CTC Kingshurst Academy
E-Safety Policy 2016/2017

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within the CTC Kingshurst Academy ("the CTC") and in their lives outside the CTC.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work at the CTC are bound. This e-safety policy aims to help to ensure safe and appropriate use. The development, implementation and continual review of this policy should involve all members of the CTC community including the Principal and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves."

The use of these exciting and innovative tools in the CTC and at home has been shown to raise educational standards and promote student achievement.

However, the use of these new technologies can put young people at risk within and outside the CTC. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorized access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers, or the risk of radicalization
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other CTC policies (e.g. behaviour, anti-bullying and child protection policies).

It is impossible to eliminate these risks completely and it is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed.

The CTC must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

1. Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a members of the SLT in consultation with staff and students.

The CTC will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students
    - parents
    - staff

2. Scope of the Policy

This policy applies to all members of the CTC community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of CTC ICT systems, both on and off the CTC premises.

The Education and Inspections Act 2006 empowers Headteachers and Principals, to such extent as is reasonable, to regulate the behaviour of students when they are off the CTC 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 CTC, but are linked to membership of the CTC.

The CTC will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place outside of the CTC.

3. Roles and Responsibilities

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

3.1. 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 Governing Body receiving regular information about e-safety incidents and monitoring reports. The Systems team will regularly update Governors via internal publications and meetings.

3.2. Principal and Senior Leaders:

The Principal is responsible for ensuring the safety (including e-safety) of members of the CTC community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator / Officer.

The Senior Leadership Team, will ensure that there is a system in place to allow for monitoring and support of those in the CTC 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 which includes IT support, HIPs, Form Tutors etc.

3.3. E-safety Officer

The E-safety Officer takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the CTC e-safety policies / documents. This includes:

- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- liaising with the Local Authority where appropriate
- liaising with IT support staff
- reporting regularly to SLT and governors.

3.4. Data Manager

The Data Manager receives reports of e-safety incidents, creates a log of incidents to inform future e-safety developments and reports regularly to E-safety Officer

3.5. Network Manager / IT Support:

The Network Manager is responsible for ensuring:

- that the CTC's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the CTC meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Government E-Safety Policy and guidance
- that users may only access the CTC's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the CTC's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that he keeps 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 in order that any misuse / attempted misuse can be reported to the E-Safety Officer or other appropriate member of staff
- that monitoring software / systems are implemented and updated as agreed in CTC policies

3.6. Teaching and Support Staff

Teacher and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current CTC e-safety policy and practices
- they have read, understood and signed the CTC Staff Acceptable Use Policy

- they report any suspected misuse or problem to a HIP/Child Protection Officer/E-Safety officer for investigation
- digital communications with students (email / Connect platform / voice) should be on a professional level and only carried out using official CTC systems
- e-safety issues are embedded in all aspects of the curriculum and other CTC activities
- students understand and follow the CTC e-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 CTC activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current CTC policies with regard to these devices
- in lessons where internet use is pre-planned students 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

3.7. Child Protection Officer:

The Child Protection Officer should be trained in e-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 adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

3.8. Students:

Students are responsible for using the CTC ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to CTC systems. They should:

- 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 CTC policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand CTC policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies outside of the CTC and realise that the CTC's E-Safety Policy covers their actions outside of the CTC, if related to their membership of the CTC

3.9. 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. 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 CTC will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website /Connect platform and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student Acceptable Use Policy
- accessing the CTC website / Connect platform / on-line student records in accordance with the relevant CTC Acceptable Use Policy.

3.10. Community Users:

Community Users who access CTC ICT systems will be expected to sign a Community User AUP before being provided with access to CTC systems.

4. Policy Statements

4.1. Education – 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 e-safety is therefore an essential part of the CTC's e-safety provision. Children and young people need the help and support of the CTC to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT and PHSE lessons and should be regularly revisited. This will cover both the use of ICT and new technologies within and outside the CTC
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities
- Students will be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Students will be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside of the CTC
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems and the internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

4.2. Education – parents / 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 and regulation of the children's on-line experiences. Parents 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.

