MALVERN
COLLEGE

POLICY ON THE ACCEPTABLE USE OF ICT AND E-SAFETY

1. Scope

1.1. This policy is addressed to all pupils and parents are encouraged to read it with their child. A copy of the policy is available to parents on request and the College actively promotes the participation of parents to help the College safeguard the welfare of our pupils and promote e-safety.

1.2. This policy relates to the use of technology, including:

- the internet
- e-mail
- mobile phones and smartphones
- desk-tops, lap-tops, netbooks, tablets/phablets
- personal music players
- devices with the capability for recording and / or storing still or moving images
- social networking, micro blogging and other interactive web sites
- instant messaging, chat rooms, blogs and message boards
- webcams, video hosting sites (such as YouTube)
- gaming sites
- Virtual Learning Environments
- Interactive Projectors
- other photographic or electronic equipment.

1.3. It applies to the use of any of the above on College premises and also any use, whether on or off College premises, which affects the welfare of other pupils or where the culture or reputation of the College are put at risk. Staff are subject to a separate policy which forms part of their contract of employment.

2. Aims

2.1. The aims of this policy are:

2.1.1. to encourage pupils to make good use of the educational opportunities presented by access to the internet and other electronic communication;

2.1.2. to safeguard and promote the welfare of pupils by preventing cyberbullying and other forms of abuse;

2.1.3. to minimise the risk of harm to the assets and reputation of the College;

2.1.4. to help pupils take responsibility for their own e-safety (i.e. limiting the risks that children and young people are exposed to when using technology);

2.1.5. to ensure that pupils use technology safely and securely.

3. Internet and e-mail

3.1. The College provides internet access and an e-mail system to pupils to support its academic activities and to maximise the educational opportunities presented by such access.

3.2. Pupils may only access the College's network when given specific permission to do so. All pupils will receive guidance on the use of the College's internet and e-mail systems and the College's curriculum includes information about online safety to build resilience in pupils to protect themselves and their peers. If a pupil is unsure about whether he / she is doing the right thing, he / she must seek assistance from a member of staff.

3.3. For the protection of all pupils, their use of e-mail and of the internet will be monitored by the College. Pupils should remember that even when an e-mail or something that has been downloaded is deleted, it can still be traced on the system. Pupils should not assume that files stored on servers or storage media are always private. Users are reminded that Internet activity may be monitored.

4. Rules and protocols

4.1. Pupils must comply with the rules set out in this policy. This policy contains the following rules and guidance:

4.1.1. Internet and e-mail protocol (Appendix 1);

4.1.2. Mobile electronic device protocol (Appendix 2);

4.1.3. E-safety Protocol (Appendix 3)

4.1.4. Sexting (Appendix 4)

4.1.5 Protocol for communication between staff and pupils (Appendix 5)

4.2. When using the College's ICT services, pupils must follow these general rules:

4.2.1. act responsibly around College computers at all times;

4.2.2. report any damage to the College computers or other hardware immediately;

4.2.3. treat staff in the ICT office with courtesy and respect;

4.2.4. be considerate of others using College computers - these are primarily for study and should be treated as such.

5. Procedures

5.1. Pupils are responsible for their actions, conduct and behaviour on the internet in the same way that they are responsible during classes or at break time. Use of technology should be safe, responsible and legal. If a pupil is aware of misuse by other pupils he / she should talk to a teacher about it as soon as possible.

5.2. Any misuse of the internet will be dealt with under the College's Behaviour and Discipline Policy.

5.3. Pupils must not use their own or the College's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the College's Anti-bullying Policy. If a pupil thinks that he /she might have been bullied or that another person is being bullied, talk to a teacher about it as soon as possible. See also Appendix 3 of this policy for further information about cyberbullying and e-safety, including useful resources.

5.4. If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the College's child protection procedures (see the College's Safeguarding Policy). If a pupil is worried about something that he / she has seen on the internet, he / she should talk to a teacher about it as soon as possible.

