CLAVERHAM COMMUNITY COLLEGE

DRAFT

E-Safety Policy

September 2015

Approved:

Date:

Reviewed:

Development, Monitoring and Review of this Policy

This e-safety policy has been developed by a working group made up of:

- *Principal and Senior Leaders*
- *E-Safety Coordinator*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Pupils via the School Council and senior prefects*
- *Governors*
- *Parents and Carers via the website and PTA*

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governing Body*	*September 2015*
The implementation of this e-safety policy will be monitored by the:	*E-Safety Coordinator*
Monitoring will take place at regular intervals:	*Annually*
The *Governing Body* will receive a report on the implementation of the e-safety policy and any e-safety incidents once a year or more frequent if any significant incidents occur.:	*Annually*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*September 2016*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer (LADO), Police, Social Services*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of*
  - *pupils*
  - parents / carers
  - *staff*

Scope of the Policy

.

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

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of pupils 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 e-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 e-safety behaviour that take place out of school.

.

Roles and Responsibilities

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

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:

- regular meetings with the E-Safety Co-ordinator.
- regular monitoring of e-safety incident logs.
- regular monitoring of filtering / change control logs.
- reporting to the Governing Body.

Principal and Senior Leaders

- The Principal 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 Principal and another member of the 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.

  (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority Personnel and other relevant body disciplinary procedures).
- The Principal is responsible for ensuring that the E-Safety Coordinator 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 Principal 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 ICT manager will meet with his/her line manager at regular intervals.
- The Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-Safety Coordinator

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / 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 Local Authority / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- meets regularly with E-Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting of *Governors*
- reports regularly to Senior Leadership Team

Network Manager and Technical staff:

The *Network Manager* is responsible for ensuring:

- that the College's technical infrastructure is secure and is not open to misuse or malicious attack
- that the College meets required e-safety technical requirements and any Local Authority E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- filtering settings are applied and updated on a regular basis and its implementation is not the sole responsibility of any single person. CCC filtering is done via the internet connection provided by ESCC.
- 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 / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal, E-Safety Coordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in College policies

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current College e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Principal or E-Safety Coordinator for investigation / action / sanction
- all digital communications with pupils/ parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils 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

Child Protection Officer

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

.

Pupils

- are responsible for using the College digital technology systems in accordance with the Pupil Acceptable Use Policy.
- have a good understanding of safe and responsible practices with regard to e-safety and be able to put these into practice.
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking or use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the College's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet or mobile devices in an appropriate way. The College will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national or local e-safety campaigns and literature. Parents and carers will be encouraged to support the College in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to parents' sections of the website and on-line pupil records.

Community Users

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

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* 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 a focus across areas of the curriculum and staff should reinforce e-safety messages through 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:

- E-safety should be provided as part of ICT, Computing, PHSE and other lessons. This should be regularly revisited;
- Key e-safety messages should be reinforced as part of a planned programme of assemblies, tutorial and PSHE activities;
- Pupils should be taught about the importance of online safety in terms of their use of the internet and social media;
- Pupils should be taught to be aware of the malicious intent and legality of some online content;
- Pupils should be taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information;
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Pupils should be taught the relevance of their digital footprint and the implications of making poor choices with regard to the information and images that represent them in the digital environment;
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school;
- Staff should act as good role models in their use of digital technologies the internet and mobile devices;
- in lessons where internet use is pre-planned, it is best practice that pupils 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 pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit;
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents and Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Letters, newsletters, web site,
- Parents / Carers evenings / sessions

- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers see Internet safety link on the college website

Education & Training – Staff / Volunteers

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: (select / delete as appropriate)

- 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.
- 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 Acceptable Use Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.
- The E-Safety Coordinator will provide advice, guidance and training to individuals as required.

Training – Governors

Governors should take part in e-safety training and awareness sessions, with particular importance for those who have responsibilities in technology, e-safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation.
- Participation in school training or information sessions for staff or parents (this may include attendance at assemblies or lessons).

Technical – Infrastructure, Equipment, Filtering and Monitoring

The College will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities

- College technical systems will be managed in ways that ensure that the College meets recommended technical requirements .
- There will be regular reviews and audits of the safety and security of school academy technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to College technical systems and devices.
- All users will be provided with a username and secure password by the ICT Network Manager) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every (90 days).
- The administrator passwords for the College ICT system, used by the Network Manager and ICT Support staff must also be available to the *Principal* and SMT .
- The ICT Network Manager 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 pupils. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- College technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed). Users report verbally to the ICT Network Manager or the E safety Coordinator.
- 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 that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school .

