LEWESTON
SHERBORNE

# 3.27 ONLINE SAFETY AND CYBER-BULLYING POLICY

This policy is written with due regard to DFE Guidance July 2017 *Preventing and Tackling Bullying*, and Keeping Children Safe in Education, 2016.

## Introduction

Leweston embraces technology and the advances in this area when used to support learning. Whilst the emphasis in education should be on the positive use of the Internet, there is a need to address the dangers and raise awareness of potential abuses of this technology, especially in light of recent high-profile cases in the media, including strong evidence of online strategies being employed to radicalise young people. This policy applies to all members of the School community, and is not limited to the School network; it is designed to cover all aspects of online safety that may impact on the School community, and should be read in conjunction with the School's Safeguarding policy, which is available on the School website.

Due to the rapidly evolving nature of this subject, terminology is likely to change frequently. This policy will be subject to a review, at least yearly, and also in light of any serious online safety incidents, and/or new guidance by government / Local Authority / safeguarding authorities / Police.

## Ethos

- At Leweston we are committed to safeguarding the welfare of all pupils.
- The School is committed to providing a safe, caring and friendly environment for all staff and pupils.
- We wish to involve the appropriate use of the Internet, and we actively invite the participation of parents to help us to do this.
- Bullying of any kind is unacceptable.
- We oppose the viewing of age-inappropriate films and DVDs. Within the Houses the screening of DVDs is vetted by the House staff, whilst subject teachers consult their Head of Department if they wish to use material in teaching which is normally only viewed by older age groups. On these rare occasions, appropriate guidance and contextualisation is given to the students.

## Objectives

- To enable pupils to learn within an environment that is as safe as possible.

- To promote and disseminate the guidelines for the safe and appropriate use of the Internet, email, and the School's other electronic resources.
- To involve pupils in protecting themselves by including safe use of the Internet in academic lessons, tutor periods, the PSHE programme and the ICT syllabus.
- To teach and reinforce the importance of maintaining a positive self-image, and adopting appropriate social skills.
- To ensure that all pupils understand that any form of bullying concerned with use of the internet or mobile phone/device (Cyber-bullying) will be regarded as serious and will be dealt with within the framework of the School's sanctions.

## The School's Responsibilities

The School provides a programme that raises awareness of online safety for pupils, including topics such as advice on grooming and radicalisation, exposure to material that is not appropriate to their age, the sharing of personal information, and their online footprint. The School agrees:

- To ensure all pupils are aware of our policies and rules on the use of email, the Internet and other information systems, including the School's Computer Resource Policy.
- To require pupils to read and sign the Computer Resource Policy on an annual basis.
- To ensure that pupils receive guidance about Internet safety through ICT and PSHE lessons and e-talks.
- To facilitate access to the wireless network and reserve the right to monitor pupil usage of the Internet.
- To block access to inappropriate sites, wherever possible.
- To filter unsuitable material, including extreme or radical content relating to terrorism, through appropriate IT systems wherever possible.
- To test the system occasionally from a pupil's point of view.
- To monitor the pupils' use of any networked device, be that a personal laptop, School computer or any mobile device that connects to the internal Leweston network or the Internet.
- To enforce the School Rules, for example by examining mobile phones where there is reason to suspect misuse or abuse.
- To run an e-safety committee that will meet at least termly to ensure that 'pupil voice' is heard, and young people's perspective is always considered.

As part of mandatory Safeguarding training, and the INSET programme, Staff will receive yearly online safety training, with new staff receiving training as part of their induction. All staff will also agree to the School's

Computer Resource Policy, and abide by the School Code of Conduct (available in the Staff Handbook), which advises on safe practices with technology.

The School's online safety guidance is directly applicable to pupils, and is published as part of this policy, and separately in the Family Handbook. This guidance includes the following:

- Never meet an 'online friend' without checking that parents/Houseparents know and approve. If they approve, such a meeting will be in a public place with a responsible adult present.
- Downloading or accessing pornographic or otherwise inappropriate/offensive/radical material will be treated very seriously.
- Using the Internet or a mobile phone to send or receive material of a pornographic, inappropriate, offensive or radical nature is prohibited and may lead to permanent exclusion, and in certain circumstances is a criminal offence.
- Sending on such material is liable to lead to suspension or permanent exclusion.

