Officer, the Online Safety Committee, the Online Safety Governor & SWGfL/Local Authority on request.

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

4.4 Password Policy

- All users will be provided with a username and password by the Network Manager who will keep an up-to-date record of users and their usernames. A password change for all staff will be enforced every 90 days to ensure data security.
- The "administrator" passwords for the College ICT system, used by the Network Manager must also be available to the Principal or the Online Safety Officer upon request.
- Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security to the Network Manager.
- College ICT technical staff regularly monitor and record the activity of users on the College ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users' activity.
- Users should report any actual/potential password breaches to the Network manager. Any incidents involving students should be passed to the relevant Head of Year or via a google CP concern form if the incident is safeguarding related.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand-held devices etc from accidental or malicious attempts, which might threaten the security of the College systems and data.
- A procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the College system. This is implemented and logged by the Network Manager.
- The Acceptable Use Policies outline the use of College ICT systems.
- The College infrastructure and individual workstations are protected by up-to-date virus software.
- Personal data cannot be sent over the internet or taken off the College site unless safely encrypted or otherwise secured.
- The College will be responsible for ensuring that the College infrastructure/network is as safe and secure as is reasonably possible and that:
  - users can only access data to which they have right of access;
  - no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the College policies);

- access to personal data is securely controlled in-line with the College's personal data protection policy and relevant data protection legislation;
- Logs are maintained of access by users and of their actions while users of the system.

- The management of the password security policy will be the responsibility of the Network Manager

- Passwords for new users and replacement passwords for existing users can be allocated by the ICT Technicians and will require immediate change of password.

- Members of staff will be made aware of the College's password policy at induction, through this policy and through the Acceptable Use Agreement.

- Students will be made aware of the College's password policy in Online Safety lessons and through the Acceptable Use Agreement.

- The Network Manager will be responsible for ensuring that full records are kept of user IDs and requests for password changes, User log-ons and security incidents related to this policy.

- In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

- Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

A safe and secure username/password system is essential if the above is to be established and will apply to all College ICT systems, including e-mail, Virtual Learning Environment (VLE) and cloud storage based services (Google drive).

5 Appendices

5.1 Sanctions

5.1.1 Sanctions for students' that fail to adhere to the Online Safety policy can be found in the College's Behaviour Policy

5.1.2 Sanctions for staff that fail to adhere to the Online Safety policy will be determined with reference to the staff "code of conduct" and relevant college disciplinary procedures.

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Principal	Refer to Local Authority / HR	Refer to Online Safety officer/Network manager	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in Section 5.1.3)		Y	Y	Y	Y			Y
Excessive or inappropriate personal use of the internet/social networking sites/instant messaging / personal email	Y	Y					Y	Y
Unauthorised downloading or uploading of files	Y	Y		Y			Y	
Allowing others to access College network by sharing username and passwords or attempting to access or accessing the College network, using another person's account	Y	Y		Y			Y	Y
Careless use of personal data e.g. holding or transferring data in an insecure manner	Y	Y		Y			Y	Y
Deliberate actions to breach data protection or network security rules	Y	Y		Y			Y	Y
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	Y	Y		Y			Y	Y
Sending an e-mail, text or instant message that is regarded as offensive, harassment or of a bullying nature	Y	Y		Y			Y	Y
Using personal e-mail/social networking/ instant messaging/text messaging to carrying out digital communications with students/pupils	Y	Y		Y			Y	Y
Actions which could compromise the staff member's professional standing	Y	Y		Y			Y	Y
Actions which could bring the College into disrepute or breach the integrity of the ethos of the College	Y	Y		Y			Y	Y
Using proxy sites or other means to subvert the College's filtering system	Y	Y		Y			Y	Y
Accidentally accessing offensive or pornographic material and failing to report the incident	Y	Y		Y			Y	Y
Deliberately accessing or trying to access offensive or pornographic material	Y	Y	Y	Y		Y	Y	Y
Breaching copyright or licensing regulations	Y	Y		Y			Y	Y
Continued infringements of the above, following previous warnings or sanctions	Y	Y		Y				Y

5.2 Roles and Responsibilities

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the College:

5.2.1 Governors

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

- regular meetings with the DSL;
- regular monitoring of Online Safety incident logs;
- regular monitoring of filtering/change control logs;
- reporting to relevant Governors committee/meeting.

