POLICY DOCUMENT No W04

DEBENHAM HIGH SCHOOL

A Church of England High Performing Specialist Academy

e-SAFETY POLICY

This policy is reviewed annually

History of Document

Issue No	Author/Owner	Date Written	Approved by Governors on	Comments
Issue 1	S Martin	Nov 2012	4 Dec 2012	First draft
Issue 2	S Martin	Jun 2013	20 Jun 2013	Inclusion of elements of Acceptable Use policy and subsequent removal of that policy
Issue 3	S Martin	July 2015	7 July 2015	Amendments and Simplification
Issue 4	S Martin	July 2016	4 October 2016	Minor amendments
Issue 5	S Martin	June 2017	4 July 2017	Minor amendment
Issue 6	S Martin	July 2018	3 July 2018	Minor amendment

CONTENTS

1. Introduction

As part of the agenda set out by the government, the Education Act 2002 and the Children's Act 2004, it is the duty of all educational establishments to ensure that children and young people are protected from potential harm both within and beyond the school setting. School Policy P18 Safeguarding Children sets out the school's general approach to this duty. However the risks associated with the continuing development of electronic technologies make it necessary that the school should have a separate policy to address the challenge of e-Safety.

2. Aims

The involvement of parents/carers and students is vital to the successful use of online technologies. This policy explains how they can be a part of e-Safety safeguarding procedures and how students are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'e-Safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from known and potential risks. The policy's aims are:

2.1.1. To emphasise the need to educate staff and students about the benefits and hazards of using new technologies both in and out of school.
2.1.2. To provide safeguards and agreement by all users, whether staff or student, on acceptable use of the Internet (see the school's Acceptable Use policy).
2.1.3. To ensure all users are clear about procedures for dealing with misuse of any technologies both in and out of school.
2.1.4. To develop links with parents/carers and the wider community so that they have continued awareness of the benefits and potential problems of information technologies and have the opportunity to contribute to school policies and procedures.

3. Roles and Responsibilities

It is the overall responsibility of the Headteacher with the Governors to ensure that e-Safety is part of the wider remit of safeguarding and that safety practices are embedded throughout teaching, learning and working in the school.

3.1. Governors

The Governing Body is responsible for adopting relevant policies and for ensuring that its employees act in a lawful manner, making appropriate use of school technologies for approved purposes only.

Governors nominate an e-Safety Governor (R. Barker) to challenge the school about having an Acceptable Use Policy (AUP) which defines roles and responsibilities for the safe management and implementation of ICT, including:

3.1.1. Firewalls;
3.1.2. Anti-virus and anti-spyware software;
3.1.3. Filters;
3.1.4. Using an accredited ISP (internet Service Provider);
3.1.5. Awareness of wireless technology issues;
3.1.6. Using personal devices.

3.2. The Headteacher

3.2.1. The Headteacher is responsible for promoting e-Safety across the curriculum and ensuring that it is included in the School Development Plan.

3.2.2. The Headteacher is responsible for ensuring that staff are aware of and understand the e-Safety and related policies.

3.2.3. The Headteacher should designate an e-Safety Co-ordinator to implement agreed policies, procedures, staff training and curriculum requirements and to take responsibility for establishing a safe ICT learning environment. Staff and students are made aware of this role.

3.2.4. The Headteacher or e-Safety Coordinator ensures that Governors are informed about the progress of the e-Safety curriculum (as delivered via PSHE or ICT) and how it relates to safeguarding.

3.2.5. Time and resources are provided for the e-Safety Coordinator and staff training

3.2.6. The Headteacher is responsible for ensuring that any incident or misuse, either by staff or students, is dealt with according to school policy and procedures and that appropriate action is taken.

3.3. e-Safety Coordinator

This position is held by S.Martin (Deputy Head)
It is the role of the designated e-Safety Coordinator to:

3.3.1. Appreciate the importance of e-Safety and to recognise that all educational establishments have a general duty of care to ensure the safety of their students and staff.