## Parental Responsibilities

Leweston will provide parents with information that may help bridge any gaps in technical knowledge between parents and children. This information can take on a variety of forms, but may include newsletters, termly correspondence, seminars and lectures, and recommended reading material. The School website has a dedicated e-safety section which publishes up-to-date and constantly changing reading material provided by The Parent Zone. With this in mind, Leweston asks parents to:

- Support the School in its online safety and Cyber-bullying policy.
- Try to know their child's online friends as they know their actual friends.
- Ensure that computer use at home is not excessive, and is appropriately monitored.

Should parents have any concerns over, or wish to seek guidance on any aspect of online safety, they are encouraged to contact the relevant Form Tutor, Head of Year, or the Deputy Head Pastoral.

Should parents have concerns that a Leweston pupil has been subjected to attempts at sexual grooming, radicalisation, or other inappropriate online contact, they should contact the School immediately. The Deputy Head Pastoral is the Designated Safeguarding Lead and will, where appropriate, liaise with outside agencies, in particular CEOP (Child Exploitation and Online Protection), and SSCT (Safe Schools and Communities Team), as well as Local Safeguarding Children Boards where appropriate.

## School Network, Social Media, and other issues

The School Internet filters are reviewed regularly, but the School cannot guarantee that such material is always inaccessible. Students are given clear advice on how to keep safe online, and what to do should they find inappropriate material.

All network users are provided with a username and password, and will have clearly defined access rights to the School ICT systems. It is a guiding principle of this policy that the safeguarding of all members of the community should be led by awareness of the issues, and a sense of responsibility from the pupils about how to behave in any given situation. Whilst the School has control of its own network, the wide availability of the Internet means that technological restrictions on behaviour can only go so far. The School's focus is very much on creating awareness, education, and a sense of responsibility.

## Cyber-bullying

Cyber-bullying can be defined as the deliberate use of ICT, particularly the Internet, mobile phones and digital devices such as cameras, tablet devices, and smartphones, to upset someone else. It may take the form of abuse of an individual due, for example, to their status, physical qualities, characteristics, race, religion, sexual orientation, class or the activities with which they have been involved.

Bullying by text, e-mail, phone call, or social media often leaves no physical scars, but can be highly intrusive and hurtful. Cyber-bullying, like all bullying, is therefore taken very seriously.

Cyber-bullying involves the use of a mobile device or the Internet to harass, threaten, taunt or ridicule a victim. For example, bully can use text messaging, voice, images, video images, instant messenger, social networking sites, video hosting sites, chat rooms, email, gaming sites. It may involve contacting the victim directly or sending or posting messages or images about the victim without their explicit consent. If a pupil sends unwanted material of an abusive nature to someone else via email, mobile phone or other digital device, this will be regarded as bullying of a serious nature.

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 engaging wilfully in bullying.

The rapid development of, and widespread access to, technology has provided a new medium for 'virtual' bullying, which can occur in or outside school. Cyberbullying is a different form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click. The Education Act 2011 amended the power in the Education Act 1996 to provide that when an electronic device, such as a mobile phone, has been seized by a member of staff who has been formally authorised by the Head, that staff member can examine data or files, and delete these, where there is good reason to do so. This power applies to all schools and there is no need to have parental consent to search through a young person's mobile phone.

If an electronic device that is prohibited by the School rules has been seized and the member of staff has reasonable ground to suspect that it contains evidence in relation to an offence, they must give the device to the police as soon as it is reasonably practicable. Material on the device that is suspected to be evidence relevant to an offence, or that is a pornographic image of a child or an extreme pornographic image, should not be deleted prior to giving the device to the police. If a staff member finds material that they do not suspect contains evidence in relation to an offence, they can decide whether it is appropriate to delete or retain the material as evidence of a breach of school discipline.

