LISKEARD SCHOOL AND COMMUNITY COLLEGE

E-SAFETY POLICY

Related Policies

- Safeguarding & Child Protection Policy
- Behaviour for Learning Policy
- Anti-Bullying Policy
- Screening, Searching and Confiscation Policy
- Data Protection Policy

General Statement

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

The Education and Inspections Act 2006 empowers the Head teacher, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

2. Roles and Responsibilities

2.1 Governors

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

- attending E-Safety working party meetings
- working alongside the E-Safety Co-ordinator on the action points arising from the 360 review tool
- feeding back to the full governing body

2.2 Head teacher

- the Head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- the Head teacher and Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- the Head teacher is responsible for ensuring that the E-Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- the Head teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- the Senior Leadership Team have access to the log of E-Safety incidents through the online reporting system My Concern.

2.3 E-Safety Co-ordinator:

- leads the e-safety working party
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Child Protection Officers and Technical Services Manager (TSM) where necessary
- receives reports of E-Safety incidents through My Concern which are used to inform future E-Safety developments.
- attends relevant Governors meetings
- reports regularly to Senior Leadership Team (once a term).

2.4 Technical staff:

The TSM is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis.
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network is regularly monitored (once a week), reports generated and sent to the E-Safety Co-ordinator and Heads of Year for follow up.
- that monitoring software / systems are implemented and updated as and when necessary.
- there will be occasions when the ICT technical team will need to override aspects of the staff AUP for the purposes of doing their job. For example, accessing other staff laptops.

2.5 Teaching and Support Staff

are responsible for ensuring that they:

- read the Liskeard School e-safety policy and are familiar with its practices
- read, understood and sign the Staff Acceptable Use Policy (AUP)
- report any suspected e-safety incidents to the relevant people in line with the Behaviour for Learning Policy (HOY for students; Head teacher for staff)
- carry out all digital communications with students, parents and carers in a professional manner and only using official school systems
- try and avoid carrying a combination of student names, addresses and dates of birth by removable device. If unavoidable then this is only permitted using a school issued encrypted memory stick issued by the ICT technicians. They are available from the technicians' office and will need to be signed for.
- encourage students to understand the issues surrounding e-safety and the importance of the Acceptable Use Policy (AUP)
- ensure students understand the need to avoid plagiarism and uphold copyright regulations
- monitor the use of devices (mobile; tablet; school PC; flip cameras etc) in lessons to the best of their ability.

It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can enter their own login details in order to 'override the filter' for students to access particular sites. It is the responsibility of the member of staff to have previously checked the suitability of these sites. Students are given access for 45 minutes, after which time the site can no longer be accessed by the student. Websites which are needed for longer periods of study can be unfiltered by the TSM. Staff making such requests are required to do so through the Helpdesk. Clear reasons need to be given as to why it is needed. Records of requests are kept.

2.6 Child Protection Officers

Should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming

- cyber-bullying

2.7 E-Safety Working Party

The E-Safety Working Party provides a consultative group that has wide representation across all stakeholders with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives.

Members of the E-Safety Working Party will assist the E-Safety Coordinator with:

- the production, review and monitoring of the school e-safety policy
- discussions about the level of school filtering and requests for filtering changes
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- consulting stakeholders – including parents/carers and the students/pupils about the e-safety provision
- monitoring improvement using the benchmarks for good practice outlined in the 360 review tool.

2.8 Students:

- are responsible for using the Liskeard School digital technology systems in accordance with the Student Acceptable Use Policy
- should understand the need to avoid plagiarism and uphold copyright regulations
- should understand the importance of reporting online abuse, misuse or access to inappropriate materials and know how to do so as outlined in the Student Acceptable Use Policy (AUP)
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the Liskeard School can take action if incidents take place online which break the school Behaviour for Learning Policy.

2.9 Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Liskeard School will take every opportunity to help parents understand these issues through emails to parents about how they can help keep their child safe online. Parents and carers will be encouraged to support Liskeard School in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices which they may bring to school as part of Bring Your Own Device (BYOD).

2.10 Community Users

Community Users who have a username and login to school systems will be expected to sign a Community User Acceptable Use Policy (CUAUP) See Appendix 1.