6. Sanctions

6.1. Where a pupil breaches this policy, the Headmaster is authorised by the College Council to apply any sanction which is appropriate and proportionate to the breach in accordance with the College's Behaviour and Discipline Policy including, in the most serious cases, permanent exclusion. Other sanctions might include increased monitoring procedures and withdrawal of the right to access the College's internet and e-mail facilities. Any action taken will depend on the seriousness of the offence.

6.2. Unacceptable use of electronic equipment could lead to confiscation in accordance with the protocols attached to this policy and the College's Behaviour and Discipline Policy (see Appendix 4 of the Behaviour and Discipline Policy for the College's policy on the searching and confiscation of electronic devices).

6.3. The College reserves the right to charge a pupil or his / her parents for any costs incurred to the College, or to indemnify any significant liability incurred by the College, as a result of a breach of this policy.

7. The liability of the College

7.1. Unless negligent under the terms of this policy, the College accepts no responsibility to the pupil or parents caused by or arising out of a pupil's use of the internet, e-mail or any electronic device whilst at College.

7.2. The College does not undertake to provide continuous internet access. E-mail and website addresses at the College may change from time to time.

8. Monitoring and review

8.1. All serious e-safety incidents will be recorded in the E-Safety log.

8.2. The Senior Deputy Head has ultimate responsibility for the implementation and annual review of this policy and will consider the record of e-safety incidents and new technologies with the Deputy Head Pastoral, E-Safety Coordinator and the Designated Safeguarding Lead, to consider whether the existing security and e-safety practices and procedures are adequate.

APPENDIX 1 – INTERNET AND E-MAIL PROTOCOL

Introduction

1. We want each pupil to enjoy using the internet, and to become proficient in drawing upon it both during their time at the College, and as a foundation for their future education. However, there are some potential drawbacks with e-mail and the internet, both for pupils and for the College.

2. The purpose of this protocol is to set out the principles which pupils must bear in mind at all times and also the rules to be followed in order for all pupils to use the internet safely and securely.

3. The principles and rules set out below apply to all use of the internet, including social media, and to the use of e-mail in as much as they are relevant. Failure to follow this protocol will constitute a breach of discipline and will be dealt with in accordance with the College's Promoting Good Behaviour and Discipline Policy.

4. Pupils should note that they will be considered to be personally responsible for material placed or appearing on a website of which they are the account holder.

Access and security

5. Access to the internet from the College's computers and network must be primarily for educational purposes. Pupils must not use the College's facilities or network for personal, social or non-educational use outside the permitted times specified by the College.

6. Pupils must not knowingly obtain (or attempt to obtain) unauthorised access to any part of the College's or any other computer system, or any information contained on such a system.

7. No laptop or other mobile electronic device may be connected to the College network without authorisation from the College. All personal devices connected to the College network must have an English language-based operating system; it is not enough to simply change the input language. It is recommended that personal devices have an up-to-date and self-updating anti-virus package installed and the College may insist on this before granting permission to access the College's network.

8. Passwords protect the College's network and computer system. Pupils should not let anyone else know their password and should treat it like a toothbrush - don't let anyone else use it and change it, where possible, regularly. If a pupils believes that someone knows his / her password she / he must change it immediately. Pupils should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which he / she is not authorised to access. If there is a problem with your passwords, pupils should please speak to ICT Services.

9. The College has a firewall in place to ensure the safety and security of the College's networks. Pupils must not attempt to disable, defeat or circumvent any of the College's security facilities, including the use of a mobile broadband network to bypass the firewall. Any problems with the firewall must be reported to ICT Services.

10. The College has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of pupils, whilst ensuring that "over blocking" does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding. The filtering is in part informed by the risk assessment required by the prevent duty to protect pupils from radicalization. Any attempt to get round the College filtering systems by way of VPNs or proxy servers will be treated as a very serious breach of the College rules.

11. Viruses can cause serious harm to the security of the College's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to e-mails. If a pupils thinks or suspects that an attachment, or other material to download, might contain a virus, he / she must speak to his / her teacher before opening the attachment or downloading the material. Pupils must not disable or uninstall any anti-virus software on the College's computers.