All of the following actions are classed as cyber-bullying, and will be dealt with accordingly by the School:

- Sending threatening or abusive messages
- Creating and sharing embarrassing videos
- 'Trolling' – the sending of menacing or upsetting messages on social networks, chat rooms or online games, whether this is from a known or unknown person
- Excluding someone from online games, activities or friendship groups
- Setting up hate sites or groups about a particular person
- Encouraging young people to self-harm
- Voting for or against someone in an abusive poll
- Creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name.

There are particular features of cyber-bullying that differ from other forms of bullying which need to be recognised and taken into account when determining how to respond effectively. The key differences are:

- **Impact** – the scale and scope of cyber-bullying can be greater than other forms of bullying.
- **Targets and perpetrators** – the people involved may have a different profile to traditional profiles.
- **Location** – the 24/7 and any-place nature of cyber-bullying.
- **Anonymity** – the person being bullied will not always know who is attacking them.
- **Motivation** – some pupils may not be aware that what they are doing is bullying.
- **Evidence** – unlike other forms of bullying, the target of the bully will have evidence of its occurrence.

This peer-on-peer abuse will not be tolerated, and never be accepted as "banter" or "part of growing up". Victims of cyberbullying and/or sexting will receive full pastoral support as outlined below; those responsible will be subject to the School's sanctions policy, and liaison with Social Care and/or the Police will be considered.

## Procedures for dealing with suspected cyber-bullying

**Reporting incidents**

- The School will deal with individual cases sensitively and appropriately.
- If a pupil feels they have been a victim of cyber-bullying, the School will always listen and take views seriously. Pupils can talk to any member of staff, including Tutors, Houseparents, the Lay Chaplain and the Deputy Head Pastoral.

- If a pupil has witnessed bullying, it is their duty to report it, as in this way the bullying can usually be stopped. Not reporting it is likely to mean that the bullying will continue.
- If a pupil makes an allegation about cyber-bullying, the member of staff who receives the allegation must take any notes as soon as they can and pass them on to the Head of Year or Deputy Head Pastoral.

## What will happen next?

- Where there is good reason to believe that a pupil has been bullied by another pupil or a member of staff, the matter will be investigated with a view to stopping the bullying quickly.
- The victim will be interviewed by the Head of Year and/or Houseparent and, if appropriate, by the Deputy Head Pastoral. The pupil may like to be accompanied by a friend; it may be appropriate for a parent or guardian to be present.
- The pupil will be asked to present any evidence they have in the form of text messages or images; these will be viewed sensitively and only seen by those who need to know.
- Different courses of action will be discussed. This will normally involve interviewing the alleged bully – who may also like to be accompanied by a friend; it may be appropriate for a parent or guardian to be present.
- An attempt will be made to help the bully/bullies change their behaviour.
- Possible actions include setting up a meeting between the bully and the victim so that the bully can see the damage they have caused and choose to stop acting the way they are; restricting the bully's access to computers and digital devices and to the internet; monitoring closely the bully's use of the internet and other means of sending messages and images; searching the relevant files in the electronic devices of the alleged bully to obtain evidence; confiscation for a time of the device; sanctions.

## Outcomes

- Support will be available for the person being bullied, for example from the Tutor, House staff and other pastoral staff, as appropriate.
- If a serious incident occurs, staff will monitor the situation closely, for example, by regular follow-up meetings with the victim, to ensure the bullying has stopped.
- In conjunction with any appropriate sanctions, support will also be given to the bully in the form of guidance to change their behaviour and monitoring use of the Internet.
- The level of sanction imposed will depend on the gravity of the offence. Any sanctions will be in line with the School's Anti-bullying and Discipline policies. Serious bullying may involve suspension or exclusion.

- Those who pass on messages or images or include themselves in a group which harasses an individual, for example, through online polls, excluding a pupil from a group or other method of humiliation or intimidation, are also involving themselves in bullying by becoming accessories to the bullying and will face the appropriate sanctions. Any participation in bullying will not be tolerated.
- Where serious bullying is deemed to have taken place, this will be logged on the central bullying record, the central discipline record and the file of the perpetrator.
- Where criminal acts are thought to have taken place, these will be reported to the Police.
- Support will be offered to the victim and the bully in line with the policy.