Bring Your Own Device (BYOD)

- Staff guidance on bringing your own device into school is contained within the Staff Use of ICT and Data Policy.
- Pupils are currently not permitted to bring their own devices into school.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents, carers and pupils 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 pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- 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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained via the ViA signed by parents when they enter the school.
- Pupil's / Pupil's work can only be published with the permission of the pupil / pupil and parents or carers.

Data Protection

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

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The College must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing.
- It has a Data Protection Policy.
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.

Staff 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.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system,

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software.
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff can find more detail in the Use of ICT and Data Policy

.

Communications

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

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

When using communication technologies the school considers the following as good practice:

- The official College email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the College email service to communicate with others when in school, or on College systems (eg by remote access).
- Users must immediately report, to the nominated person – in accordance with the College policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat, etc) must be professional in tone and content. These communications may only take place on official (monitored) College systems. Personal email addresses, text messaging or social media must not be used for these communications.
- • Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

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

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/colleges/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *College* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *College* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Further guidelines for staff are detailed in the Use of ICT and Data Policy.

The *College's* use of social media for professional purposes will be checked regularly by the e-safety officer to ensure compliance with the Use of ICT and Data Policy.

Unsuitable or 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. The school policy restricts usage as follows:

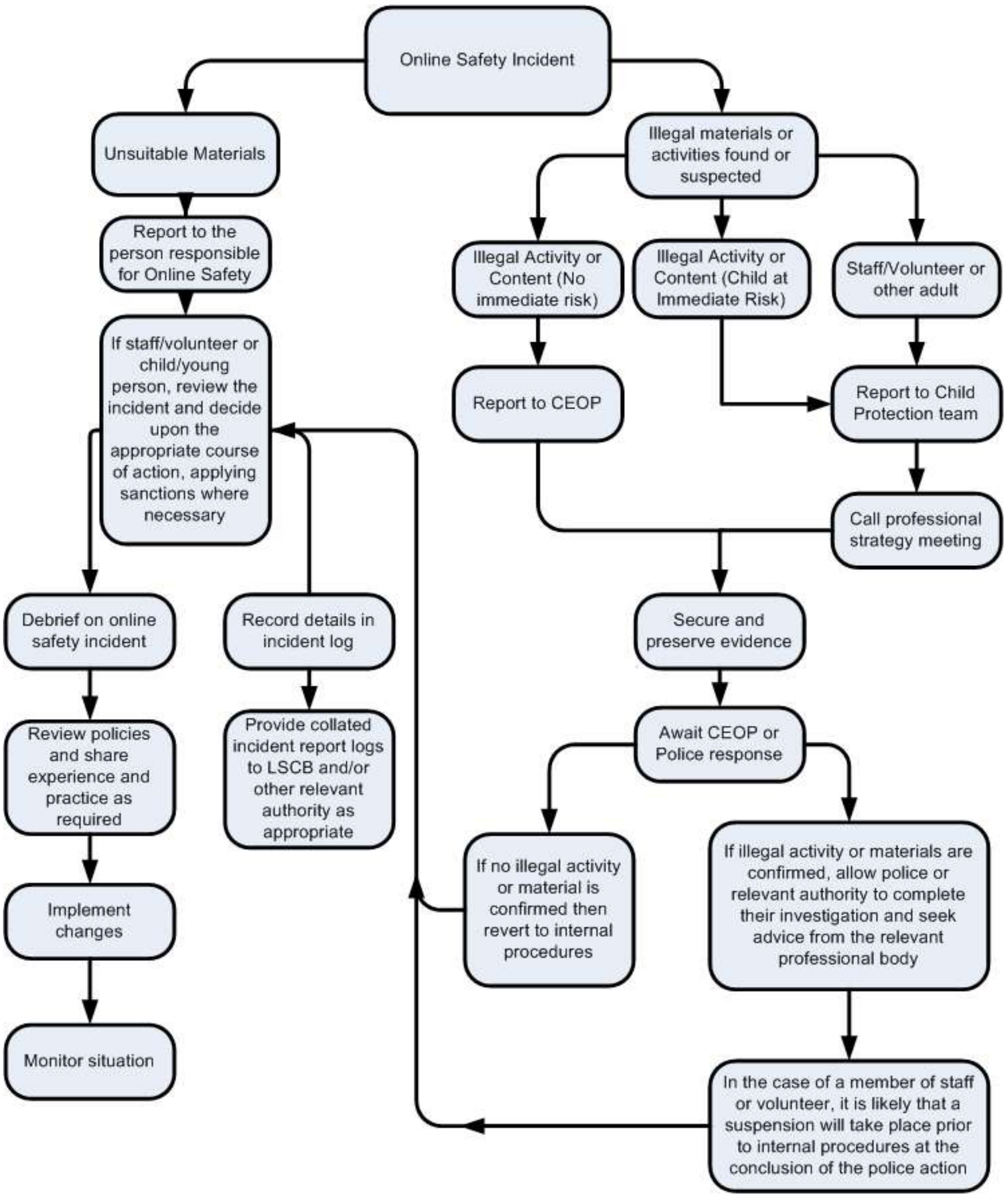
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –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
	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	
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 College					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 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			
On-line gaming (non educational)					x	
On-line gambling					x	
On-line shopping / commerce					x	
File sharing			x			
Use of social media					x	
Use of messaging apps					x	
Use of video broadcasting eg Youtube			x			

Responding to incidents of misuse

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 (see “User Actions” above).

