INTRODUCTION

Materials on the Kent Trust Website have been used to inform this policy. (http://www.kenttrustweb.org.uk/Children/safeguards_esafety.cfm)

It has been updated to reflect amendments made in 'Keeping Children Safe in Education Sept 2016'

This policy has been developed to ensure that all adults in Abbey Woods Academy are working together to safeguard and promote the welfare of children and young people. This policy has been ratified by the Governing Body at the meeting and will be reviewed annually. E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

The Headteacher/ Manager or, in their absence, the authorised member of staff for e-safety has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

This policy complements and supports other relevant school and Local Authority policies.

The purpose of internet use in school is to help raise educational standards, promote pupil achievement, support the professional work of staff as well as enhance the school's management information and business administration systems.

The internet is an essential element in 21st-century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience.

A risk assessment will be carried out before children and young people are allowed to use new technology in schools and settings.

ETHOS

It is the duty of the school to ensure that every child and young person in its care is safe. The same 'staying safe' outcomes and principles outlined in the 'Every Child Matters' agenda apply equally to the 'virtual' or digital world. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures.

All staff have a responsibility to support e-Safe practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

E-safety is a partnership concern and is not limited to school premises, school equipment or the school day.

Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will dealt with in accordance with the school's Anti-Bullying and Behaviour Policy.

Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

ROLES AND RESPONSIBILITIES

The Headteacher /Manager of Abbey Woods Academy will ensure that:

- All staff should be included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- A Designated Senior Member of Staff for E-Learning/Safety is identified and receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding.
- All temporary staff and volunteers are made aware of the school's E-Learning/Safety Policy and arrangements.
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.
- Ensure that teaching staff are aware of the risks posed by online activity of extremist and terrorist groups
- Liaise with the LSCB to establish what advice and support they provide and their assessment of general risk in the local area

The Governing Body of the school will ensure that:

- There is a senior member of the school's leadership team who is designated to take the lead on E-Learning/Safety within the school. Mr Mottram - Headteacher
- Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority and CST procedures.
- All staff and volunteers have access to appropriate ICT training.

The Designated Senior Member of Staff for E-Learning/Safety will:

- Act as the first point of contact with regards to breaches in e-safety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff and volunteers on E-Safety.
- Ensure that all staff and volunteers have received a copy of the school's Acceptable Use of ICT Resources document.
- Ensure that all staff and volunteers understand and are aware of the school's E-Learning/ Safety Policy.
- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Discuss security strategies with the Local Authority particularly where a wide area network is planned.
- Regularly check files on the school's network.
- Ensure that staff and students are safe from terrorist and extremist materials when accessing the internet in school

TEACHING and LEARNING

Benefits of internet use for education

The internet is a part of the statutory curriculum and a necessary tool for staff and children and young people and benefits education by allowing access to worldwide educational resources including art galleries and museums as well as enabling access to specialists in many fields for pupils and staff.

Access to the internet supports educational and cultural exchanges between students worldwide, and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home.

The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with the Local Authority and DfE.

The internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives.

The internet offers opportunities for mentoring pupils and providing peer support for them and their teachers.

Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the children and young people.

Children and young people will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Children and young people will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Children and young people will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance.

Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

MANAGING INTERNET ACCESS

Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children and young people.

Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in online activities that will support the learning outcomes planned for the pupil's age and maturity.

Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Co-ordinator.

The school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law.

Pupils will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

MANAGING EMAIL

Personal email or messaging between staff and pupils should not take place.

Staff must use the school email address if they need to communicate with pupils about their school work e.g. study leave, course work etc.

Pupils and staff may only use approved email accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive email. Whole-class or group email addresses should be used at KS1 and below.

Pupils must not reveal details of themselves or others in any email communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.

Access in school to external personal email accounts may be blocked.

Excessive social email use can interfere with learning and will be restricted.

Email should be authorised before sending to an external organisation just as a letter written on school headed note-paper would be.

The forwarding of chain letters is not permitted.

Incoming email should be monitored and attachments should not be opened unless the author is known.

MANAGING WEBSITE CONTENT

Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

Photographs of pupils will not be used without the written consent of the pupil's parents/carers.