3.3.2. Establish and maintain a safe ICT learning environment within the school.

3.3.3. Ensure that the Acceptable Use Policy is reviewed periodically with up-to-date information.

3.3.4. Ensure that training is available for all staff to teach e-Safety.

3.3.5. Ensure that parents/carers feel informed and know where to go for advice (see section 6 below).

3.3.6. Ensure that filtering is set to the correct level for staff and students in the initial set up of a network, stand-alone PC, staff/student laptops and the school's Learning Platform.

3.3.7. Ensure that all adults are aware of the filtering levels and why they are there to protect students.

3.3.8. Report issues and update the Headteacher on a regular basis. Review any issues relating to e-Safety and make reports at termly intervals to the e-Safety Governor who reports termly to full Governing Body meetings. This is a regular agenda item.

3.3.9. Liaise with staff responsible for PSHE, safeguarding and ICT so that policies and procedures are up to date to take account of any emerging issues and technologies.

3.3.10. Update staff training (all staff) according to new and emerging technologies so that the correct e-Safety information can be taught and adhered to.

3.3.11. Work alongside the Network Manager to ensure transparent monitoring of the Internet and online technologies by means of programmes such as Impero (to monitor student use in lessons) and filters for Internet traffic.

3.3.12. Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified. Refer to the school's Safeguarding Policy to ensure the correct procedures are used in incidents of misuse.

3.3.13. Work alongside the Network Manager to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-alone PCs and teacher/student laptops and that this is reviewed and updated on a regular basis.

3.3.14. Ensure that unsolicited emails to members of staff from other sources are minimised. Refer to the school's Safeguarding Policy for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.

3.3.15. E-mails are monitored by an automated systems.

3.4. Staff or Adults

It is the responsibility of all adults within the school to:

3.4.1. Be familiar with the Safeguarding, Positive Behaviour, Anti-bullying, and Acceptable Use Policy and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. If there is any doubt, the matter must be referred to the Senior Designated Person (or Alternate) immediately.

3.4.2. Alert the e-Safety Coordinator of any new or arising issues and risks that may need to be included within policies and procedures.

3.4.3. Ensure that students are protected and supported in their use of electronic technologies so that they know how to use them in a safe and responsible manner. Students should know what to do in the event of an incident.

3.4.4. Be up to date with e-Safety knowledge that is appropriate for the age-group taught and reinforce it throughout the curriculum.

3.4.5. Sign the Acceptable Use Agreement which they receive upon commencement of employment (a copy of which is kept on their personal file) and read and understand the Acceptable Use Policy (Appendix 2).

3.4.6. Use electronic communications in an appropriate way. Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user are logged on.

3.4.7. Report accidental access to inappropriate materials to the e-Safety Coordinator in order that inappropriate sites can be added to the restricted list.

3.4.8. Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the Internet on a regular basis, especially when not connected to the school's network.

3.4.9. Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.

3.4.10. Report incidents of personally directed bullying or other inappropriate behaviour via the Internet or other technologies. Incidents are recorded, investigated and followed up in the same way as for other non-physical assaults.

3.5. Students

Students should:

3.5.1. be responsible for reading and signing the Acceptable Use Agreement when they join the school.

3.5.2. be taught to use the Internet in a safe and responsible manner through the ICT and PSHE curriculum.

3.5.3. be confident about telling an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand.

4. Acceptable and Inappropriate Use

4.1. Staff

Staff members have access to the network so that they can obtain age-appropriate resources for their classes and create folders for saving and managing resources.

All staff have a password to access a filtered Internet service and know that they must not disclose their password to anyone or leave a computer or other device unattended while they are logged on.

The Acceptable Use Agreement is displayed in key positions as a reminder to staff that they need to safeguard themselves against potential allegations.

The Acceptable Use Agreement applies when accessing the Learning Platform from home.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the Internet or Learning Platform in an abusive or illegal manner, a report must be made to the Headteacher or Senior Designated Person immediately. The School Disciplinary procedure will then be followed.

The school has the right to monitor and read emails where it is felt that the user has not adhered to the AUP or there is concern of a nature which could lead the school or teacher into disrepute.