3. The teaching of E-Safety

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

E-safety should be taught as a discrete topic (in line with best practice), however staff should take every opportunity to reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- a planned e-safety curriculum should be provided as part of PSCHE programme
- key e-safety messages should be reinforced as part of a planned programme of assemblies
- 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
- students should be helped to understand the need for the Student Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside school.

3.1 Training

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

- a planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly (once annually).
- all new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and AUPs.
- the E-Safety Coordinator will receive CEOPS Ambassador training and access to the latest advice and guidance through the CEOPS site as a result of attending the course.
- the E-Safety Coordinator will provide training to individuals as required.
- Governors should take part in e-safety training/awareness sessions. There will be an annual update of key messages to the full governing body.

3.2 Technical – infrastructure/equipment, filtering and monitoring

The school is responsible for ensuring that the school network is as safe and secure as is reasonably possible. Broadly speaking:

- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling must be securely located and physical access restricted
- all users will have clearly defined access rights to school technical systems and devices.
- all users will be provided with a username and secure password by the TSM who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- the "master/administrator" passwords for the school ICT system, used by the TSM must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. school safe).
- *t*he TSM is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students, e.t.c.)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the AUP.
- reports concerning misuse of the internet are generated fortnightly and sent to the Heads of Year and E-Safety Co-ordinator.
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- an agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- if staff need a new programme installed on their school device then they must hand the device into the technical team. Staff are not permitted to install programmes on school devices themselves.

4. Bring Your Own Device (BYOD)

Bring your own device (often shortened to BYOD) is the term used to describe the connection of a personally-owned device (such as a laptop, smartphone or tablet) to a wi-fi network provided by a company or other organisation, in this case Liskeard School. The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration of users bringing their own technologies into school in order to provide a greater freedom of choice and usability.

Students and staff using BYOD are subject to internet filtering (set at the strictest setting of the filtering levels within school) and students and staff are expected to abide by the AUPs they have signed. Student signatures are checked by the tutor and staff forms are collected and chased by the Head's PA.

4.1 Consequences for Misuse/Disruption (one or more may apply):

- access to the wireless network will be removed.
- device taken away for the day.
- device taken away and kept in the Year Head Office until parent picks it up.

- student is not allowed to use personal devices at school.

Serious misuse of Internet capable devices is regarded as a serious offence within the School's Behaviour for Learning Policy and will be dealt with in accordance with this policy.

4.2 Emails protocols

Liskeard School encourages emails as the main form of written communication between staff as part of our sustainable schools strategy and because of its potential to improve communication and reduce workload. However, it is important that staff adhere to some simple protocols:

- avoid blanket emails; select recipients carefully. Inboxes become overcrowded very quickly. We need to avoid this or people will become overloaded or will simply not bother to read emails
- users should be responsible for setting up and using distribution lists effectively, e.g. Y9 tutors.
- for non-urgent messages for all staff, the message should be emailed to the Admin member responsible for collating information for the weekly communication sheet.
- addressee boxes should be checked carefully – it is very easy to send the wrong item to the wrong person – it is annoying for the recipient and could be embarrassing for the member of staff sending the message.
- be specific in the subject line about the context of the email.
- emails to students should be about school work only and not used as a means of personal communication. Always use work email addresses not your own personal email address. The use of Chat rooms such as 'Facebook' is also inappropriate between teachers and current students unless a specific group page has been set up for educational reasons.
- staff are advised not to write an email when cross or annoyed. A face to face meeting is always better.
- emails tend to be an informal text and more in common with talk rather than letters or memos. However, without facial expression to accompany the words, offence can be caused. Staff are advised to take care with their emails. A rule of thumb is: 'if you would not like the head or governors to read it, it is not appropriate for a work email'
- no offensive language should be used in any email as emails can be used as contractual evidence and presented in any case of grievance.
- if staff are emailing parents, it is essential that they check the standard of their written communication and are careful about the tone. Emails to parents should be treated in the same way as a letter. They should be written as a formal text. Any email must be copied in to the appropriate head of year so that the email can be included on the pupils' SIMs file.