Illegal Incidents

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 and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the school 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, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *College* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

College Actions & Sanctions

It is more likely that the College will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour or disciplinary procedures.

Appendices

- Pupil Acceptable Use Agreement
- Community User Acceptable Use Agreement
- Record of reviewing devices / internet sites (responding to incidents of misuse)
- Reporting Log
- Training Needs Log

CLAVERHAM POLICY FOR THE ACCEPTABLE USE OF INFORMATION COMMUNICATION TECHNOLOGY (ICT)

The College is committing increasingly large resources towards ensuring that pupils, adult students and staff benefit from ICT facilities that are of a high standard, reliable and readily available. It is important that **all** users of Claverham's computer network appreciate that enjoyment of these facilities is accompanied by responsibilities that must be taken seriously. The purpose of this document is to clearly define these responsibilities.

1. Users must treat all equipment with appropriate care at all times.

- Food and drink must not be consumed around any computer system.
- Keyboards and mice are essential components of every computer system. Users must not tamper with them or move them between computers. Inform a member of staff if there is a problem.
- Printers are complex pieces of equipment. Pupils may refill them with paper when necessary when supervised by a member of staff, but must never attempt to replace inkjet or toner cartridges.

2. Users may only access their own folders and the '*shared documents*' folders.

- No user is permitted to access other users' files stored on the network by using their password or any other means.
- Users may store or retrieve files on their own CD/DVD, USB flash drive ('memory stick') or memory card, but these must not be used to bring unacceptable material or any software into school.
- Offensive material of any type must not be stored in users' folders. Users should be aware that their network folders are not private and may be scanned for inappropriate or excessively large files, which may be deleted without warning and/or passed onto senior staff for further action.
- Users must keep their network password secure. This means it must **never** be revealed to another user.

The password is for your protection - it stops other users accessing your work and impersonating you.

3. Users must not interfere with the operation of the network, a workstation or any installed software.

- No attempt may be made to alter network, workstation or software settings or configurations.
- Users must not attempt to install any other software from any other source - it can cause serious problems with existing software packages and make a workstation temporarily unusable.
- All software used within the College is subject to copyright and it is illegal for any user to take copies of any software package.

4. Internet access must not be abused in any way.

- Users must not knowingly attempt to visit web-sites containing offensive material, e.g. any site that is of a sexual, racist, or violent nature.
- Both inside and outside of school, users must not post or publish material concerning any members of the College community to external web-sites such as social networking sites *(Facebook, YouTube, Twitter etc).*
- Users must not download files that have no relevance to their work in school.
- Users must not send any e-mail or other message that could cause offence or distress in any way. Users should be aware that **all Internet use is monitored and recorded**. E-mail messages sent using the College facilities are not private and are subject to scrutiny.
- Users must **never open** and should immediately delete e-mail attachments of unknown content. These are often computer viruses and could cause serious disruption to the network.

5. Consider the needs of other users.

In computer rooms at lunch times priority must be given to pupils working on examination coursework and other school work. Please do not occupy a workstation unless you really need to use it.

Any misuse of our computer network will be taken very seriously. Deliberate acts of vandalism or abuse will be referred to senior staff and may result in withdrawal of part or all access to the College ICT facilities and exclusion of the user(s) concerned. The time taken to repair problems resulting from a user's activities will be charged to them at the market rate. Any illegal activities may be referred to the relevant authorities.

Please make full use of the ICT facilities available around the College. We hope you will enjoy using them and develop confidence and expertise in using ICT in much of your school work.

Claverham Community College

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of College digital technologies will be responsible users and stay safe while using these systems and devices
- that College systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the College

- I understand that my use of College) systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user’s files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, 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 school device, nor will I try to alter computer settings, unless I have permission to do so.
- 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, however this may have happened.
- 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 if I fail to comply with this Acceptable Use Agreement, the College has the right to remove my access to school systems / devices

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.

Name

Signed Date

.

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	**Reason for concern**

Conclusion and Action proposed or taken

.

Reporting Log

Reporting Log Group …………………………………………………………						
Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Training Needs Audit

Training Needs Audit Log Group .... Date						
Name	Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date