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

- Letters, newsletters, web site
- Parents evenings

4.3. Education - Extended Services

The CTC will offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e-safety will also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

4.4. Education & Training – Staff

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. An audit of the e-safety training needs of all staff will be carried out regularly
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the CTC e-safety policy and Acceptable Use Policies

4.5. Training – Governors

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

4.6. Technical – infrastructure / equipment, filtering and monitoring

The CTC will be responsible for ensuring that its 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:

- There will be regular reviews and audits of the safety and security of CTC ICT systems
- Servers, wireless systems and cabling will be securely located and physical access restricted
- All users will have clearly defined access rights to CTC 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 Data Manager.
- All users will be provided with a username and password for all CTC systems by IT Support who will keep an up to date record of users and their usernames. Users will be required to change their password every term.

- The “master / administrator” passwords for the CTC ICT system, used by the Network Manager will also be available to the Director of IT or other nominated leader and kept in a secure place (e.g. CTC safe)
- Users will be made responsible for the security of their username and password, 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.
- The CTC maintains and supports the filtering service provided by Websense.
- 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 and carried out by a process that is agreed by the Vice Principal or Director of IT.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and Director ICT. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Systems Team
- IT Support regularly monitor and record the activity of users on the CTC 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
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager or E-Safety Officer.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the CTC systems and data.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the CTC system.
- An agreed policy is in place regarding the downloading of executable files by users
- An agreed policy is in place regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on laptops and other portable devices that may be used outside of the CTC. (see CTC Remote Access Policy for further detail)
- The CTC infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the CTC site unless safely encrypted or otherwise secured.

5. Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- 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.

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

6. Use of digital and video images - 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 CTC 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 will 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.
- Staff are allowed to take digital / video images to support educational aims, but must follow CTC policies concerning the sharing, distribution and publication of those images and must check with the Data Manager that authorisation for this has been granted by the parent/carer. Those images should only be taken on CTC 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 CTC into disrepute. Staff must not use mobile technology with camera or recording facilities in changing areas.
- 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' 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 before photographs of students are published on the CTC
- Student's work can only be published with the permission of the student and parents or carers.

7. 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.

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, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device 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

8. Communications

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

	Staff & other adults				**Students**			
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 CTC	**X**				**X**			

Making phone calls in lessons				X				X
Making phone calls in social time	X					X		
Use of mobile functions e.g. cameras and recording facilities in lessons		X				X		
Use of mobile functions e.g. cameras and recording facilities in social time	X					X		
Use of hand held devices eg PDAs, Smart Phones	X					X		
Use of personal email addresses in CTC, or on CTC network		X				X		
Use of CTC email for personal emails		X				X		
Use of personal chat rooms / facilities		X				X		
Use of personal instant messaging		X				X		
Use of social networking sites		X				X		
Use of personal blogs		X				X		

- CTC systems that provide social facilities are closed systems and are a protected environment therefore this access is allowed.
- The official CTC email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the CTC email service to communicate with other staff and students.
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) CTC systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the CTC website and only official email addresses should be used to identify members of staff.

9. Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from CTC and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The CTC 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 inside or outside the CTC when using CTC equipment or systems. The CTC policy restricts certain internet usage as follows:

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
- promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- 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 CTC or brings the CTC into disrepute
- Using CTC systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the CTC
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gaming (non educational)
- On-line gambling
- File sharing

10. Responding to incidents of misuse

It is hoped that all members of the CTC community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the

policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Contact a member of the senior leadership team as a matter of urgency.

It is more likely that the CTC 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 CTC community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

11. Policy review

This policy will be kept under review in order to keep it in line with relevant legislation and modifications authorised by the governing body and the SLT.