4.2. Students

The Acceptable Use Agreement for students and Student Rules for the use of the Internet and Learning Platform are on display in computer rooms. See Appendix 3. These documents help students to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example:

- understanding what action to take should there be the rare occurrence of sighting unsuitable material
- knowing the consequences of deliberate searching for inappropriate materials
- Knowing that downloading materials, for example, music files and photographs, needs to be appropriate and fit for purpose, based on research for work and copyright free
- Understanding that file-sharing via email, weblogs or any other means online should be appropriate and be copyright free when using the Learning Platform in or out of school.

In the Event of Inappropriate Use

Failure to comply with the Acceptable Use Agreement is likely to result in the following measures (although more serious offences will be treated with appropriate severity):

First Offence:	Letter home and a ban from the Computer Room at lunch times and from Internet use for up to half a term.
Second Offence:	Letter home, ban for half a term and internal isolation.
Third Offence:	Letter home, fixed term exclusion

If a student **accidentally** accesses inappropriate materials he or she should immediately hide the screen or close the window and report this to an adult who can take the appropriate action. Where students feel unable to disclose abuse, sexual requests or other misuses to an adult, they can use the Report Abuse button on the website www.thinkuknow.co.uk to make a report and seek further advice.

There is regular workshop and information provision in small groups to advise students on the safe use of social media.

5. The Curriculum and Tools for Learning

The teaching and learning of e-Safety is embedded within the school curriculum to ensure that the key safety messages about engaging with people are the same whether children and young people are on- or off-line.

5.1. Internet Use

The school undertakes to teach students how to use the Internet safely and responsibly. They are taught in ICT and all other lessons how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies will have been taught by the time they leave Year 11:

- Internet literacy
- Making good judgements about websites and emails received
- Knowledge of risks such as viruses and opening mail from a stranger
- Access to resources that teach how to be safe and responsible when using any online technologies
- Knowledge of copyright and plagiarism issues
- File sharing and downloading illegal content
- Uploading information – knowing what is safe to upload and not uploading personal information (see 5.2 below)
- Where to go for advice and how to report abuse
- Safe use of social media.

These skills and competencies are taught within the curriculum so that students can gain the confidence to explore how online technologies can be used effectively but in a safe and responsible manner. Students learn how to deal with any incidents with confidence and are never blamed for accidentally accessing inappropriate materials.

Students are also taught to understand the use of a public domain and the consequences of misuse. Relevant curriculum links are made to highlight the legal implications and the involvement of law

enforcement. Other technologies used with students include Photocopiers, Fax machines and Telephones.

5.2. Personal safety

Students are taught that they must not email or upload to websites any personal information including:

- Full name (first name is acceptable, without a photograph)
- Address
- Telephone number
- Email address
- School
- Clubs attended and where
- Age or DOB
- Names of parents
- Routes to and from school
- Identifying information, e.g. I am number 8 in the school Football Team.

Photographs should only be uploaded with the approval of a member of staff or parent/carer who should monitor their content. Images of children and young people should be stored in accordance with the Data Protection policy.

Staff and parents/carers need to ensure they consider the risks and consequences of anything they or children and young people may post to any web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and can affect future careers. (see Code of Conduct for Teaching and Support Staff)

5.3. Students with Additional Learning Needs

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each student. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-Safety awareness sessions and Internet access.

5.4. Student login

Students must use their login and password to access the Learning Platform and the Internet, so that the level of filtering is appropriate. Staff ensure that students are not bypassing the login to get to the Learning Platform so that they are protected to the best of the school's ability, in line with the school's Acceptable Use policy.

5.5. School Website

The uploading of images to the school website is subject to the same Acceptable Use agreement as uploading to any personal online space. Permission will be sought from parents/carers prior to the uploading of any images. Staff should consider what information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

5.6. External Websites

If members of staff find themselves or another adult as a victim on an external website, such as 'Rate My Teacher' they must report the matter to the Headteacher and to their union.

5.7. Email Use

All students are issued with an individual school email address as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms.

Staff and students must use their school email address for any communication between home and school. A breach of this may be considered a misuse.

Parents/carers are encouraged to be involved with the monitoring of emails sent; the best approach with children and young people is to talk about who they may be writing to and to assess risks together.

Individual email accounts can be traced if there is an incident of misuse. Monitoring software is used to flag up inappropriate terms. See section 5.14 Monitoring.