12. If a pupil suspects that a computer or system has been damaged or affected by a virus or other malware or if a College-related document or file is lost, he / she must report this to ICT Services as soon as possible.

Use of the internet

13. Pupils must not use the internet to access, obtain or distribute inappropriate or illegal material. This includes, but is not restricted to, pornography; videos and computer games with a certificate rating older than the person possessing them; and pirated software, music and films.

14. Pupils must use the College's computer system for educational purposes only and are not permitted to access non-educational or non-College approved websites when using College computers or, if using personal laptops or other devices, on College premises outside the permitted times specified by the College.

15. Pupils must take care to protect personal and confidential information about themselves and others when using the internet, even if information is obtained inadvertently. Pupils should not put information such as their full name, birthday, address, mobile number etc online. Receiving or using this kind of information may be unlawful under data protection legislation and laws relating to confidentiality.

16. Pupils must not attempt to install on College computers any purchased or downloaded software, including browser toolbars. Pupils must not load material from any external storage device brought in from outside the College onto the College's systems, unless this has been authorised by a member of staff.

17. Pupils should assume that all material on the internet is protected by copyright and such material must be treated appropriately and in accordance with the owner's rights - pupils must not copy (plagiarise) another's work.

18. Viewing, retrieving, downloading or sharing any material which in the reasonable opinion of the Headmaster is unsuitable, at any time, is strictly prohibited. Pupils must report to the Head of ICT Services immediately if they have accidentally read, downloaded or have been sent inappropriate material, including personal information about someone else.

19. Pupils must not enter into any contractual commitment beyond their age limit using the internet when in the care of the College, or otherwise associated with the College, whether for themselves or on behalf of another.

20. Pupils must not bring the College into disrepute through their use of the internet.

Use of e-mail

21. Pupils must not use any personal web based e-mail accounts such as Yahoo or Hotmail outside the permitted times specified by the College.

22. E-mail should be treated in the same way as any other form of written communication. Pupils should not include or ask to receive anything in an e-mail which is not appropriate to be published generally or which the pupil believes the Headmaster and / or his / her parents would consider to be inappropriate.

23. Pupils must not send, search for or (as far as pupils are able) receive any e-mail message which contains offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. If pupils are unsure about the content of a message, they must speak to a member of staff. If a pupil comes across such material he / she must inform a member of staff as soon as possible. Use of the e-mail system in this way is a serious breach of discipline. The College will take no responsibility for any offence caused by a pupil as a result of downloading, viewing or forwarding inappropriate e-mails.

24. Trivial messages and jokes should not be sent or forwarded through the College's e-mail system. Not only could these cause distress to recipients (if inappropriate) but could also cause the College's ICT system to suffer delays and / or damage.

25. Pupils must not read anyone else's e-mails without their consent.

APPENDIX 2 – MOBILE ELECTRONIC DEVICES PROTOCOL

Use of mobile electronic devices

1. "Mobile electronic device" includes without limitation mobile phones, smartphones, tablets, laptops, MP3 players.

2. All mobile devices brought onto College premises must be registered on the appropriate form with the Housem.

3. Lower School pupils must hand their mobile phones into the House staff before lessons begin. They may have them back after lessons have finished, unless for exceptional reasons determined by the House staff. Lower School pupils may not use mobiles during Hall, unless for academic purposes with the House staff permission.

4. Lower School boarders must hand in their laptops, tablets and mobile phones to the House staff before bedtime.

5. Mobile electronic devices may not be used by Sixth Formers:

   5.1. in classrooms without the teacher's permission;

   5.2. between lessons unless to check emails and timetables;

   5.3. during Hall or study periods, unless for academic purposes with the teacher's permission

   5.4. at meal times

   5.5. for boarders, after lights out.

   Calls and texting on a mobile phone are not permissible during the school day unless in the House.

6. In emergencies, pupils may request to use a College telephone. Parents wishing to contact their children in an emergency should always telephone the boarding house and a message will be relayed promptly.

7. Pupils may not bring mobile electronic devices into examination rooms under any circumstances, except where special arrangements for the use of a tablet or laptop have been agreed with the Head.

8. Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline, whether or not the pupil is in the care of the College at the time of such use. Appropriate disciplinary action will be taken where the College becomes aware of such use (see the College's Anti-bullying Policy and Promoting Good Behaviour and Discipline Policy).

9. The College reserves the right to confiscate a pupil's mobile electronic device for a specified period of time if the pupil is found to be in breach of this protocol. The pupil may also be prevented from bringing a mobile electronic device into the College temporarily or permanently and at the sole discretion of the Head.

10. The College does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto College premises, including devices that have been confiscated or which have been handed in to staff.

11. Photographs and images

    11.1. Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

    11.2. Pupils may only use cameras or any mobile electronic device with the capability for recording and / or storing still or moving images with the express permission of the member of staff in charge and with the permission of those appearing in the image.

    11.3. All pupils must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so.

    11.4. The posting of images which in the reasonable opinion of the Headmaster are considered to be offensive on any form of social media or websites such as Youtube etc is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using College or personal facilities.

12. Mobile electronic devices may be confiscated and searched in appropriate circumstances. Please see Appendix 4 of the College's Promoting Good Behaviour and Discipline Policy on the searching of electronic devices. It is expected that all pupils will allow members of the Safeguarding team and/or the E-Safety Co-ordinator access to images stored on mobile electronic devices and must delete images if requested to do so.

APPENDIX 3 – E-SAFETY PROTOCOL

1. The College is committed to safeguarding the welfare of all pupils in all respects to the best of our ability.

2. The College's responsibilities include:

   2.1. providing pupils with the available technological tools for learning within an environment that is as safe as possible

   2.2. ensuring that pupils receive guidance through ICT and Life Skills lessons about internet safety. E-Safety talks are delivered regularly to pupils by staff trained by the Child Exploitation and Online Protection Centre (CEOP);

   2.3. ensuring that all pupils are aware of its policies and rules on the use of email, the internet and other information systems and enforcing these appropriately;

   2.4. filtering unsuitable material through systems in place and to block access to certain sites, wherever possible;

   2.5 informing all staff, pupils and parents that internet activity may be monitored in order to ensure as much as possible that users are not exposed to illegal or inapprorate websites, and to ensure as much as possible that users do not actively seek access to illegal or inappropate websites.

   2.6. monitoring pupil use, including the amount of time spent on computers;

   2.7. testing the system occasionally from a pupil's point of view;

   2.8. monitoring the pupils' use of any networked device, be that a laptop, College computer or any mobile electronic device that connects to the internal College network or the internet;

   2.9. to deal with individual cases sensitively and appropriately.

Cyberbullying

3. Cyberbullying is the use of a mobile electronic device or the internet to harass, threaten, taunt or stalk a victim. A bully can use text messaging, voice, images, video images, instant messenger, social networking sites, video hosting sites, chat rooms, email. There is also another aspect to this sort of bullying – 'bystander bullying': laugh at it and you are part of it. In other words, if you pass on the malicious message or image, you are then also a bully.

4. Any incident of cyberbullying will be dealt with in accordance with the College's Anti-bullying Policy and, where applicable, the Promoting Good Behaviour and Discipline Policy.

5. Pupils are required to follow the rules set out in this policy which are in place to help keep pupils safe online. Key things to remember include:

    5.1. Always respect others - be careful what you do online, what you say and what images you send. What you think is a joke may hurt someone else. Do not forward offensive material.

    5.2. Think before you send. What you send can be made public very quickly and could stay online for years.

    5.3. Treat your password like your toothbrush. Don't let anyone use your passwords and give your mobile number or personal website / email address only to trusted friends.

    5.4. Don't just stand there - if you see cyberbullying going on, support the victim and report the bullying.

6. If you are being cyberbullied:

    6.1. Tell someone. You have the right not to be harassed and bullied online. Tell an adult you trust - your parents, your Housem, your tutor, the e-safety coordinator (Mrs Young 01684 581699), any other member of staff, the College's Independent Listeners (Angela Rafferty 01684 577 478 and Tim Wright 01684 541 102) or a helpline like Childline on 08001111. See the College's Anti-bullying Policy for guidance.

    6.2. Don't retaliate or reply! Replying to bullying messages is just what the bully wants.

6.3. Save the evidence. Learn how to keep records of offending messages, pictures or online conversations - please ask a member of staff if unsure. These will help you to demonstrate to others what is happening, and can be used by the College, Internet provider, mobile phone company or even the police, to investigate the cyberbully.

6.4. Block the bully. Most responsible websites and services allow you to block or report someone who is behaving badly.

6.5. Tell the provider of the service that you have been bullied (e.g. your mobile phone operator or social network provider). Check their websites to see where to report.

Parents

7. The College expects parents to promote e-safety and to:

7.1. support the College in the implementation of this policy and report any concerns in line with the College's policies and procedures; and

7.2. try to know your child's online friends as you know their actual friends.

8. If parents have any concerns or require any information about online safety, they should contact the E-Safety Co-ordinator on vy@malcol.org or 01684 581 862.

8.1 The College will update parents regarding online safety via the College website (http://www.malverncollege.org.uk/Parent-Info) and through the pastoral bulletin which is emailed to all parents. Our digital leaders who are current students will also be making presentations to parents from 2018.

8.2 The College online safety group includes parent, pupil and College Council representation as well as pastoral staff. This meets termly with the aim of improving the online safety of the College Community.

Useful information for pupils and parents

http://www.saferinternet.org.uk

http://vodafonedigitalparenting.co.uk

http://www.kidsmart.org.uk

http://www.safetynetkids.org.uk

http://www.safekids.com

http://www.thinkuknow.co.uk

Published as a link on the College network. All information on this site is generated by the CEOP.

http://www.websafecrackerz.co.uk

DfE's Advice for Parents and Carers on Cyberbullying

Appendix 4 – Sexting

Sexting is the exchange of self-generated sexually explicit images, through mobile picture messages or webcams over the internet.

Sexting is often seen as flirting by children and young people who think that it is part of normal life. Often, incidents of sexting are not clear-cut or isolated; there may be a variety of scenarios. Sexting incidents can be divided into two categories – aggravated and experimental.

Aggravated incidents of sexting involve criminal or abusive elements beyond the creation of an image. These include further elements, adult involvement or criminal or abusive behaviour by minors such as sexual abuse, extortion, threats, malicious conduct arising form personal conflicts, or the creation or sending or showing of images without the knowledge or against the will of a minor.

Experimental incidents of sexting involve youths taking pictures of themselves to share with established boy or girl friends, to create romantic interest in other youth, or for reasons such as attention seeking. There is no criminal element (and certainly no criminal intent) beyond the creation and sending of the images and no apparent malice or lack of willing participation.

The consequences of sexting can be devastating for young people. In extreme cases it can result in suicide or a criminal record, isolation and vulnerability. Young people can end up being cirminalised for sharing an apparently innocently created image which may have, in fact, been created for exploitative reasons.

Due to the prevalence of sexting, young people are not always aware that their actions are illegal. In fact, sexting as a term is not something that is often recognised by young people made more complex by the fact that the cultural norm for adults can often be at variance with a younger generation. Some celebrities have made comments which appear to endorse sexting – 'it's ok as long as you hide your face' – giving the impression that sexting is normal and acceptable. However, in the context of the law it is an illegal activity and young people must be made aware of this.

The Law - Much of the complexity in responding to youth produced sexual imagery is due to its legal status. Making, possessing and distributing any imagery of someone under 18 which is 'indecent' is illegal. This includes imagery of yourself if you are under 18. 'Indecent' is not defined in legislation. For most purposes, if imagery contains a naked young person, a topless girl, and/or displays genitals or sex acts, including masturbation, then it will be considered indecent. Indecent images may also include overtly sexual images of young people in their underwear.