Policy owner: VP for Inclusion & Safeguarding
Supported by: Director for Social, Emotional and Mental Health

Authorisation and Issue				
Action	**Date**	**Committee / Position**	**Name**	**Signature**
Approved	01.09.16	Chair of Governors	Angela Pocock	
Issued	01.09.16	Principal	Damon Hewson	
Annual Review	June – August 2017 (for September 2017)			

Acceptable Use Policies

Student ICT Acceptable Use Policy

The CTC Kingshurst Academy will try to ensure that students will have good access to ICT to enhance their
learning and will, in return, expect students to agree to be responsible users. All students are required to
agree to the following before being given access to the Academy's ICT network and equipment:

Acceptable Use Policy Agreement

I understand that I must use Academy's ICT systems in a responsible way, to ensure that there is no risk to my safety or to that of others.

For my own personal safety:

- I understand that the CTC Kingshurst Academy will monitor my use of the ICT systems.
- I will not share my username or password, nor will I try to use any other person's username and password.
- I will not attempt to access illegal or offensive content online.
- I will not disclose or share personal information about myself or others when online.
- I will inform a member of staff if I see any inappropriate material or messages, or anything that makes me feel uncomfortable on-line.

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

- I will respect other's work and property and will not access, copy, remove or otherwise alter any other user's files.
- I will treat the Academy's ICT equipment with respect and not do anything that is likely to damage it.
- I will report any damage I see to a member of staff.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language.
- I will not take or send images of anyone without their permission.
- 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.

I understand that I am responsible for my actions, both inside and outside of CTC Kingshurst Academy:

- I understand that CTC Kingshurst Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, when I am outside of the Academy and where they involve my membership of the CTC Kingshurst Academy community.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the Academy's ICT network, contact with parents or exclusion.

Name: _____ Signature:_____

Tutor Group:_____ Date:_____

CTCKA Staff Acceptable Use

All staff working with ICT equipment at the CTC Kingshurst Academy must ensure that they have read and agree to abide by these terms.

- Access for staff and students to the network can only be made via an authorised user account and password, which is confidential to the individual and should not be made available to any other person;
- Activity that threatens the integrity of the CTC's ICT systems or activity that attacks or corrupts other systems is forbidden;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of materials must be respected. When publishing materials on the internet, CTC network or Connect platform staff must ensure they have appropriate permission/ copyright for the number of users who will have access to it or a site/ CTC licence;
- Posting anonymous messages and forwarding chain letters is forbidden;
- The same professional levels of language and content should be applied in email as for letters or other media. Staff should not include anything in an email that they would not include in a letter or say on the telephone. Poorly written emails to external contacts can reflect a poor image of the CTC. Staff should use proper English and spelling in emails – not text message short cuts;
- Staff should take care when addressing emails, particularly when using address groups, in order to send them only to those recipients who will have an interest or "need to know". Staff should be aware that if they use multiple addresses on email messages they send the whole list of addresses to all recipients and that this may not be advisable, or welcomed by all those recipients.
- Before forwarding a received email to a third party, in some instances it may be appropriate to notify, or even seek permission from, the original sender, to preserve confidentially.
- Staff should take account of the Data Protection Act (see below) when considering sending personal data by email that could be linked to a named individual. It should be remembered that staff do not have absolute control over who will read their emails

or who they will be forwarded to. The Data Protection Officer (the Director of Finance) should be consulted if staff have doubts about how to proceed in connection with personal data.

- Staff should not use the CTC email to express views or pass on material which could be construed as canvassing, lobbying, advocacy or endorsement, particularly if this is commercially or politically based and if this expresses a personal rather than a CTC view. If in doubt, staff should consult their line manager.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Users should be aware that internet use is 'filtered' and computer use is monitored.
- If a user accesses any site on the internet which they feel is in appropriate, or if they wish to access a site which is currently blocked but which they feel should be accessible, it should be reported to the Network Manager as soon as possible.
- Misuse of CTC computer equipment, email or the Internet are serious offences.
- The CTC reserves the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request.
- All computers and electronic equipment must be either kept in sight of an adult or securely locked away, never left accessible to students without supervision;
- Teachers should ensure that computers are treated well by students and used in a manner consistent with supporting learning (not to play games etc.)
- Teachers should ensure that pupils only use their mobile phones or other electronic devices in the CTC when they have express permission to do so;
- All faults and problems should be reported promptly to the Network Manager
- Equipment must be returned to ITS when required for repair, maintenance or upgrade.
- Laptops and other electronic equipment are loaned to staff for use within the CTC and at home when working on CTC business. Staff must take full responsibility for the security of this equipment.
- Staff must only use legal, authorised software and must ensure any software they install themselves is legal. Staff must not install their own software onto CTC computers, unless given express permission by the network manager.