4.3 Use of digital and video images

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 all stakeholders need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- when using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images. This will be communicated to students/parents/the public through one of the following ways:
  a) a message on event programmes;
  b) a message on the plasma screen;
  c) verbally announced.
- staff are allowed to take digital/video images to support educational aims, but publication of such images must be in line with parent permissions (on individual SIMS records)
- those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes

- care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images
- students' names will be used online in accordance with parent permissions (on individual SIMS records).

4.4 Data Protection

Personal data will be recorded, processed, transferred and made available according to General Data Protection Regulation (GDPR) rules 2018. In terms of data protection and e-safety all users must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- never share their passwords with anyone. Doing so may result in disciplinary procedures for staff. Students will be dealt with in line with the Behaviour for Learning Policy.

4.5 Use of Social Media

Social media sites can be used by staff for educational purposes. However a set of protocols must be adhered to:

- the school Twitter account will be run by the SMART Publicity and Web Manager.
- Staff who wish to create Facebook or other social media accounts for educational purposes must inform the E-Safety Co-ordinator in advance.
- the member of staff who created the account is responsible for checking the appropriateness of the comments made by students on the site. Any issues must be reported to the E-Safety Co-ordinator as soon as they arise.
- any misuse of sites by students must be reported (in line with the school's Behaviour for Learning Policy)

In terms of personal social media activity school staff should ensure that:

- they do not make reference to any students, parents or carers
- they do not engage in online discussion on personal matters relating to the school
- they do not make any comments which may bring the school into disrepute.

In the light of a complaint being made Liskeard School reserves the right to ask to look at the member of staff's personal social media account.

Liskeard School's use of social media for professional purposes will be checked regularly by the SMART Publicity and Web Manager to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

4.6 Unsuitable/inappropriate activities

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for staff only	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material,	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X

remarks, proposals or comments that contain or relate to:	**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**					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
	Radicalisation, extremist views, hate material and anything related to weapons construction				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright						X
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)						X
Creating or deliberately propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
Student on-line gaming (non educational) outside of lesson time			X			
On-line gambling					X	
On-line shopping / commerce for educational reasons				X		
File sharing eg: DropBox		X				
Use of social media for educational purposes		X				
Use of messaging apps for educational purposes		X				
Use of video broadcasting eg Youtube for educational purposes		X				
Student use of social media for personal reasons outside of lesson time		X				
Staff use of social media for personal reasons during lesson time					X	

4.7 Reporting e-safety incidents

E-safety issues which involve the safety of students should be reported in line with the schools' Safeguarding and Child Protection Policy. Any issues which relate to staff / community users should be reported directly to the Head teacher.

4.8 Sanctions for e-safety incidents

It is important that any e-safety incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with in line with the school's Behaviour for Learning Policy and dealt with on a case by case basis. However, broadly speaking the following sanctions may apply:

Students Actions / Sanctions

Incidents:	To be dealt with by the class teacher	To be dealt with by the Head of Faculty	Refer to Head of Year	Refer to Head teacher	Refer to Police	Refer to the TSM for action re filtering / security	Inform parents / carers	Removal of network / internet access rights for an appropriate period of time	Warning and After School	Internal Exclusion	External Exclusion
Deliberately accessing or trying to access material that could be considered illegal.				X	X						
Unauthorised use of non-educational sites during lessons	X										
Unauthorised use of mobile phone / digital camera / other mobile device in lessons			X								
Unauthorised use of social media / messaging apps / personal email in lessons	X					X					
Unauthorised downloading or uploading of files in lessons	X					X					
Allowing others to access the school network by sharing username and passwords			X			X	X	X	X		
Attempting to access or accessing the school network, using another student's account			X			X	X	X	X		
Attempting to access or accessing the school network, using the account of a member of staff				X						X	
Corrupting or destroying other students' work	X										
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X				X		X		
Continued infringements of the above, following previous warnings or sanctions		X	X				X			X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school							X				X
Using proxy sites or other means to bypass the schools' filtering system			X			X		X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident			X			X	X				
Deliberately accessing or trying to access offensive or pornographic material			X				X	X		X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X			X	X		X		

Appendices

A: Community Users Acceptable Use Agreement
B: Student Acceptable Use Agreement
C: Staff Acceptable Use Agreement Policy

Appendix A: Community Acceptable Use Policy

I understand that I must use school 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. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school 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 school ICT systems (eg laptops, email, moodle etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are only intended for educational use and that I am only allowed to use them for this purpose.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may access it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using the school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's data protection policy.
- I will only use chat and social networking sites for educational reasons
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not use personal email addresses on the school ICT systems
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with best practice as outlined by the school.
- 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 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 / security systems in place to prevent access to such materials.
- 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 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 this is allowed in school/academy policies. (schools/academies should amend this section in the light of their policies on installing programmes/altering settings)
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will 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 download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of *school*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police. Any breach of this procedure by a Governor would be reported to the Chair of Governors and the Head.