The law criminalising indecent images of children was created long before mass adoption of the internet, mobiles and digital photography. It was also created to protect children and young people from adults seeking to sexually abuse them or

gain pleasure from their sexual abuse. It was not intended to criminalise children. Despite this, young people who share sexual imagery of themselves, or peers, are breaking the law.

The National Police Chiefs Council (NPCC) has made clear that incidents involving youth produced sexual imagery should primarily be treated as safeguarding issues. Schools may respond to incidents without involving the police. Where the police are notified of incidents of youth produced sexual imagery they are obliged, under the Home Office Counting rules and National Crime Recording Standards, to record the incident on their crime systems. The incident will be listed as a 'crime' and the young person involved will be listed as a 'suspect.' This is not the same as having a criminal record.

Every 'crime' recorded on police systems has to be assigned an outcome from a predefined list of outcome codes. As of January 2016 the Home Office launched a new outcome code (outcome 21) to help formalise the discretion available to the police when handling crimes such as youth produced sexual imagery. This means that even though a young person has broken the law and the police could provide evidence that they have done so, the police can record that they chose not to take further action as it was not in the public interest.

Procedures in the case of an incident of sexting

Disclosure by a pupil: Sexting disclosures should follow the normal safeguarding practices and protocols (see the Safeguarding Policy). A pupil is likely to be very distressed especially if the image has been circulated widely and if they don't know who has shared it, seen it or where it has ended up. They will need pastoral support during the disclosure and after the event. They may even need immediate protection or a referral to Social Care. The following questions will help decide upon the best course of action:

- Is the pupil disclosing about themselves receiving an image, sending an image or sharing an image?
- What sort of image is it? Is it potentially illegal or is it inappropriate?
- How widely has the image been shared and is the device in their possession?
- Is it a school device or a personal device?
- Does the pupil need immediate support and/our protection?
- Are there other pupils and/or young people involved?
- Do they know where the image has ended up?

This situation will need to be handled very sensitively. Whatever the nature of the incident, the College's safeguarding policies and practices must be adhered to.

Searching a device: it is highly likely that the image will have been created and potentially shared through mobile devices. The image may not be on one single

device, but maybe on a website or multitude of devices; it may be on either a College-owned or personal device. It is important to establish the location of the image, but it should be borne in mind that the process of searching may be distressing for the young person involved who may require support.

When searching a mobile device the following conditions should apply:

- the action is in accordance with the College Safeguarding Policy
- the search is conducted in line with appendix 4 of the promotion of good behaviour and discipline policy
- a member of the safeguarding team is present
- the search is conducted by a member of the same sex

If any illegal images of a child are found, informing the police should be considered. It will almost always be proportionate to refer any incidents involving "aggravated" sharing of images to the police, whereas purely "experimental" conduct may be proportionately dealt with without such referral, most particularly if it involves the child sharing images of themselves.

Any conduct involving, or possibly involving, knowledge or participation of adults must always be referred to the police.

If an "experimental" incident is not referred to the police the reasons for this should be recorded in writing.

The child must be put first. The device must not be searched if it will cause additional stress to the person whose image has been distributed.

If there is an indecent image of a child on a website or a social networking site in this must be reported to the site hosting it. In the case of a sexting incident involving a child or young person who may be at risk of abuse then this should be reported directly to CEOP www.ceop.police.uk/ceop-report so that law enforcement can make an assessment, expedite the case with the relevant provider and ensure that appropriate action is taken to safeguard the child.

ACTION TO BE TAKEN WITH THE IMAGE:

If the image has been shared across a personal mobile device:

- Confiscate and secure the device
- Complete the Investigation Impact Assessment (see appendix 4a)
- Do not to view the image unless there is a clear reason to do so
- Do not send, share or save the image anywhere
- Do not allow pupils to view images or send, share or save them anywhere

If the image has been shared across the College network, a website or social network:

- Block the network to all users and isolate the image

- Do not send or print the image
- Do not move the material from one place to another
- Do not view the image outside of the protocols of the College Safeguarding Policy and procedures

Who should deal with the incident?