Social Networking Sites

If staff do access social networking sites in their own time on their personal computer, the following guidelines should be adhered to in order to protect themselves:

- Do not allow current students to be recorded as a "friend" or "contact"
- If former students are allowed to be recorded as a "friend" or "contact", strictly limit their access to your profile. Former students often have friends and/or siblings who are still at the CTC.
- Do not post personal information or contact details on such sites.
- Always consider your colleagues. Do not put your colleagues at risk by posting photos of them on your pages that could in any way be deemed to be risqué or cause them to be accused of unprofessional conduct.

- Give special consideration to groups. Your name will potentially be associated with the comments made by other site users.
- Hide your profile to public users where possible.
- Do not voice your opinions regarding work. These sites are in the public domain. You cannot control who can see your posts on your friends' pages.

Personal email / websites / instant messengers.

In order to protect themselves:
- Staff should not give their personal email address to students
- Staff should be careful with personal websites – students will find them and the information and pictures posted on them.
- Staff should not use personal messengers to chat to students.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from CTC and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The CTC believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities inside or outside the CTC when using CTC equipment or systems. The CTC policy restricts certain internet usage as follows:
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate (including email) or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- 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 CTC or brings the CTC into disrepute
- using CTC systems to run a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the CTC

- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- on-line gaming (non educational)
- on-line gambling
- file sharing

Responding to incidents of misuse

It is hoped that all members of the CTC community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or through deliberate misuse.
Illegal activity

The principal or another member of the senior leadership team should be contacted urgently if any member of the CTC staff becomes aware of, or suspects, any apparent or actual misuse of CTC equipment or systems which appears to involve illegal activity. Examples of such activity include, but are not limited to:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Inappropriate use

It is more likely that CTC staff will need to deal with incidents that involve inappropriate rather than illegal misuse of CTC equipment or systems. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the CTC community are aware that incidents have been dealt with. Incidents of misuse by students will be dealt in accordance with the CTC students' behaviour policy. Incidents of misuse by staff will be dealt with in accordance with the CTC staff disciplinary policy and procedures.

Signed: _____ Date:_____

Print Name:_____

Community User ICT Acceptable Use Policy

The CTC Kingshurst Academy will try to ensure that community users will have good access to ICT and will, in return, expect all to agree to be responsible users. All users are required to agree to the following before being given access to the Academy's ICT network and equipment:

Acceptable Use Policy Agreement

I understand that I must use Academy's ICT systems in a responsible way, to ensure that there is no risk to my safety or to others.

For my own personal safety:

- I understand that the CTC Kingshurst Academy will monitor my use of the ICT systems.
- I will not share my username or password, nor will I try to use any other person's username and password.
- I will not attempt to access illegal or offensive content online.
- I will not disclose or share personal information about myself or others when online.
- I will inform a member of the CTC staff if I see any inappropriate material or messages on-line.

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

- I will respect other's work and property and will not access, copy, remove or otherwise alter any other user's files.
- I will treat the Academy's ICT equipment with respect and not do anything that is likely to damage it.
- I will report any damage I see to a member of staff.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language.
- I will not take or send images of anyone without their permission.
- 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.

I understand that I am responsible for my actions, both inside and outside of CTC Kingshurst Academy:

- I understand that CTC Kingshurst Academy also has the right to take action against me if I am involved in incidents of inappropriate or illegal behaviour. This may include informing the police.

Name: _____ Signature:_____

Date:_____

Legislation

Users should be aware of the legislative framework under which this E-Safety Policy has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
    - Ascertain whether the communication is business or personal;
    - Protect or support help line staff.