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

Community User Name	
Signed	
Date	

Appendix B

Liskeard School and Community College

Computer Resources – Acceptable Use Policy
Student Guidelines September 2018

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you do not keep to the points listed below, access to the Internet and school ICT facilities will be denied and you will be subject to disciplinary action.

Equipment

- Do not attempt to install or store programs of any type on the school computers.
- Damaging, disabling, tampering with or otherwise harming the operation of computers, or intentionally wasting resources puts your and other people's work at risk, and will cut short your time with the ICT equipment. Do not do it.
- Only use the computers for educational purposes. Activities such as social media, chat, buying or selling goods, gaming, watching non-educational movies and videos are strictly forbidden.
- If you chose to bring your own ICT equipment into school then you are responsible for its safety.

Security and Privacy

- Protect your work by keeping your password to yourself; NEVER use someone else's logon name or password.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted as this is a form of bullying in line with our school behaviour policy and could also lead to criminal action.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the standard settings is forbidden and may put you or your work at risk.
- All your internet activity is logged and your home drive monitored. Any inappropriate use is reported to your Head of Year who will decide on a sanction. This could involve informing your parents/carers; detention; Internal Exclusion, or in extreme cases referral to the Head Teacher and External Exclusion.

Internet

- Do not reveal personal information about yourself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- NEVER arrange to meet someone you have met online. They may not be who they say they are! Be aware of 'stranger danger.'
- Immediately report any unpleasant or inappropriate material or messages or anything that makes you feel uncomfortable when I see it on-line.
- You should access the Internet only for study or for school authorised/supervised activities in lesson time.
- You are permitted to use your own or school devices for leisure reasons outside of lesson time as long as you keep within the Behaviour for Learning Policy.
- Only access suitable material – using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is forbidden. If you accidentally access such a site then it is important you report it to a member of staff immediately.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- 'Chat' activities take up valuable resources which could be used by others to benefit their studies, and you can never be sure who you are really talking to. For these reasons 'chat' rooms must not be used in school.
- These rules also apply when using your own devices (mobile phones/tablets) in school.
- Creating Facebook or other social media pages in the name of 'Liskeard School' is strictly not allowed.
- Taking pictures/video footage of staff is not allowed.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is NOT acceptable.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.

- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff. The sending or receiving of an email containing content likely to be unsuitable for children or schools is strictly forbidden.

Printing

- All students need to be aware of the need to reduce waste and when it comes to printing we expect computer users to act in a responsible manner. Check "Print Preview" before printing, copy text and pictures/images from the Internet into an application like WORD, rather than printing straight from the Internet. Only send a job to the printer once and inform staff if it does not print – DO NOT send repeat prints.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Student Name: _____ Signature: _____

Tutor Group: _____

I have read and understand the above.

Parent/Guardian Name: _____ Signature: _____

Appendix C

Liskeard School and Community College

Computer Resources – Acceptable Use Policy
Staff Guidelines September 2018

Please read this document carefully. Violation of these provisions may be subject to disciplinary action.

The school has provided computers for use by staff, offering access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these school resources, and help to ensure they remain available to all. The use of computers for personal purposes, social media, e-bay, e-shopping etc during the school working day is inappropriate.

Equipment

- Do not attempt to install or store programs of any type on the school computers. If you need a new programme installed, please submit a helpdesk ticket and the technical staff will access the software for you and install, if appropriate.
- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work and the students learning at risk.
- Only use the computers for educational purposes.
- Only use files brought in on removable media (such as memory sticks etc) if they are clean of viruses. If in doubt consult with the IT technicians.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.
- You are responsible for the safety of ICT equipment (eg: laptops, media devices, cameras, etc) loaned to you by the school. If you lose these items or unreasonable damage is caused to them then you will be expected to pay for repairs or replacements.

