E-SAFETY POLICY

March 2014

Aims of this Policy

- To acknowledge that the internet and other digital and information technologies are an essential part of the student's learning experience and a necessary tool for both staff and students.
- To ensure that all members of the Kineton High School community are able to use the internet and related communications technologies appropriately and safely on our ICT systems both in and out of school.
- To build students' resilience to the risks to which they may be exposed and the skills they need to deal with them.
- To give guidance to staff on access to images through technology, taking images of young people and the use of new technology, propriety and behaviour.
- To educate parents about the benefits and risks of new technologies and how they might effectively guide their children's use of them.

Some of the risks we aim to reduce are:

- Access to illegal, harmful or inappropriate images or other content including illegal downloading of music or video files and access to unsuitable video or internet games
- Unauthorised access to or loss of or sharing of personal information, including the

sharing or distribution of personal images without an individual's consent or knowledge

- Inappropriate communication or contact with others, including strangers, and the risk of being subject to grooming by those with whom students make contact on the internet
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

This policy works in conjunction with our Behaviour, Anti-bullying and Child protection policies and our ICT Acceptable Use Agreements for both staff and students.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the e-safety Policy and for reviewing its effectiveness. This will be carried out by the Student Committee receiving regular information about e-safety incidents and monitoring reports from the ICT Steering Group.

Headteacher and Senior Leaders:

- The Headteacher is responsible 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 ICT Steering Group and the Designated Child Protection Teacher.
- The Headteacher is responsible for ensuring that the ICT Steering Group and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher 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.
- The Headteacher will take the lead on any serious breach of our e-safety policy by a member of staff.

ICT Steering Group:

- Has a leading role in establishing and reviewing the school e-safety policies, procedures and curriculum for staff and students.
- 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 school ICT technical staff.

- Reviews reports of e-safety incidents to inform Governors on developments needed.
- Reports regularly to the Governors' Student Committee to discuss current issues, review incident logs and filtering logs

Network Manager
The Network Manager is responsible for ensuring:

- Taking day to day responsibility for e-safety issues
- The school's ICT infrastructure is implemented, secure and is not open to misuse or malicious attack.
- The school meets the e-safety technical requirements outlined in this Policy, the ICT Acceptable Use agreements and any relevant WCC policies and guidance
- Users may only access the school's networks through properly enforced password protection
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- He/she 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
- The use of the network, Virtual Learning Environment, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported as appropriate

Teaching and Support Staff
Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the ICT Acceptable Use Agreement for staff
- They report any suspected misuse or problem as appropriate
- Digital communications with students are only ever through our Virtual Learning Environment and only for matters related to learning
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the ICT Acceptable Use Agreement for students
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- ICT activity in lessons, extracurricular and extended school activities is actively monitored.
- E-safety issues related to the use of mobile phones, cameras and hand held devices are implemented

- Where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that any unsuitable material that is found in internet searches is reported to the network manager

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, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. Students should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information

Designated Child Protection Teacher

Should be trained in e-safety issues and know how to respond to incidents that arise from sharing of personal data , access to illegal or inappropriate materials, inappropriate on-line contact with adults or strangers, potential or actual incidents of grooming and cyber-bullying.

Students

- Responsible for using the school ICT systems in accordance with the ICT Acceptable Use Agreement for students, which they will be expected to sign before being given access to school system
- Should avoid plagiarism and uphold copyright regulations
- Report abuse, misuse or access to inappropriate materials to an appropriate adult
- Must follow school policies on the use of mobile phones, digital cameras and hand held devices.
- Must follow school policies on the taking or use of images and on cyber-bullying.
- Must understand that this policy applies when using digital technologies out of school

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and 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 school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, VLE and information about national and local e-safety campaigns and literature. Parents and carers will be responsible for endorsing (by signature) the ICT Acceptable Use Agreement for students.

The E-Safety Curriculum

The e-safety curriculum is led by the Learning Leader for ICT who is responsible for the overall planning, implementation and review of the programme in every year group. E-safety is taught discretely through the ICT curriculum and as part of the wider PSHE programme. A series of lessons conducted in each year group gradually explore the risks that young people can be exposed to, as well as how to minimise the risks and to report abuse effectively. Topics covered include cyber-bullying, staying safe when social networking, grooming, identity theft and reporting incidents effectively. CEOP materials are used to supplement these topics further.

Supporting and Educating Parents about e-safety issues
E-safety education is provided to parents through information events, letters, newsletters and our web site.