The CTC reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the CTC context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The CTC is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the CTC site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Links to other organisations or documents

The following links may help those who may be called upon to review the CTC e-safety policy.

Child Exploitation and Online Protection Centre (CEOP)

http://www.ceop.gov.uk/

ThinkUKnow

http://www.thinkuknow.co.uk

CHILDNET

http://www.childnet-int.org/

INSAFE

http://www.saferinternet.org/ww/en/pub/insafe/index.htm

BYRON REVIEW ("Safer Children in a Digital World")

http://www.dcsf.gov.uk/byronreview/

Becta

Website e-safety section - http://schools.becta.org.uk/index.php?section=is

Developing whole school policies to support effective practice:

http://publications.becta.org.uk/display.cfm?resID=25934&page=1835

Signposts to safety: Teaching e-safety at Key Stages 1 and 2 and at Key Stages 3 and 4:

http://publications.becta.org.uk/display.cfm?resID=32422&page=1835

"Safeguarding Children in a Digital World"

http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_tl_rs_03&rid=13344

LONDON GRID FOR LEARNING

http://cms.lgfl.net/web/lgfl/365

KENT NGfL

http://www.kented.org.uk/ngfl/ict/safety.htm

NORTHERN GRID

http://www.northerngrid.org/index.php/resources/e-safety

NATIONAL EDUCATION NETWORK

NEN E-Safety Audit Tool: http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html

CYBER-BULLYING

DfE - Cyberbullying guidance

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Teachernet

http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/

Teachernet "Safe to Learn – embedding anti-bullying work in schools"

http://www.teachers.gov.uk/wholeschool/behaviour/tacklingbullying/safetolearn/

Anti-Bullying Network
http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org
http://www.cyberbullying.org/

East Sussex Council – Cyberbullying - A Guide for schools:
https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying/Pages/eastsussexandnationalguidance.aspx

References to other relevant anti-bullying organisations can be found in the appendix to the DCSF publication "Safe to Learn" (see above)

SOCIAL NETWORKING

Home Office Task Force - Social Networking Guidance -
http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce

Digizen – "Young People and Social Networking Services":
http://www.digizen.org.uk/socialnetworking/

Ofcom Report:
http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/

MOBILE TECHNOLOGIES

"How mobile phones help learning in secondary schools":
http://partners.becta.org.uk/index.php?section=rh&catcode=_re_rp_02_a&rid=15482

Mobile phones and cameras:
http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_mob_03

DATA PROTECTION AND INFORMATION HANDLING

Information Commissioners Office - Data Protection:
http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

BECTA - Data Protection:
http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_saf_dp_03

PARENTS GUIDES TO NEW TECHNOLOGIES AND SOCIAL NETWORKING:
http://www.iab.ie/

Resources

Links to other resource providers:

BBC Chatguides: http://www.bbc.co.uk/tees/chatguide/index.shtml

Kidsmart: http://www.kidsmart.org.uk/default.aspx

Know It All - http://www.childnet-int.org/kia/

Cybersmart - http://www.cybersmartcurriculum.org/home/

NCH - http://www.stoptextbully.com/

Chatdanger - http://www.chatdanger.com/

Internet Watch Foundation: http://www.iwf.org.uk/media/literature.htm

Digizen – cyber-bullying films: http://www.digizen.org/cyberbullying/film.aspx

London Grid for Learning: http://cms.lgfl.net/web/lgfl/safety/resources

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology)
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
DCSF	Department for Children, Schools and Families
ECM	Every Child Matters
FOSI	Family Online Safety Institute
HSTF	Home Secretary's Task Force on Child Protection on the Internet
ICO	Information Commissioners Office
ICT	Information and Communications Technology
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
Learning Platform	A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
LSCB	Local Safeguarding Children Board
MIS	Management Information System
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
SEF	Self Evaluation Form – used by schools for self evaluation and reviewed by Ofsted prior to visiting schools for an inspection
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol