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, 2024.

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 Designated Safeguarding Lead 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, bullies 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 child-on-child abuse will not be tolerated, and never be accepted as "banter" or "part of growing up". Victims of cyberbullying and/or sexting (YPSI – Youth Produced Sexual Imagery) 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 Chaplaincy Co-ordinator 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 or 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, Deputy Head or 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, Deputy Head 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 / YPSI 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.