### Searching electronic devices

The School expressly reserves the right to search files on personal electronic devices brought into the School, as advised by the cyberbullying section in the document DFE Guidance 2017 *Preventing and Tackling Bullying*.

- Searches will be undertaken in the following way:

  i. the device will be searched in the presence of the pupil, who can assist in identifying the offensive files, and another member of staff;

  ii. the search will be conducted in a proper manner – where possible avoiding accessing areas which are clearly not relevant to the specific information the School has a legitimate interest in finding, thereby respecting the privacy of the individual as far as possible;

  iii. the parents will be informed that a search of a pupil's device has taken place, but parental consent is not explicitly needed for a search to go ahead;

  iv. a record will be kept of the incident – including the reasons why the search took place and the outcome

### Radicalisation

Radicalisation is the process by which individuals or groups come to adopt extreme views on political, religious, ideological, or social matters, notably with the result of violent extremism. The School has a responsibility to protect children from extremist views, and to equip them with the ability to recognise, question and resist attempts to radicalise. The School therefore monitors its filtering systems for attempts made online by those wishing to radicalise others, using 'key words' identified by the Home Office and our own risk assessment. The School also educates pupils, staff and governors in how to recognise attempts to radicalise others, and those pupils who may be susceptible to radicalisation. The PSHE, ICT curriculums, and the Tutor time programme promotes critical thinking and wider knowledge for all pupils.

### Useful Contact Numbers and Websites

- http://www.dfes.gov.uk/bullying/cyberbullying - Useful websites selected by DFES under the page

- ‘Don’t suffer in silence’.
- http://www.wiseuptothenet.co.uk - Home Office. For a hard copy of the booklet phone 0800 771234
- http://www.parentsonline.gov.uk - gives up to date safety information and the best interactive educational sites
- http://www.kidsmart.org.uk
- http://www.safekids.com/
- http://www.thinkuknow.co.uk
- http://www.websafecrackerz.co.uk

# APPENDIX 1

## Suggested outcomes for specific incidences

To promote positive pupil behaviour there should be a demonstrable correlation between procedures and sanctions for pupils, and procedures and sanctions for staff.

**Illegal activities**

- The Head or the Deputy Head Pastoral will deal with the matter.
- The Police and IWF/CEOP will be contacted.
- The Network Manager will be contacted to obtain further evidence.

**Bypassing the school's filtering system**

- Pupil: the Head of Year or Deputy Head Pastoral will deal with the matter and write up an incident report. Staff: the issue may be raised by SLT to the Head as a disciplinary matter.
- The Network Manager will be contacted to obtain further evidence.
- Parents or guardians of pupils will be informed.
- The person involved will lose access to the network and/or Internet.
- Pupils involved will receive a disciplinary sanction.

**Viewing pornographic material**

- Pupil: A Head of Department or Head of Year or the Deputy Head Pastoral will deal with the matter and write up an incident report. Staff: the issue may be raised by SLT to the Head as a disciplinary matter.
- The Police and IWF will be contacted if indecent material was uploaded or downloaded. CEOP will be contacted if grooming / sexting or unwanted sexual advances were involved.
- The Network Manager will be contacted to obtain further evidence.
- Parents or guardians will be informed if appropriate.
- The person involved will lose access to the network and/or Internet.
- Pupils involved will receive a disciplinary sanction.

**Pupils Using Social Media (Twitter and Facebook) in lesson time**

- The class teacher or Form Tutor will deal with the matter and write up an incident report to submit to the Head of Year.
- The Network Manager may be contacted to obtain further evidence.

- Parents or guardians may be informed.
- The pupil involved will receive a warning or a disciplinary sanction.

**Writing malicious comments about Leweston School, a Leweston pupil, bringing the School name into disrepute, or setting up false accounts/profiles on Social Media**

- Pupil: The Head or Deputy Head Pastoral will deal with the matter. Staff: the issue may be raised by SLT to the Head as a disciplinary matter.
- The Network Manager will be contacted to obtain further evidence.
- Parents or guardians will be informed.
- The person involved will lose access to the network and/or Internet.
- The pupil involved will receive a disciplinary sanction.

**Deleting another pupil's work or unauthorised deletion of School files**

- A Head of Department, Head of Year, or the Deputy Head Pastoral will deal with the matter and write up an incident report.
- The Network Manager will be contacted to obtain further evidence.
- Parents or guardians will be informed.
- The pupil involved will lose access to the network and/or Internet.

**Trying to hack or hacking into another pupil's account, School databases, School website, School emails, or online fraud using the School network**

- The Head or the Deputy Head Pastoral will deal with the matter.
- Depending on the severity of the incidence, the cybercrime unit, www.actionfraud.police.uk/ or local police could be contacted.
- The Network Manager will be contacted to obtain further evidence.
- Parents or guardians will be informed.
- The pupil involved will lose access to the network and/or Internet, and a sanction will be imposed.

**Copyright infringement of text, software or media**

- A Head of Department or Head of Year or the Deputy Head Pastoral will deal with the matter and write up an incident report.
- The Network Manager may be contacted to obtain further evidence.
- The pupil involved will receive a warning or a disciplinary sanction.

# APPENDIX 2

## Computer Resource Policy and Internet Access Agreement

The school has provided computers for use by students, offering access to a vast amount of information for use in studies, acting as an extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all students, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all. You are responsible for good behaviour with the resources and on the Internet just as you are in a classroom or in a school corridor. Remember that access is a privilege, not a right, and inappropriate use will result in that privilege being withdrawn.

The school provides a screening service for Internet use. However no solution can completely guarantee the prevention of students' access to unwanted Internet material. Articles of unacceptable material such as racist, extremist (relating to terrorism), political, homophobic or violent material for example, are not as easy to screen out as pornography; however we work hard to ensure such sites are filtered. Computers will be used to access the Internet only where staff can monitor their use.

## Equipment

- Installing, attempting to install or storing programs of any type on the computers is not allowed. If you need a specific program for your studies you will need to talk to the Network Manager or your teacher.
- Damaging, disabling or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the ICT equipment.
- Only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate.
- Flash Games are not permitted in school, unless authorised by a member of staff supervising the lesson.
- Always check files brought in on removable media (such as CDs, flash drives etc.) with antivirus software and only use them when they are found to be clean of viruses.
- Laptops are not permitted to be connected to the network until an additional agreement has been signed following a meeting with the network manager. A charge for this service is applicable.
- No eating or drinking is allowed in the IT rooms to protect the computers from spillages.
- Do not use the network in any way that would disrupt use of the network by others.
- Unapproved system utilities and executable files will not be allowed in work areas, attached to e-mail or run from an external drive.

## Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name and password.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- Computer storage areas and portable storage will be treated as school books. Staff may review your files and communications at any time to ensure that you are using the system responsibly.
- Do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users' files or folders.

## Internet

- Access to the Internet at school and use of the school network are privileges not rights.
- You should access the Internet only for study or for school authorised/supervised activities.
- Only access suitable material – Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene, homophobic, extreme/radical, discriminatory, or abusive is not permitted. You are responsible for rejecting these links if any appear inadvertently during your research.
- Respect the work and ownership rights of people outside the school, as well as other students and staff. This includes abiding by copyright and intellectual property rights.
- Do not try and bypass the filters which are in place as they are there for your protection.
- If you find unsuitable websites through the school network you should report the web address to the network manager.

## Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive/discriminatory behaviour is as anti-social on the Internet as it is in public. You should remember that you are representatives of the school on a global public system.
- Only open attachments to emails if they come from someone you already know and trust. Attachments contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an e mail containing material of a violent, dangerous, racist, radical, discriminatory, homophobic, or inappropriate content, always report such messages to a member of staff. The school will treat this misuse in line with the school's code of conduct.

- The sending or receiving of an e mail containing content likely to be unsuitable for children or schools is strictly forbidden.
- Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority groups.
- Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities.