Supporting and Educating staff about e-safety issues
E-safety education will be provided to staff through our cycle of child protection training, additional CPD events as required, staff newsletters and our web site.

E-safety through our infrastructure

- There will be regular reviews and audits of the safety and security of school ICT systems through self-evaluation.
- Servers, wireless systems and cabling are securely located and physical access restricted
- All users have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager.
- All users will be provided with a username and password.
- The administrator passwords for the school ICT system, used by the Network Manager (or authorised person) are available to the Headteacher.
- 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 school maintains and supports the managed filtering service provided by Lightspeed.
- In the event of the Network Manager 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 Headteacher.
- Any filtering issues should be reported immediately to the Network Manager.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and the Designated Child Protection Teacher. If the

request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the ICT Steering Group

- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Agreements.
- An appropriate system is in place for users to report any actual or potential e-safety incidents to the Network Manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Users and the network is monitored to ensure that executable files are not run
- The school infrastructure and individual workstations are protected by up to date antivirus software.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured and only via a laptop or tablet.

E-safety and the use of digital and video images (Photographic and Video)

- When using digital images, staff should inform and educate students about the risks associated with taking, 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 or 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 or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Parents are required to send a written request to the Headteacher if they do not give permission for photographs of students to be published on the school website.

E-safety and 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
- Accurate, adequate, relevant and not excessive
- Kept no longer than is necessary
- Secure and processed in accordance with the data subject's rights
- Only transferred to others with adequate protection.

At all times, Staff must ensure that they:

- 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.

Where 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

E-safety and Communications

The official school email service may be regarded as safe and secure. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).Users need to be aware that email communications are 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. Staff should report to the Headteacher; students should report to their Head of House/Head of 6th Form

Any digital communication between staff and students or parents/carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat or social networking programmes **must not** be used for these communications.

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

E-safety and 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 should not engage in these activities in school or outside school when using school equipment or systems.

- Whilst systems are in place to prevent most of the following forms of behaviour, users shall not visit internet sites, make, post, download, upload, transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to child sexual abuse images, promotion of illegal acts. This includes obscenity, computer misuse and fraud, racism, promotion of any kind of discrimination or racial and 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 school or brings the school into disrepute.
- A user should not use school systems to run a private business.
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- 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
- On-line gaming that is not educational
- On-line gambling

Responding to incidents of misuse

There may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse, such as:

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

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school 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 by reporting concerns about members of staff to the Headteacher and concerns about students to the Designated Child Protection Teacher.

Monitoring

The ICT Steering Group will monitor the implementation and progress of this policy and report to the Governors' Student Committee

Evaluation

The impact of this policy will be evaluated by:

- the annual student and parent survey
- the log of e-safety incidents which are reported as child protection concerns (Child Protection Records)
- the log of e-safety incidents which are technical (Network Manager Logs)
- internet logs and filtering reports

Kineton High School

ICT Acceptable Use Agreement (Staff)

This agreement is made in accordance with the E-safety and Use of Social Networking and Internet sites policies

The ICT systems within school are made available to students, staff and other authorised persons to further enhance both educational and professional activities including teaching, research, administration and management. There has been a substantial investment in ICT to enable us to work more effectively and efficiently.

The school trusts you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties and with respect for your colleagues.

Any inappropriate use of the school's ICT facilities may lead to disciplinary action.

1. Use of equipment

ICT Equipment must be used appropriately and carefully looked after. Portable equipment, including laptops, should not be left unattended in a car, classroom or office. ICT Equipment that is on loan should be stored securely in the home.

Always ensure that the computer is left in full working order for the next user, and report any accidental damage to the ICT technician. Do not try to repair problems yourself.

Do not eat or drink near any ICT equipment.

Always get permission before installing, attempting to install or storing programs of any type on the computers.

Users who wish to use their own devices on the ICT network must have this authorised by the network manager.

You are expressly prohibited from:

- Seeking to gain access to restricted areas of the network
- Knowingly seeking to access data which you are not authorised to view
- Introducing any form of computer viruses
- Carrying out other hacking activities

2. Security, privacy and integrity

Protect your work by keeping your password to yourself. Never use someone else's logon name or password, and tell the ICT technician if you suspect someone else knows yours.

Log off or lock any workstation before leaving it, even for just a short period of time.

File storage areas must be used responsibly, and spring cleaned regularly. Your storage area may be reviewed to monitor this.

Ensure that work is backed up to a network location regularly.

Be aware of the threats posed by viruses and take steps to avoid infection of data and technology.