5.8. Mobile Phones and Other Emerging Technologies

5.8.1. Students

School policy is that students may not use mobile phones and any devices with a camera function in school. If a student is seen using such a device at school it will be confiscated. Multiple offences will result in an after-school detention and parents will be asked to come to school to collect the device. These devices can give rise to the following areas of concern:

- *Inappropriate or bullying text messages.*
- *Images or video taken of adults or peers without permission being sought.*
- *'Happy slapping' – the videoing of violent or abusive acts towards a child, young person or adult which is often distributed.*
- *Sexting - the sending of suggestive or sexually explicit personal images via mobile phones.*
- *Wireless Internet access, which can bypass school filtering and allow access to inappropriate or potentially harmful material or communications.*

Students may take mobile phones on school trips for emergency use only.

The school is not responsible for any theft, loss or damage of any personal mobile device.

5.8.2. Staff

Staff may bring in personal mobile phones or devices for their own use in staff-only areas, but **must not use personal numbers to contact children and young people under any circumstances.**

- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras. Staff should not use their own cameras or phones to capture images. If this does happen the memory card should stay on the school premises until the file is deleted.

- The school is not responsible for any theft, loss or damage of any personal mobile device.

School Issued Mobile Devices

In addition to the clauses in 5.8.2 above:

- Where the school has provided a mobile device to a member of staff, such as a laptop, PDA or mobile phone, s/he is responsible for any use of this device and should be aware of any confidential information it holds. *It is advisable that only the member of staff uses this device.*

5.9. Video and Photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

Prior to uploading any image staff should check with the e-Safety Coordinator that there is no inappropriate content and that parents/carers' permission has been granted.

The sharing of photographs via weblogs, forums or any other means online should only occur after permission has been given by a parent/carer or member of staff.

Photographs/images used to identify children and young people in a forum or using Instant Messaging within the Learning Platform should represent the child rather than be a true likeness.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website.

Group photographs are preferable to individual students and should not be of any compromising positions or in inappropriate clothing. The school will need to decide how photographs will be used, including where they will be stored (central location which could be viewed by anyone) and when they will be deleted.

It is current practice by external media such as local and national newspapers to include the full name of children and young people in their publications. Photographs of students should only be used after permission has been given by a parent/carer.

5.10. Video-Conferencing and Webcams

The use of webcams to video-conference will be through the school filtering. Publicly accessible webcams are not used in school.

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Permission will be sought from parents and carers if their child is engaged in video conferencing with individuals or groups out of school. This process will always be supervised by a member of staff and a record of dates, times and participants held by the school.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).

5.11. Managing Social Networking and Other Web 2.0 Techdata nologies

Both staff and students are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published.

The following measures are in place:

- Access to social networking sites is controlled through existing filtering systems.
- Students are advised against giving out personal details or information, which could identify them or their location (e.g. mobile phone number, home address, school name, groups or clubs attended, IM and email address or full names of friends).
- Students are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos, which could reveal personal details (e.g. house number, street name, school uniform).
- Students are advised on social networking security and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- Staff are aware that social networking can be a vehicle for cyber-bullying. Students are encouraged to report any incidents of bullying in accordance with the procedures set out in the school Anti-bullying Policy.

5.12. Social Networking Advice for Staff

Social networking outside of work hours, in a non-school setting or other is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with students such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with students outside of Headteacher authorised systems (e.g. school email account for homework purposes).
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invitations from colleagues until they have checked with them in person that the invitation is genuine (avoiding fake profiles set up by students).
- Staff should not use Social Networking to contact present students or past students who are under the age of 18.

5.13. Safeguarding Measures – Filtering

Staff and students are required to use the learning platform and all tools within it, in an acceptable way in accordance with the Acceptable Use Agreements for staff and students (see Appendices 2 and 3).

The school uses the Netsweeper filter system. Regular checks are undertaken of the effectiveness of this filtering system. These are organised by the Network Manager on a termly basis

Regular monitoring (fortnightly) of the log of the internet filtering system is undertaken by the IT department.

The Learning Platform is set within a filtering service which is the same as the internet filtering service, that will provide the same level of protection for all users.

Anti-virus and anti-spyware software is used on all network and stand-alone PCs or laptops and is updated on a regular basis.