5.2.2 Principal and Senior Leaders

- The Principal is responsible for ensuring the safety (including Online Safety) of members of the College community, though the day-to-day responsibility for Online Safety will be delegated to the Online Safety Officer.
- The Principal is responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in College who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Leadership Team will receive regular monitoring reports from the DSL as part of regular safeguarding monitoring and reporting.
- The Principal and Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff (see SWGfL flow chart).

5.2.3 Online Safety Officer (Lead)

- Lead on Online Safety as part of the wider Safeguarding team and sits within the SLT.
- Takes day-to-day responsibility for Online Safety issues and has a leading role in establishing and reviewing the College Online Safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority and other relevant outside agencies such as CEOP.
- Liaises with College ICT technical staff
- Receives reports of Online Safety incidents and ensures they are logged on CPOMS using the appropriate "Online Safety" tag to inform future Online Safety developments.

- Is alerted to any CPOMs logs tagged with "Online Safety" so they can review, offer advice and challenge as appropriate in liaison with the DSL.
- Liaises with the DSL who attends relevant meeting/committee of Governors
- Reports regularly to Leadership Team alongside the DSL as part of regular safeguarding reporting.

5.2.4 Network Manager

The Network Manager is responsible for ensuring:

- That the College's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the College meets the Online Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance.
- That users may only access the College's networks through a properly enforced password protection policy, in which passwords are changed every 90 days.
- SWGfL is informed of issues relating to the filtering applied by the Grid.
- That they are kept up-to-date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant.
- That the use of the network/Show My Homework/Google drive/remote access/e-mail is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Officer and other relevant member of staff for investigation/action/sanction.
- That monitoring software/systems (Smoothwall) are implemented and updated as agreed in College policies.

5.2.5 Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of Online Safety matters and of the current College Online Safety policy and practices.
- They have read, understood and signed the College Staff Acceptable Use Policy/Agreement (AUA).
- They report any suspected misuse or problem to the Online Safety Officer.
- Digital communications with students (e-mail/Show My Homework/Google classroom) should be on a professional level and only carried out using official College systems.
- Online Safety issues are embedded in all aspects of the curriculum and other College activities.
- Students understand and follow the College Online Safety and Acceptable Use policy.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended College activities.
- They are aware of Online Safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current College policies with regard to these devices.

- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

5.2.6 Designated Safeguarding Lead

Designated Safeguarding Leads should be trained in Online Safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data;
- Access to illegal/inappropriate materials;
- Inappropriate on-line contact with strangers;
- Potential or actual incidents of grooming;
- Cyber-bullying.

5.2.7 Students:

- Are responsible for using the College ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to College systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand College policies on the Use of Mobile Phones, Digital Cameras and Hand-held Devices. They should also know and understand College policies on the Taking/Use of Images and on Cyber-Bullying.
- Should understand the importance of adopting good Online Safety practice when using digital technologies out of College and realise that the College's Online Safety Policy covers their actions out of College, if related to their membership of the College.

5.2.8 Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The College will therefore take every opportunity to help parents and carers understand these issues through parents' evenings, newsletters, letters, website/VLE and information about national/local Online Safety campaigns/literature. Parents and carers will be responsible for:

- Endorsing the Student Acceptable Use Policy;
- Accessing the College website/Show My Homework/School gateway in accordance with the relevant College Acceptable Use Policy.

5.2.9 Community Users

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

5.3 Training

5.3.1 Students

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

Online Safety education will be provided in the following ways:

- A planned Online Safety programme should be provided as part of ICT/Computer Science/PHSE/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in College and outside College.
- Key Online Safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students should be helped to understand the need for the student Acceptable Use Policy (AUA) and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside College.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rather than seek to equip students to deal with every single potential online safety issue in an ever changing online environment, the College will seek to draw their attention to methods of reporting inappropriate content online, direct them to reputable sources of advice such as "ThinkUKnow" and ensure they know who they can talk to should they see content which concerns them or should they need to seek support including tutors, Heads of Year and the Safeguarding team.
- Rules for use of ICT systems/Internet will be posted in all rooms with ICT access.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

5.3.2 Parents and carers

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

The College will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters (Callington voice), College website and via School Comms messages.
- Parents evenings and training events.
- Reference to relevant advice online including: THINKUKNOW from CEOP and the UK Safer Internet Centre.