Users should not change, damage, dismantle, corrupt or destroy network components, equipment, software or data.

3. Data and information

All information relating to students, parents and staff (i.e. personal data) is confidential. You must treat it with the utmost care whether held on paper or electronically and must not disclose it to any other person unless authorised to do so.

You should exercise due care when collecting, processing or disclosing any personal data and should only do so on behalf of the school where it is necessary for your duties. The processing of personal data is governed by the Data Protection Act 1998 and schools are defined in law as separate entities for the purposes of complying with the act.

Individuals have the right to see all information the school holds on them (subject to any exemptions that might apply) so do not make any personal or inappropriate remarks about students, parents or colleagues on manual or computer records.

All aspects of communication are protected by intellectual property rights. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

4. The Internet

NB Your use of the internet is monitored by the school.

The internet should be used sensibly. Access is intended to be for school business or professional development. Any personal use is subject to the same terms and conditions and should be with the agreement of the headteacher.

When entering an internet site, always read and comply with the terms and conditions governing its use. Do not download any images, text or material which is copyright protected without the appropriate authorisation.

Do not download any images, text or material which is inappropriate or likely to cause offence.

Do not download any software without seeking permission from the network manager.

If you are involved in creating, amending or deleting the school's web pages or content on our websites, such actions should be consistent with your responsibilities and in the best interests of the school.

5. Email

NB Your use of the email system is monitored by the school.

Email access is intended to be for school business or professional development. Any personal use is subject to the same terms and conditions and should be with the agreement of the headteacher.

Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the school's business purposes.

Remember you are acting as a representative of Kineton High School and you should take as much care over your emails as you would over written communication. Be polite, use appropriate language and do not send unsuitable material.

The content of emails you send or receive will be subject to the same legal considerations and access to information rules as paper communications are. Remember, email is not a confidential means of communication, and the content of emails may reach a wider audience than originally intended.

Communication between you and students/parents should be made using your school email address.

Ensure emails are only sent to those for whom the information is relevant. Messages intended for all staff should be communicated using the weekly newsletter.

Incoming email should be treated with as much courtesy as incoming post. Check emails regularly, at least once a day. Reply promptly to all messages requiring a reply. Where this is not possible, a short email acknowledging receipt should be sent, which gives an estimate of when a detailed response will be sent.

Appreciate that other users might have different views from your own.

Only open attachments to emails if they come from someone you already know and trust.

If you receive an email containing material of a violent, dangerous, racist or inappropriate content, always tell the network manager.

Emails should not be relied upon as the sole method of communication for important messages.

I have read and fully understand the agreement. I agree to adhere to the Code of Practice, as detailed above

Signed____Date_____________

Print name____

Kineton High School

ICT Acceptable Use Agreement (Students)

The aim of this agreement is to allow all users to access and use computers for educational purposes. Remember that access is a privilege, not a right and inappropriate use will result in the privilege being withdrawn.

1. Use of equipment

Only use the computers for educational purposes.

Always ensure that the computer is left in full working order for the next user, and report any accidental damage to a member of staff. Do not eat or drink near any ICT equipment.

Do not install any of your own programmes on our network

2. Security and Privacy

Protect your work by keeping your password to yourself. Never use someone else's logon name or password, and tell a member of staff if you suspect someone else knows yours.

File storage areas must be used responsibly, and cleared of outdated material regularly. Staff may review your files and communications to monitor this.

3. The Internet

You should only access the internet for study or for school authorised activities.

Only access suitable material, and do not download or transmit any material which is unlawful, obscene or abusive.

Respect the work and ownership rights of others, both within and outside the school. This includes abiding by copyright laws.

You are not allowed to use chat rooms or social networking sites in school.

4. E - mail

People you contact or who contact you are not always who they seem. Do not give personal details or meet anyone you contact by e-mail ever.

Be polite, avoiding the use of inappropriate language.

Appreciate that other users might have different views from your own.
Only open attachments to e-mails if they come from someone you already know and trust.

If you receive an e-mail containing material of a violent, dangerous, racist or inappropriate nature, always tell a member of staff.

5. Printing

You will be allowed a weekly quota of free printing. Any printing you do after you have used up your quota will be charged for.

Please read this document carefully. It is an integral part of the school's Code of Conduct. Use of the computers, including Internet Use, will be monitored regularly. If you break these rules, access to the computers will be denied, and you will be subject to disciplinary action.

Student's name ____

Signature______________________________________Date_______________

Parent's name ____

Signature____Date_________________