A firewall ensures information about students and the school cannot be accessed by unauthorised users.

Links or feeds to e-Safety websites are provided.

The Report Abuse button on the website www.thinkuknow.co.uk is available should there be concern about inappropriate or malicious contact made by someone unknown. This provides a safe place for children and young people to report an incident if they feel they cannot talk to a known adult.

CEOP (Child Exploitation and Online Protection Centre) training for secondary students (and Year 6 Primary children) is annual and part of the PSHE curriculum for raising awareness on staying safe and being responsible. A link to the www.thinkukknow.co.uk website is part of the skin layout for further advice and information on children or young people's personal online spaces. Encryption codes on wireless systems prevent hacking.

Tools for Bypassing Filtering

Students and staff are forbidden to use any technology designed to circumvent, avoid or bypass any school security controls (including internet filters, antivirus solutions or firewalls) as stated in the Acceptable Use Agreements.

Violation of this rule will result in disciplinary or in some circumstances legal action.

It is worth noting however, that block banning of student's ICT or Internet access can be severely disruptive to learning across the curriculum and can also affect lesson planning and should only be applied in the most serious breaches.

5.14. Monitoring

The e-Safety Coordinator is responsible for monitoring the use of online technologies by students and staff. The school uses specialist software with alerts sent in real-time to highlight any potential misuse or risk. The Network Manager reports alerts to the e-Safety Coordinator.
Teachers are responsible for monitoring the use of the Learning Platform and Internet during lessons and also for monitoring the use of emails from school and at home.

6. Parents

Each student will receive a copy of the Acceptable Use Agreement on joining the school. Parents/carers are asked to discuss the Agreement with their child so that it is clearly understood and to return a signed copy, signifying acceptance, to school for their child's file.

Parents/carers are encouraged to support their children in the acceptable use of online technologies at home as well as at school.

6.1. Support

As part of the approach to developing e-Safety awareness with children and young people, the school will offer parent/carers the opportunity to find out more about how they can support the school in keeping their child safe and find out what they can do to continue to keep them safe whilst using online technologies beyond school. The school wants to promote a positive attitude to using the World Wide Web and therefore wants parent/carers to support their child's learning and understanding of how to use online technologies safely and responsibly.

The school will do this by holding an e-Safety Parent/Carer Information Evenings at regular intervals