5.3.3 Staff

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online Safety training will be made available to staff as part of annual safeguarding training. An audit of the Online Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify Online Safety as a training need within the performance management process.

- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the College Online Safety Policy and Acceptable Use Policies.

- The Online Safety Officer (or other nominated person) will receive regular updates through attendance at or reference to SWGfL/LA/DfE guidance/training sessions and by reviewing guidance documents released by Common Sense/SWGfL/CEOPS/ and others.

- This Online Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.

- The Online Safety Officer (or other nominated person) will provide advice/guidance/ training as required to individuals as required.

5.3.4 Governors

Governors should take part in Online Safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in ICT/ Online Safety/health and safety/ child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/SWGfL or other relevant organisation.

- Participation in College training/information sessions for staff or parents and carers.

- Undertake Online Safety training as part of the e-learning safeguarding training package used by the College.

6 Staff Advice & Guidance

This section includes:

1. Acceptable use summary table
2. Illegal and unacceptable activities
3. Responding to online incidents
4. Staff who need to manage Online Safety incidents
5. Who to see for help?

6.1 Table of acceptable use for digital communications technology

	Staff and other adults				Students			
Communication Technologies	Allowed	Allowed with details logged with Online Safety Officer	Allowed for staff for educational purposes	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones and other personal digital devices may be brought to College	√				√			
Use of mobile phones and other digital devices in lessons for personal use				√				√
Use of mobile phones and other digital devices in lessons for educational use			√				√	
Use of mobile phones and other digital devices in social time (keeping to Online Safety Policy)	√							√
Taking photos of students or staff on personal mobile phones or other digital devices				√				√
Use of personal email addresses in College, or on College network				√				√
Use of College email for personal emails				√				√
Use of chat rooms (unless College systems)				√				√
Use of instant messaging (unless College systems)				√				√
Use of social networking sites for educational use*		√					√	
Use of social networking sites for personal use				√				√

*To use Social Networking in College staff must log details with the Online Safety officer and seek relevant training from the Faculty leader for Computing and/or the Network manager.

6.2 Illegal and unacceptable activities

The College believes that the activities referred to in the following section would be inappropriate in a College context and that users should not engage in these activities in College or outside College when using College equipment or systems.

Users must not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to any of the following:

Illegal Activity:

- Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008
- Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986

Unacceptable Activity

- pornography
- promotion of any kind of discrimination
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the College or brings the College into disrepute
- Using College systems:
    - to access pornography
    - to run a private business
    - to upload, download or transmit commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
    - to reveal or publicise confidential or proprietary information (e.g. financial/personal information, databases, computer / network access codes and passwords)
    - to create or propagate computer viruses or other harmful files
    - to carry out sustained or instantaneous high volume network traffic (downloading/uploading files) that cause network congestion and hinders others in their use of the internet
    - for online gambling
    - for gaming or online shopping/commerce during work hours.
    - for file sharing
    - to use social networking sites for personal use during work hours
    - to use video broadcasting/streaming for large numbers of classes, unless agreed with the Network Manager (due to high volume of network traffic).
6. Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and/or the College

Online Radicalisation

From July 2015 all schools (as well as other organisations) have a duty to safeguard children from radicalisation and extremism. This means we have a responsibility to protect children from extremist and violent views in the same way we protect them from drugs or gang violence. Importantly, we can provide a safe place for pupils to discuss these issues so they better understand how to protect themselves.

Further details on how the College protects students from radicalisation can be found in the College's Safeguarding policy.

6.3 Responding to Online Safety incidents

It is hoped that all members of the College's community will be responsible users of digital technologies, who understand and follow College policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion of a student then this should be reported to the Head of Year or curriculum leader in the first instance.

In the event of suspicion of a member of staff then this should be reported in line with the Whistleblowing policy.

Full details of the College's approach to Searching and Screening including the items that Staff are able to search for and the staff authorised to conduct searches are set out in the College's Behaviour policy.

Searching electronic devices.