If you violate these provisions, access to the Internet will be denied and you will be subject to disciplinary action and/or the Law of the Land. Repeated misuse of the internet could result in removal of all ICT access. Additional action may be taken by the school in line with existing policy regarding school behaviour. Where appropriate, local authorities may be involved or further legal action taken.

LEWESTON
SHERBORNE

# 3.25 CYBER-WORLD SAFETY POLICY FOR PUPILS

## Leweston Guide to Keeping Safe in the Cyber World

Chatting to friends on apps like Facebook, WhatsApp, Skype, Twitter, Instagram, and SnapChat can be useful, fun and a great way of keeping in touch, but how much information does your profile give away about you - are you sure that you are doing all you can to keep safe? Remember - your personal information may be more public than you think. The Internet is a real community of people who are connected by computers, so treat people who you don't know on the Internet as strangers that you might meet in a street.

Read the following guidelines and make sure you use them to keep safe online.

- **Do not give out any personal information** related to your family, friends or yourself like full names, addresses, telephone or mobile numbers or those of your parents. Other information like the name and location of your School or details of School activities can also identify you to others, whether you are in a chat room, message board or newsgroup. Sometimes there are people who watch out for such information, and they can put together a picture of your activities over a period of time that could be several weeks. So be careful with what you say, and never give out your personal details.
- **Be aware when choosing your chat username or email username** not to pick a provocative name as you would be more likely to be sent provocative emails or harassed online. Sites such as Omegle, Periscope, Kik and ChatRoulette do not require a login, and therefore can be used for untoward, inappropriate or even illegal behaviour.
- **Make sure you know everyone on your 'friends' list.** If you haven't met the people face-to-face, they may not be who they pretend to be. Also, instant messaging strangers is an invasion of their privacy.
- **Never agree to meet someone whom you've met through the Internet,** in real life without your parents' permission, and if they agree, never go alone, but go with a trusted adult.
- **Use your common sense.** Someone you are chatting to may not be who they say they are.
- **Do not fill out forms or 'fun' questionnaires online without consulting your parents or teachers.** There are websites which seek personal information and which use this information for marketing or other commercial purposes. Always check a website's privacy statement.
- **Do not open an email or IM from someone you do not know** as you don't know who they are and you might download viruses (which even come from people you do know), or it may have contents that can upset you.

- **There's no such thing as "private" on the Internet.** You may think so, but it's not true. People can find anything they want — and keep what you post to reuse — forever.
- **Many chain emails or emails with virus warnings are hoaxes.** Before you forward virus warnings to your friends and family, check that it is not a hoax.
- **Only upload photos you'd be happy to show your gran, mum or a future employer.** YOU NEVER KNOW WHERE THEY MAY END UP. Using the internet or mobile phone to send provocative or sexual pictures of yourself or friends can get you in serious trouble with the Law; making, possessing, or distributing photographs of young people who appear to be under-18 in a state of undress is ILLEGAL. Be extra vigilant if using websites and apps that offer 'temporary' or anonymous viewing/posting of photographs and material, such as Kik and SnapChat. Sending or sharing pictures/videos over these types of chat apps can still get you in trouble with the Law; additionally, any photographs or messages sent using these apps may disappear for the receiver after a given time, but are still stored on the company's servers. There is no such thing as temporary or anonymous when online!
- **Don't feel pressured into sending photos or videos online.** Nobody should pressure you into sharing or sending pictures that you are not comfortable with. If somebody has asked you to share a provocative picture online or via email, tell your parents or teachers, and save a copy of the message if possible in order to report the situation**.**
- **Don't send pictures of other people unless you have their permission.** Forwarding an embarrassing picture of someone else is a form of bullying. How would you like it if someone did that to you?
- **Always tell your teachers/parents if you come across stuff on the Internet which makes you feel uncomfortable,** or if someone on the Internet harasses you or threatens you.
- **Never respond to provocative, rude, obscene, threatening or blackmailing messages** (whether in chat, newsgroups or message boards) which make you feel uncomfortable. Tell your parents or teachers about such messages and where possible, save a copy of the message so that your parents or teachers can forward it to your Internet Service Provider, or use it to make a police report.
- **Be careful not to express extreme or radical views online.** It is very important that we extend our community of tolerance and acceptance into the online world. Therefore, if you come across extreme views online, particularly relating to radicalisation and/or terrorism, make sure you inform your parents or teachers, saving messages where possible/appropriate.
- **Always assess the information you read on websites.** Because it's on the Internet does not mean that it's always truthful information, especially when it comes to health issues, or when you are doing research for homework.
- **Be responsible and ethical when using the Internet** whether at home, at School or in a public online centre, for example not plagiarising information from the Net, using the computer equipment responsibly, not causing harm to others through your online activities.