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- It is critical that you log off when not using your computer and never let students use any staff computer.
- If you are away from your laptop even for a short while, make sure that you lock it first so that no-one can gain access to it.
- **Do not allow anyone to use your school issued laptop**. No-one, including staff, should have access to your desktop or documents.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security settings on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- Do make regular back-ups and save your work folders onto the main servers (H drive) or your One Drive. For GDPR purposes, avoid saving data to the computer or unencrypted media devices.
- IT technicians may review your files and communications from time to time to ensure that the system is being used responsibly.
- All departments/faculties will be requested to give their laptops to the ICT team in order for them to clear any history from previous users.
- If taking any student data/personnel information home, then any media device should be encrypted. We have a duty to comply with data protection guidelines under GDPR.

Internet

- You should access the Internet only for school related activities.

- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted and is a criminal offence.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- The use of school IT equipment for 'chat' rooms/social media purposes is not appropriate unless this is directly related to the education of students and conforms with policy guidelines
- Ensure that if you are searching for images "live" on the internet that your projector is switched off and that your screen cannot easily be overlooked by students.
- If recommending an unfiltered site to students, ensure you have checked it for suitability beforehand.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not acceptable.
- It is good practice to re-read your email before sending it and be aware that the message might be misconstrued. Always check the distribution list and ensure that you are sending it to only the people that really need to read it.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of SLT. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.

You should be aware that sites visited on the internet are logged by the IT system, and work areas and emails can be monitored.

Additional action may be taken by the school in line with existing staff disciplinary procedures if required. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Name …… Signature ……

Date ……..

Liskeard School & Community College is committed to safeguarding and promoting the welfare of children.

Appendix D

Preventing radicalisation

Protecting children from the risk of radicalisation should be seen as part of schools' and colleges' wider safeguarding duties and is similar in nature to protecting children from other forms of harm and abuse. During the process of radicalisation, it is possible to intervene to prevent vulnerable people from being radicalised.

Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism.[1] There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. It can happen in many different ways and settings. Specific background factors may contribute to vulnerability which are often combined with specific influences such as family, friends or online and with specific needs for which an extremist or terrorist group may appear to provide an answer. The internet and the use of social media, in particular, has become a major factor in the radicalisation of young people.

As with other safeguarding risks, staff should be alert to changes in children's behaviour which could indicate that they may be in need of help or protection. Staff should use their judgement in identifying children who might be at risk of radicalisation and act proportionately, which may include making a referral to the Channel programme. As with any safeguarding concern, staff are directed to report this to the Designated Safeguarding Lead (DSL) or Assistant DSLs.

In line with *Keeping Children Safe in Education (Sept 2018),* Liskeard School and Community College (LSCC) has a duty to have "due regard[2] to the need to prevent people from being drawn into terrorism."[3] This duty is known as the Prevent duty, which builds on existing local partnership arrangements (e.g. Local Safeguarding Children Board) and recognises the importance of effective partnership with parents/carers to spot any signs of potential radicalisation. At LSCC, staff are required to complete face to face training or an e-learning channel awareness programme[4], which focusses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. It provides a mechanism for schools to make referrals if they are concerned that an individual might be vulnerable to radicalisation. Staff at LSCC are provided with a hard copy of Part 1 and Annex A of *Keeping Children Safe in Education (Sept 2018)* and asked to sign that they have read and understood this.

The Government has launched educate against hate[5], a website designed to equip school and college leaders, teachers and parents with the information, tools and resources they need to recognise and address extremism and radicalisation in young people.

- [1] Extremism is vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs, including calls for the death of members of our armed forces, whether in this country or overseas.
- [2] "having due regard" means that the authorities should place an appropriate amount of weight on the need to prevent people being drawn into terrorism when they consider all the other factors relevant to how they carry out their usual functions.
- [3] "Terrorism" for these purposes has the same meaning as for the Terrorism Act 2000 (section 1(1) to (4) of that Act).
- [4] http://course.ncalt.com/Channel_General_Awareness/01/index.html
- [5] http://educateagainsthate.com