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.
- As with all prohibited items, staff should first consider the appropriate safeguarding response if they find images, data or files on an electronic device that they reasonably suspect are likely to put a person at risk
- Staff may examine any data or files on an electronic device they have confiscated as a result of a search. If there is good reason to do so (defined earlier in the guidance as)
    - poses a risk to staff or pupils;
    - is prohibited, or identified in the school rules for which a search can be made or
    - is evidence in relation to an offence.
- ***If the member of staff conducting the search suspects they may find an indecent image of a child (sometimes known as nude or semi-nude images), the member of staff should never intentionally view the image, and must never copy, print, share, store or save such images. When an incident might involve an indecent image of a child and/or video, the member of staff should confiscate the device, avoid looking at the device and refer the incident to the designated safeguarding lead (or deputy) as the most appropriate person to advise on the school's response.***
- If a member of staff finds any image, data or file that they suspect might constitute a specified offence, then they must be delivered to the police as soon as is reasonably practicable.
- In exceptional circumstances members of staff may dispose of the image or data if there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files, the member of staff must have regard to the following guidance issued by the Secretary of State
- In determining whether there is a 'good reason' to examine the data or files, the member of staff should reasonably suspect that the data or file on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.
- In determining whether there is a 'good reason' to erase any data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable. If the data or files are not suspected to be evidence in relation to an offence, a member of staff may delete the data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves.

6.4 Staff who need to manage Online Safety incidents

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities. If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.

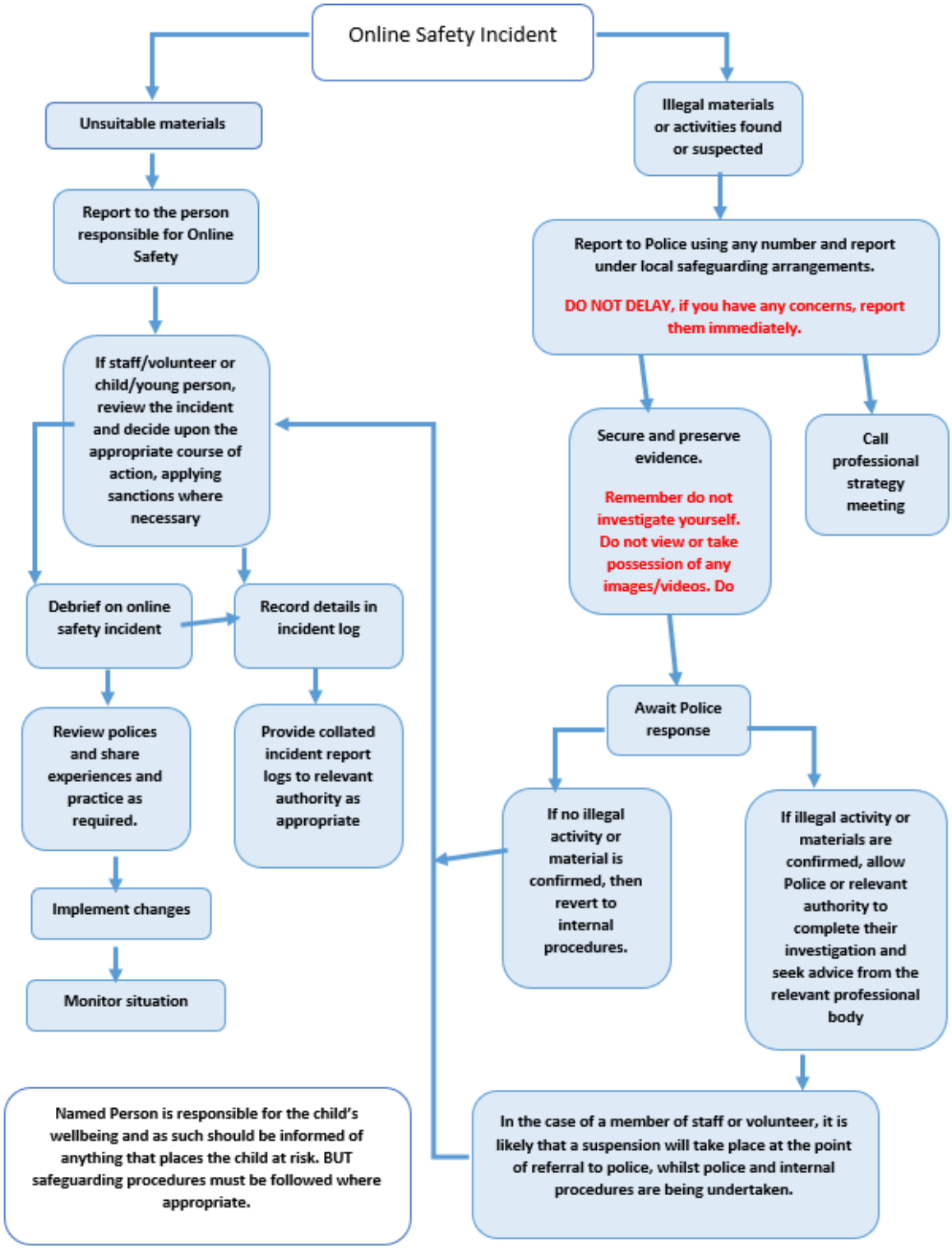

Figure 1: https://swgfl.org.uk/resources/online-safety-policy-templates/ [Accessed on 11/09/22]