- **On Facebook and Instagram, set ALL settings to 'Private', and 'protect' your Tweets** so only people you accept as friends can view your profile.
- **Don't let friends influence** your better judgement when on-line together.
- Add the Facebook 'CLICKCEOP' APP - www.facebook.com/clickceop
- If something is happening online that makes you feel strange or uncomfortable, there are people you can tell that can help.
    - Visit www.thinkuknow.co.uk for lots of information and advice about how to protect yourself and where to go for help with different issues.
    - Check out the ClickCEOP button in places like Microsoft's Internet Explorer 8, Windows live Messenger, Google Chrome and Facebook, or speak to a member of staff.

## How to use Skype safely in the Boarding House

When you make calls on Skype, it's important to keep safety and courtesy in mind. Always keep these safety tips in mind.

- Set your video settings so that you only receive calls from people in your contacts list. Do the same in the calls and IM section
- When adding/accepting a friend request, be certain you know them personally.
- Choose a strong password for your Skype account. Hackers try lists of common passwords and password variations to crack passwords.
- Don't post personal information on your Skype account e.g. email address, birthday, phone numbers, location or full name.
- Know Skype rules on age. By default, Skype restricts the privacy settings of users under 16 years old to ensure maximum protection.
- If someone walks into the room, let them know you're on a call. Otherwise they could say or do something disruptive or inappropriate without even realizing you're using Skype. This is especially important if you're on a video call. Not everyone is comfortable appearing on camera.
- If you're not conversing in a private space, give the caller fair warning too. Otherwise the same risks apply. The person on the other end is just as likely to say or do something in confidence.
- Always hang up when you have finished. It's the only way to prevent the other person from seeing or hearing you later by accident. If you choose to leave the call engaged while you do something else, be especially mindful of your privacy. It's easy to forget the presence of another person when they're not physically in the room.
- Be sensible about when you use Skype and for how long. We totally appreciate the value of Skype for keeping in touch with your friends and family – but it should not impact on your studies or sleep! Please be mindful of this – both for you and your friends.

## Useful websites

http://www.kidsmart.org.uk

http://www.safekids.com/ http://www.thinkuknow.co.uk

http://www.websafecrackerz.co.uk

http://www.skype.com/en/security/

## Mobile Device Guidance:

All pupils using mobile devices at School are reminded of the necessity to use them in a responsible manner. Calls and text messages of an abusive nature are illegal and will be deemed a serious breach of School discipline. No information may be posted online which identifies the School with unacceptable opinions or activities, or which would bring the School into disrepute.

The following guidance must be strictly followed whether using the School network, home network, or 3G/4G:

- Use of devices for storage and/or distribution of offensive (including pornographic) material is forbidden.
- Taking photos, video or audio recordings of fellow members of the School community without permission for a specific purpose will not be tolerated. No device, personal or otherwise, may be used to record, store or transmit any type of image, sound or video from Leweston without teacher permission.
- Use of mobile devices in any way that may cause embarrassment or discomfort to fellow members of the School community is unacceptable.
- All communications sent using the network will befit the image of the School and use appropriate language.
- Users will never seek to harass or abuse students or staff through obscene or offensive language or images, and will report any cases of inappropriate use.

If the School has reasonable suspicion that a student has violated the terms of these guidelines, or other School policy, the student's device may be inspected and/or confiscated. Further misuse may lead to the removal of access to Leweston's IT systems, and referrals to the authorities may be necessary.