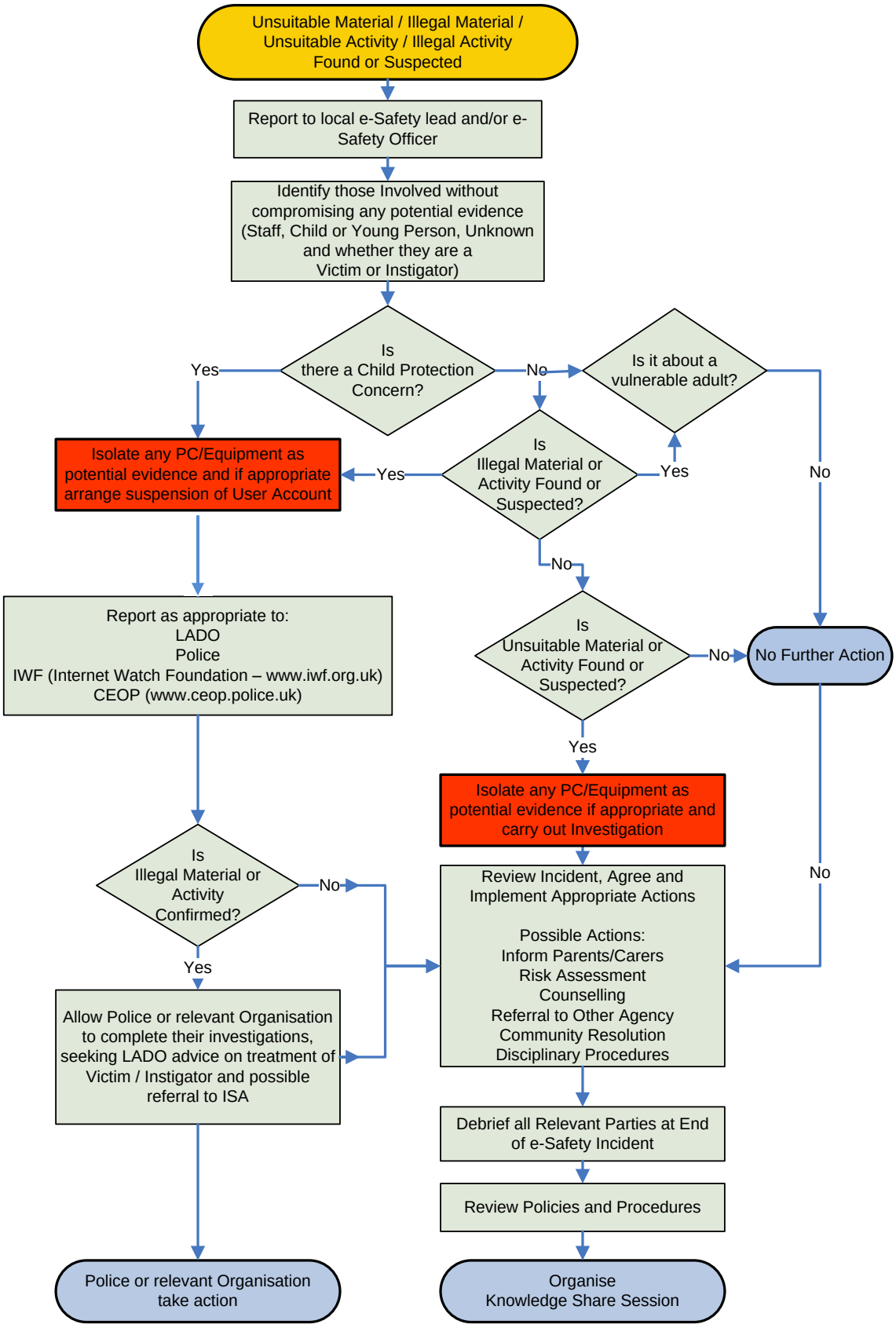
Part of this evening will provide parent/carers with information on how the school protects students whilst using the Learning Platform facilities, such as the Internet and email. It will also be an opportunity to explore how the school is teaching students to be safe and responsible Internet users and how this can be extended to use beyond the school.

7. Managing Allegations against Adults Who Work With Children and Young People

The school's Safeguarding policy is followed in dealing with incidents that occur as a result of using personal mobile or email technologies and allegations of misuse or misconduct made by any child or adult about a member of staff.

.

Appendix 1 e-Safety Flow Chart



Appendix 2 Acceptable Use Agreement for Staff, Governors and Visitors

This agreement applies to all online use and to anything that may be downloaded or printed.

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, email or social networking sites. They are asked to sign this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to students before they can upload images (video or photographs) to the Internet or send them via email.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I am familiar with the Procedures for Incidents of Misuse so that I can deal with any problems that may arise effectively.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the Headteacher, Senior Designated Lead or e-Safety Coordinator in accordance with school procedures listed in the Acceptable Use Policy.
- I know who my Senior Designated Leader is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact students via personal technologies, including my personal email. I know I should use the school email address and phones (if provided) and only use a child's school email. I know that I must not use the school system for personal use unless this has been agreed by the Headteacher and/or e-Safety Coordinator.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the school data protection policy.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Coordinator prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software that has been agreed by the Headteacher and/or e-Safety Coordinator.
- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-Safety issues and procedures that I should follow.

I have read, understood and agree with these statements as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using online technologies.

Signed_____ Name (printed)_____ Date _____

APPENDIX 3 Acceptable Use Rules and Agreement for Students

Dear Parent/Carer

USE OF THE INTERNET / ON-LINE LEARNING PLATFORM

As you may be aware the school network has Internet access and email available for both staff and students. This enables students to explore information and communicate with other Internet users throughout the world.

Before being allowed access to these facilities, however, the school asks for an Acceptable Use Agreement to be returned after being signed by both a parent/carer and the student, indicating that you agree to access for your son/daughter and to him/her complying with the code of conduct stated in this letter. Please read this letter and the Student Rules carefully before you and your child sign the agreement.