6.5 Who to see for help?

Problem	**Who to see**
Concerns about student activity	Designated Safeguarding Lead, Online Safety lead or relevant HOY
Concerns about staff activity	Designated Safeguarding Lead, Principal or Vice Principal
Problems with network logins	ICT Technical team (ext 227)
College website concerns	C Harbottle (CLH)
Damage to equipment	ICT Technical team (ext 227) & HOY
A problem with a projector	ICT Technical team (ext 227 or email ICT)

CALLINGTON COMMUNITY COLLEGE

STUDENT ACCEPTABLE USE AGREEMENT

THIS IS AN APPENDIX OF THE ONLINE SAFETY POLICY

New technologies have become integral to the lives of children and young people in today's society, both within College and in their lives outside College. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That College ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The College will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Agreement

- I understand that I must use College ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
- I understand that being allowed to bring mobile phones and other digital devices to the College is a privilege and I will adhere to this AUA at all times and follow staff instructions on its acceptable use.
- I understand mobile phones and other digital devices are expensive items and the College will not take any responsibility for the device if it happens to be stolen or lost whilst in College. I understand that if I bring a digital device such as a mobile phone to College it is at my own risk. During PE lessons I will hand phones and other valuable items in to the valuables box.

For my own personal safety:

- I understand that the College will monitor my use of the ICT systems, email and other digital communications.

- I understand that the rules set out in this agreement also apply to use of College ICT systems (Google suite for education, email, Show My Homework) out of College.

- I will not share my username or password with other students nor will I try to use any other person's username and password.

- I will immediately report any illegal, inappropriate or harmful material or incident, that I become aware of, to my teachers and/or tutor.

- I will not disclose or share personal information about myself with others online.

- I will not arrange to meet anyone I have met online and will tell my teacher or parent, carer or guardian immediately about any invitations I receive to meet online contacts.

- I will immediately report any unpleasant or inappropriate material or messages, or anything that makes me feel uncomfortable when I see it online.

Distance/remote learning:

- I will not share links to online/live lessons on public platforms such as social media or with anyone who is not intended to be invited to the lesson.

- I will not share my screen during a live lesson, unless I am invited to do so by the teacher and I will ensure that there is no inappropriate, personal or confidential information visible.

- I will ensure I am dressed appropriately for online lessons for which webcams are in use.

- I will ensure there are no inappropriate images/posters in the background for online lessons.

- I recognise that I am bound by the same expectations of behaviour as I would be in College including, but not limited to using appropriate language and treating others with respect.

- I agree not to make audio/video recordings or take screenshots of staff or students during live or pre-recorded lessons.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the College ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not use the College ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing

- I will not use video broadcasting/streaming (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act towards me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will not take or distribute images of anyone in College, taking part in a College activity or wearing College uniform, nor will I record video or sound (including uploading to social media sites), without permission from staff. Staff permission will be strictly for educational purposes only.

For security and integrity of the technology I use in College

- I will only use my personal hand-held/external devices (mobile phones/USB devices etc) in College with staff permission. This does not apply to social or movement time.

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place, to prevent access to such materials.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any attachments to emails, unless I know and trust the person/organisation who sent the e-mail, due to the risk of the attachment containing viruses or other harmful programmes.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings (unless creating programmes as part of their Computing lessons).

- I will not use chat sites at any time.

- I will not use social networking sites unless it is a teacher directed activity as part of a lesson. If I am using these sites in an activity, I will follow the guidance given by the teacher in its use.

- If I wish to use a laptop or similar device in lessons, this will only be with the approval of the SENDCo who will inform teaching staff. I will need to present my device to the network manager first so that it can be safely configured for use on the network and be checked for suitable anti-virus provision.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not try to download copies (including music and videos).