The point of contact on the school website will be the school address, school email and telephone number. Staff or pupils' home information will not be published.

The headteacher or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.

The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing.

Use of site photographs will be carefully selected so that any pupils cannot be identified or their image misused.

The names of pupils will not be used on the website, particularly in association with any photographs.

Work will only be used on the website with the permission of the pupil and their parents/carers.

The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

SOCIAL NETWORKING AND CHAT ROOMS

The school will control access to moderated social networking sites and educate pupils in their safe use.

Pupils will not access social networking sites e.g. 'My Space', 'Facebook' or 'Bebo'.

Pupils will be taught the importance of personal safety when using social networking sites and chat rooms.

Pupils will not be allowed to access public or unregulated chat rooms.

Pupils will only be allowed to use regulated educational chat environments and use will be supervised.

Newsgroups will be blocked unless an educational need can be demonstrated.

Pupils will be advised to use nick names and avatars when using social networking sites.

Staff will not exchange social networking addresses or use social networking sites to communicate with pupils.

Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a pupil is necessary, the agreement of a senior manager should always be sought first and language should always be appropriate and professional.

MOBILE PHONES, Smart Phones and other devices

Mobile phones will not be used by pupils at all on school premises and will be confiscated if found and parents will be asked to come to school and take the device home. If a child requires a mobile phone as they are traveling on public transport alone, then an agreement will be reached between the school and the parent on the safekeeping of the device until the pupil leaves the premises. For staff, mobile phones will not be used during lessons or formal times in school. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden and will be dealt with in accordance with the school's Anti-bullying and Behaviour Policies.

Staff will be issued with a school mobile phone where contact with pupils is necessary or where mobile phones are used to photograph school activities involving pupils.

The use of mobile technology is addressed in 'Keeping Children Safe in Education Sept 2016.

FILTERING

The school will work in partnership with parents/carers, the Local Authority, the DfE and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly.

If staff or pupils discover unsuitable sites, the URL **(address)** and content must be reported and the E-Safety Co-ordinator **Mr Mottram.**

Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk).

Regular checks by Senior Staff will ensure that the filtering methods selected are appropriate, effective and reasonable.

Filtering methods will be selected by the school in conjunction with the Local Authority and will be age and curriculum appropriate.

'Keeping Children Safe in Education Sept 2016 has established that, whilst trusts should do all that they can to protect children from potentially harmful and inappropriate online material, the measures that are taken should be reasonable, and they should not "overblock" the information available to children.

AUTHORISING INTERNET ACCESS

All staff must read and sign the school's 'Staff Code of Conduct for ICT' before using any school ICT resources and any staff not directly employed by the school will be asked to sign the school's 'Acceptable Use of ICT Resources' document before being allowed internet access from the school site.

The school will maintain a current record of all staff and pupils who are allowed access to the school's ICT systems.

The school will maintain a record of pupils whose parents/carers have specifically requested that their child be denied internet or email access.

Parents/carers will be asked to sign and return the school's form stating that they have read and understood the school's 'Acceptable Use' document and give permission for their child to access ICT resources.

Staff will supervise access to the internet from the school site for all pupils.

PHOTOGRAPHIC, VIDEO AND AUDIO TECHNOLOGY

When not in use all video-conferencing cameras will be switched off and turned towards the wall.

It is not appropriate to use photographic or video technology in changing rooms or toilets.

Staff may use photographic or video technology to capture to support school trips and appropriate curriculum activities.

Audio and video files may not be downloaded without the prior permission of the network manager.

Pupils must have permission from a member of staff before making or answering a video-conference call or making a video or audio recording in school or on educational activities.

Video-conferencing and webcam use will be appropriately supervised for the pupil's age.

ASSESSING RISKS

Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

In common with other media such as magazines, books and video, some material available through the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of internet access.

Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

The headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy is monitored.

Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.

INTRODUCING THE POLICY TO PUPILS

Rules for internet access will be posted in all rooms where computers are used.

Responsible internet use, covering both school and home use, will be included in the PSHE curriculum.

Pupils will be instructed in responsible and safe use before being allowed access to the internet and will be reminded of the rules and risks before any lesson using the internet.

Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

CONSULTING STAFF

It is essential that teachers and learning support staff are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies:

- All staff are governed by the terms of the school's 'Staff Code of Conduct for ICT' and will be provided with a copy of the School Internet Policy and its importance explained.
- All new staff will be given a copy of the policy during their induction.
- Staff development in safe and responsible use of the internet will be provided as required.
- Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential.
- Senior managers will supervise members of staff who operate the monitoring procedures.

MAINTAINING ICT SECURITY

Personal data sent over the network will be encrypted or otherwise secured.

Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to emails.

The ICT Manager will ensure that the system has the capacity to deal with increased traffic caused by internet use.

DEALING WITH COMPLAINTS

Staff, children and young people, parents/carers must know how and where to report incidents. Concerns related to Safeguarding issues must dealt with through the school's Safeguarding Policy and Procedures.

The school's designated person for e-safety will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the headteacher immediately.

Pupils and parents/cares will be informed of the complaints procedure.

Parents/carers and pupils will work in partnership with the school staff to resolve any issues.

As with drugs issues, there may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

Sanctions for misuse may include any or all of the following:

- Interview/counselling by an appropriate member of staff
- Informing parents/carers
- Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system, including examination coursework.
- Referral to the police.

PARENTS/CARERS SUPPORT

Parents/carers will be informed of the school's Internet Policy which may be accessed on the school website and in the school brochure.

Any issues concerning the internet will be handled sensitively to inform parents/cares without undue alarm.

Advice on filtering systems and appropriate educational and leisure activities including responsible use of the internet will be made available to parents/carers.

Interested parents/carers will be referred to organisations such as Child Exploitation and Online Protection (CEOP).

A partnership approach will be encouraged with parents/carers and this may include practical sessions as well as suggestions for safe internet use at home.

COMMUNITY USE

School ICT resources may be increasingly used as part of the extended school agenda.

Adult users will sign the school's acceptable use policy.

Parents/carers of children and young people under 16 years of age will be required to sign the acceptable use policy on behalf of their child.

Arrangements for monitoring and evaluation

The Governing Body *(or Pupil Discipline Committee)* will evaluate the impact of this Policy by receiving data from the headteacher regarding the effectiveness of the procedures outlined above.

Prior to any review of the policy, feedback will be sought from the designated governor, school council, staff and parents on the effectiveness of the policy.

Signed: _____

Date: _____

Last updated:

Review date:

Appendix 1

e-Safety Policy: self-audit

We are grateful to Kent County Council e-safety team for allowing us to use this audit.

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Staff who could contribute to the audit include: Designated Child Protection Coordinator, SENCO, E-safety Coordinator, Network Manager and Headteacher.

Has the school an e-Safety Policy that complies with CST guidance?	Y
Date of latest update: new Policy	
Date of future review: January 2017	
The school e-Safety Policy was agreed by governors on:	
The Policy is available for staff to access at: Staff/Policies 2016	
The Policy is available for parents/carers to access at: School Website	
The responsible member of the Senior Leadership Team is: Mr Mottram	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is: Mr Mottram	
The e-Safety Coordinator is: Mr Mottram	

Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the school's e-Safety Policy?	N
Has up-to-date e-Safety training been provided for all members of staff (not just teaching staff)?	Y
Do all members of staff sign an Acceptable Use Policy on appointment?	Y
Are all staff made aware of the school's expectation around safe and professional online behaviour?	Y
Is there a clear procedure for staff, pupils and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	Y
Have e-Safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	Y
Is e-Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y
Are e-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y
Do parents/carers or pupils sign an Acceptable Use Policy?	TBC
Are staff, pupils, parents/carers and visitors aware that network and internet use is closely monitored and individual usage can be traced?	Y
Has an ICT security audit been initiated by the SLT?	Y
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y

Is internet access provided by an approved educational internet service provider which complies with DfE requirements (e.g. KPSN)?	Y
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	Y
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of the SLT?	Y
Does the school log and record all e-Safety incidents, including any action taken?	Y
Are the Governing Body and SLT monitoring and evaluating the school e-Safety Policy and ethos on a regular basis?	y

Schools e-Safety Audit

Taken from Kent Trust Web website:

http://www.kenttrustweb.org.uk//Children/safeguards_esafety.cfm