Our Internet Service Provider is the county's broadband firewalled community which manages its own filtering. This is more restrictive than the normal Windows security settings. Although students will be supervised whenever accessing the Internet we cannot guarantee that they will not gain access to unsavoury material. If this should happen accidentally, we would ask the student to report the source to staff immediately. We would expect, however, that students do not actively seek such material and doing so would be to contravene this agreement and would therefore hold serious consequences.

The school also provides an online space, called a Learning Platform, for each student, where school tasks will be available for both class work and homework use. These include forums and the ability to message which are within the closed community of the school.

When sending information from or within the school or the Learning Platform, students should take care to maintain the same codes of politeness and respect as with any written communication of a formal nature, and be careful not to offend, especially when communicating with a variety of different cultures and organisations.

During school, teachers will guide students towards appropriate materials and appropriate methods when using the Learning Platform and accessing the Internet. We therefore ask you, as parents, to discuss the contents of this letter and the Students' Rules with your children and to sign that you support the standards of the school in this matter.

Yours sincerely

J Upton
Headteacher

DEBENHAM HIGH SCHOOL

STUDENT RULES FOR USE OF THE INTERNET AND LEARNING PLATFORM

Both the Internet access and the Learning Platform provided by the school are additional learning resources and all use should be of an educational nature.
The computer equipment provided by the school should be treated with respect and not tampered with.
Parent/carer permission is required for in-school Internet use and it is assumed that both parents/carers and students will honour the agreement forms they have signed.
In order to protect themselves and others students should never reveal their complete name, address or other personal information, including photographs, which might identify them on the Internet.
When using email, forums, blogs, messaging facilities and web space provided by the school, students are to communicate with respect for others. They are ambassadors for the school and should observe the standards expected within school. They should avoid including material that may cause offence or nuisance to any person and should immediately report any similar material received by them.
Students cannot assume that information found on the Internet is necessarily correct and should check the validity of the information or the site with a member of staff before using in work.
Students should not actively seek unsavoury material on the Internet or via email, and should report any they find to a member of staff immediately.

Failure to comply with these rules is likely to result in the following measures (although more serious offences will be treated with appropriate severity):

First Offence:	Letter home and a ban from the Computer Room at lunch times and from Internet use for up to half a term.
Second Offence:	Letter home, ban for half a term and internal suspension
Third Offence:	Letter home, fixed term exclusion

Persistent Offenders will be considered for permanent exclusion.

Acceptable Use Agreement for Students

All young people are encouraged to use computers and to enjoy the world of opportunities and knowledge that the Internet provides. However, so that you understand and accept responsibility for keeping yourself and other young people safe when online, it is important that you agree to the following statements.

1. I will not create, browse, copy, download, forward or post any material:
   - which supports or encourages the use of illegal drugs or substances or criminal activity.
   - that may be pornographic, racist or illegal.
   - which might upset people, cause offence or make people feel that they are being bullied.
   - that condones violence or intolerance, which would breach copyright laws or intellectual property laws.
2. I will not publish or distribute personal information about other people such as names, phone numbers, address details or photographs.
3. I will not deliberately damage any hardware, try to bypass the Internet filtering system or install software on the network.
4. I will be responsible for my behaviour when using the Internet, including the resources and websites that I access and the language that I use.
5. If I come across any inappropriate or harmful material online, I will report it immediately to a member of staff.
6. I understand that my computer use is monitored and recorded and that Internet access is filtered.
7. I understand that these conditions are designed to keep me safe, and that if they are not followed appropriate sanctions will be applied and my Internet use withdrawn.

Members of staff are available in school to provide help and advice about how to protect yourself when online. For further information about e-Safety go to the CEOP website for young people: **www.thinkuknow.co.uk**

PARENT/CARER SECTION

I am aware that _____(full name) of Form _____ may be given access to the Internet and I have emphasised to him/her the importance of the contents of the Headteacher's letter and the Student Rules for the use of the Internet and Learning Platform.
I give permission for him/her to use this facility. (If you do not wish to give permission, please contact the school to discuss the matter.)

Signed_____ Name (printed) _____

STUDENT SECTION

As a school user of the Internet I agree to abide by the school's rules.

Signed _____ Date _____