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of College:

- I understand that the College also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of

College and where they involve my membership of the College community (examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Agreement, I will receive sanctions. In cases of illegal activities this may include involvement of the police.

- I understand that the minimum age for social networking sites is set for my protection and I that I should not set up social networking accounts without my Parents' or Carers' permission. (The minimum age for most major social networking sites is usually around 13 or 14)

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

Student Acceptable Use Agreement Form

This form relates to the student Acceptable Use Agreement (AUA), to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to College ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the College ICT systems and equipment (both in and out of College).

- I use my own equipment in College (when allowed) e.g. mobile phones, iPads, PDAs, cameras etc.

- I use my own equipment out of College in a way that is related to me being a member of this College e.g. communicating with other members of the College, accessing College e-mail, VLE, Google drive, website etc.

Each time you log on to our network you will be agreeing to this acceptable use agreement. If you do not agree then you <u>should not</u> log in or use any of our digital equipment.

Name of Student:…….

Tutor Group:……

Signed:……..

Date:……..

STAFF (AND VOLUNTEER) ACCEPTABLE USE AGREEMENT

This is an appendix of the Online Safety policy

New technologies have become integral to the lives of children and young people in today's society, both within College and in their lives outside College. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That College ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

The College will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students' learning. In return, the College will expect staff, volunteers or visitors using our ICT systems to agree to be responsible users.

Acceptable Use Agreement

- I understand that I must use College ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

- I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT (see Online Safety policy Section 1).

- I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people (see Online Safety policy Section 1).

For my professional and personal safety:

- I understand that the College will monitor my use of the ICT systems, email and other digital communications through the College network and on College equipment.

- I understand that the College ICT systems and equipment are primarily for educational use. However, they can be used for personal purposes but staff must use their professional judgement when doing so and ensure the integrity and safety of data at all times.

- If I have a College laptop or tablet, I will not allow it to be used by anyone who is not a member of Callington Community College staff. However, for student access on College iPads app access must be restricted and appropriate training sought to ensure safe use.

- I will not disclose my username, password or PIN to anyone else, nor will I try to use any other person's username, PIN or password accept, accept for ICT administration purposes (See Code of conduct section 10 and Online Safety Policy section 2.1).

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the Online Safety Officer(s) or Network Administrators.

- If I use a College laptop and other devices within another establishment, I will adhere by their acceptable use policies as well as this policy.

When using the Internet in College (See Online Safety Policy Section 1)

- I will report to the Network manager sites accessed, by me or students in my care, that are found to have any unsuitable material (refer to Appendix 6 for further guidance).

- I will be vigilant in monitoring the content of the websites the young people visit and remind students of the AUA they have signed.

- If for good educational reasons my students need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked, I will put in a request by email to the Network Manager so these sites can be temporarily unblocked for the period of study, giving a minimum of 24 hours notice.

- I will teach students in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.

- I will teach students to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- I will ensure that I have permission to use the original work of others in my own work by checking copyright statements and will acknowledge the source I have used.

- Where work is protected by copyright, I will not download or distribute copies as this would be breaking the law (including music, video and printed materials).

Bringing own devices (See Online Safety Policy Section 2.2)

- I understand that the College will not take any responsibility for personal digital devices brought into College and I do so at my own risk.

- When connecting to the Wi-Fi, I agree to abide by the Acceptable Use Agreement and will be required to securely login.

- To the best of my knowledge I will ensure that any devices that are connected to our network or WI-FI are protected by up to date anti-virus software and are free from viruses.

Using our College network (See Online Safety Policy Section 2.1)

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or which are inappropriate or may cause harm or distress to others.

- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place to prevent access to such materials.

- I will not try (unless I have prior permission from the Network Manager) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not disable or cause any damage to College equipment, or the equipment belonging to others.

- I will immediately report any damage or faults involving equipment or software to the IT administrators, however this may have happened.

- When using ICT rooms with classes I recognise it is my responsibility to ensure equipment is used appropriately and is not damaged. I will abide by the rules of use of these rooms (see Appendix 6 – Advice and guidance).

Acceptable use of all digital mobile devices (See Online Safety policy Section 2.3)

- I will not use digital mobile devices (including mobile phones) to communicate in any form during lessons, unless it is part of the learning activity. A member of LT may give permission in extenuating circumstances for one-off use.