Whoever the initial disclosure is made to act in accordance with the College safeguarding policy, ensuring that the DSL or a senior member of staff is involved in dealing with the incident.

The DSL should always record the incident and senior management should always be informed. There may be instances where the image needs to be viewed and this should be done in accordance with protocols. The best interests of the child should always come first; in light of the fact that interviewing the child is likely to cause additional stress, staff should make a judgement about whether or not it is appropriate to do so.

Deciding on a response

There maybe a multitude of reasons why a pupil has engaged in sexting - it may be a romantic or sexual exploration, or it may be due to coercion. There are occasions when it will not always be appropriate to inform the police; this will depend on the nature of the incident (cf: above). Incidents must be consistently recorded. It may also be necessary to assist the young person in removing the image from website or elsewhere.

If indecent images of a child are found:

- Act in accordance with the safeguarding policy and notify the DSL
- Store the device securely
- Carry out a risk assessment in relation to the young person
- Make a referral if needed
- Contact the police, as appropriate
- Put the necessary safeguards in place for the pupil, eg, counselling support, immediate protection and parents must also be informed.
- Inform parents and/or carers about the incident and how it is being managed.

Contacting other agencies (making a referral)

If the nature of the incident Is high-risk, consideration will be given to contacting Children's Social Care. Depending on the nature of the incident and the response it may be appropriate to contact local police or refer to CEOP.

Containing the incident and managing pupil reaction

- The pupil will be anxious about who has seen the image and where it has ended up.
- Occasionally, the fallout from such incidents can result in pupils having to leave their school.
- Reassurance will have to be given regarding the removal from the platform on which the image(s) were shared.
- The young person is likely to need support from the College (Housem, tutor, DSL), their parents and their friends.
- Education programmes can reinforce to all pupils the impact and severe consequences that this behaviour can have.
- Other staff not involved in the incident may need to be informed and should be prepared to act if the issue is continued or referred to by other pupils.
- The College, its pupils and parents should be on high alert, challenging behaviour and ensuring that the victim is well cared for and protected.
- The young person's parents should usually be told what has happened so that they can keep a watchful eye over their child, especially when they are online at home.

Reviewing Outcomes and Procedures to prevent further incidences

A review process ensures that the matter has been managed effectively and that the College learns and improve its handling procedures.

Further information is available from the NSPCC website

Appendix 5 – Protocol for communication between staff and pupils

PLEASE READ THIS IN CONJUNCTION WITH THE STAFF CODE OF CONDUCT

1. The College is committed to safeguarding and promoting the welfare of children at the College. As part of our safeguarding policy we expect staff and pupils, and where appropriate, parents, to follow this protocol on communication by mobile phone. Throughout this protocol the term mobile phone includes a PDA or other mobile electronic device.

On College premises

2. Staff and pupils should avoid using mobile phones to speak to or send each other messages, unless it is the most appropriate method. Any messages that are sent should be brief, courteous and related to educational purposes.

Emergencies

3. Staff on supervisory duties on campus, on playing fields or in relation to transport may carry and use a mobile phone to seek assistance from colleagues or emergency services.

4. Where a pupil or group of pupils are involved in an emergency situation they may use a mobile phone to seek assistance.

Outside College

5. Again, staff and pupils should avoid using mobile phones to speak to or send each other messages outside College. Any messages that are sent should be brief and courteous.

6. The leader of an educational visit will carry a mobile phone supplied by the College and, as part of the preparations for the visit, will ensure that other adults taking part in the visit are equipped with mobile phones and that relevant numbers are exchanged.

7. Staff and pupils taking part in such visits should avoid using mobile phones to speak or send messages to each other except in emergencies. Any messages that are sent should be brief and courteous.

Inappropriate communications

8. If there are reasonable grounds to believe that inappropriate communications have taken place, the Headmaster will require the relevant mobile phones to be produced for examination. The usual disciplinary procedures will apply. Pupils may expect to have mobile phones confiscated if there has been a breach of this protocol.