- If I feel it is beneficial for students to use digital mobile devices in my lesson I will be clear with students about my expectations in terms of their use and I will deal with any misuse adhering to sanctions outlined in the College Online Safety policy (Appendix 1).

- I will challenge students using digital mobile devices during the college day (unless as part of an authorized learning activity) including during social time as this is not allowed.

- I will not take a photograph, voice recording or video of anyone without their permission.

- I will not give out my personal mobile phone numbers or personal email addresses to students or parents and carers.

Data Protection when using digital technology (See Online Safety policy Section 2.4)

- I will take care to ensure the safe-keeping of personal data, minimising the risk of its loss or misuse.

- I will only store personal College data on secure College encrypted devices, ensuring that:

    - all devices must be password protected
    - all devices must offer approved virus and malware checking software.
    - the data must be securely deleted from the device, once it has been transferred or its use is complete (see Appendix 6 for Advice and Guidance).
    - I will properly log off at the end of any session

- If using College tablets I will ensure I have PIN code set up and that this has been checked and details logged with the ICT Administration team.

- If I need to transfer personal data I will do so using the College network or email system. Encrypted USBs are available to staff on request.

Social networking and chatrooms (See Online Safety policy Section 2.5)

- I will not use chatrooms at the College.

- I will not use College systems or personal devices during lessons to access social networking sites for personal use within my working day.

- If I wish to use social networking for educational purposes I will complete a Social Networking Use Proforma, seek relevant training and will have authorisation to continue from the Curriculum Leader, Trainer and then the Online Safety Officer before starting the activity.

- I will not use any social networking sites or other web-based methods to

    - post or send inappropriate comments about students, their parents or staff.

- post or send comments that could bring the College or its staff or students into disrepute.

- I will not have students or their parents and carers as online friends using my personal social networking profiles (see Code of Conduct section 11 and 12).

Use of email and other digital communication (See Online Safety policy section 2.6)

- I will only use College email and agreed College social networking profiles to communicate with students, staff or parents.

- If communicating digitally with staff, students or parents and carers I will ensure these communications are professional in tone and content.

- I will not send emails to students, parents and carers or other teachers that could be offensive, abusive or cause another person distress.

- I understand that the College e-mail service may be regarded as safe and secure and is monitored.

- If I receive offensive, threatening of bullying emails I will immediately report this to one of the Online Safety officers and will not respond to the email.

- When emailing students I will only use students' College email addresses.

- I will teach my students email safety issues when I need students to use email.

- I will not open any attachments to e-mails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

Using images of students (See Online Safety policy section 3 and WeST Code of conduct section 11)

I will follow the WeST Code of Conduct (Section 11)

> *"Photographs/still images or video footage of students should only be taken using Trust equipment, for purposes authorised by the school/Trust. Any such use should always be transparent and only occur where parental consent has been given. The resultant files from such recording or taking of photographs must be stored in accordance with the Trust's procedures on Trust equipment"*

Please keep the policy safe and tear off this page.

Important: Please read the Online Safety full policy, the Acceptable use Agreement and then sign and return to the data office.

I have read and understand the above and agree to use the College ICT systems (both in and out of College) and my own devices (in College and when carrying out communications related to the College) within these guidelines.

Staff / Volunteer Name:……

Signed:……..

Date:……..

CALLINGTON COMMUNITY COLLEGE (ACADEMY TRUST)

PARENT AND CARER ACCEPTABLE USE AGREEMENT

This is an Appendix of the Online Safety policy

New technologies have become integral to the lives of children and young people in today's society, both within college and in their lives outside college. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That college ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The college will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use Policy is available as a separate document which should be read in conjunction with this information, so that parents and carers will be aware of the college expectations of the young people in their care.

As the parent or carer of a student,

- I give permission for my child to have access to the internet and ICT systems at college.
- I know that my child has signed an Acceptable Use Agreement and has received, or will receive, Online Safety education to help them understand the importance of safe use of ICT – both in and out of college.
- I understand that the college will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the college cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my child's activity on the ICT systems will be monitored and that the college will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the college if I have concerns over my child's Online Safety.
- I will monitor my childs' use of ICT at home and I understand that the minimum age for social networking sites is set for their protection. (The minimum age for most major social networking sites is usually 13).

Parents and carers are **not** requested to sign an Acceptable Use Agreement but should contact the school if there are any concerns with the conditions set out in this document.