ANTI-BULLYING POLICY:
APPENDIX ON CYBER-BULLYING

School update	
Responsible for review of policy	Deputy Head Pastoral
Last school update	April 2024
Governor Sub-Committee approval	
Sub Committee to review and approve	Pastoral
Review Period	Annual
Last Sub- Committee review date	May 2024
Scheduled review	May 2025
Approved by Sub Committee (Meeting date)	8 May 2024
Next Sub-Committee Review	May 2025
Related policies	Safeguarding, Anti-bullying, Digital Safety Policy Sharing of nudes and semi-nudes

Uploaded to Staff Shared	May 2024
Uploaded to Website	May 2024

1. POLICY STATEMENT

1.1 RMS embraces the advantages of modern technology in terms of the educational benefits it brings, however the School is mindful of the potential for bullying to occur. Cyber-bullying must be understood as a form of bullying in the same way as the more traditionally understood forms.

1.2 Cyberbullying differs from other forms of bullying in several significant ways and can have far greater impact than 'traditional bullying' because of a number of factors including:

- the invasion of personal space and time.
- the anonymity (at least initially) of the bully.
- the ability to broadcast upsetting messages and images rapidly to a potentially huge audience and to continue to do so repeatedly over a long period of time.
- the knowledge that the data is in the global domain, disproportionately amplifying the negative effect on the victim, even though the bully may feel their actual actions had been no worse than conventional forms of bullying
- the fact that cyberbullying can take place between peers and across generations. Teachers can be victims and age is not important.
- the fact that this can take place at any time in or out of school.

1.2.1 Another difference is that other pupils who would not normally take part in bullying behaviour may be drawn in as accessories or bystanders. This can happen, for example, when an image is circulated on a mobile phone by a bully and recipients extend the circulation further by passing it on. By passing on a humiliating picture or message, a bystander becomes an accessory to the bullying.

1.3 The School adopts exactly the same approach to cyber-bullying as to any other form of bullying and will not hesitate to call in external agencies including the police, as appropriate:

1.3.1 The School will support victims and, when necessary, work with the police to detect those involved in criminal acts

1.3.2 The School will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, both in or out of school

1.3.3 The School will use its power of confiscation where necessary to prevent pupils from committing crimes or misusing equipment

1.3.4 All members of the School community are made aware they have a duty to bring to the attention of the School any example of cyber-bullying or harassment that they know about or suspect.

1.3.5 The School has an educative approach for all students who misuse technology

1.4 The School endeavours to block access to inappropriate websites, using firewalls, antivirus protection and filtering systems and up-to-date filtering technology is used to provide a safe platform within the School system. Where appropriate, the Network Manager audits online communications and tracks pupil usage of the School Network.

2. DEFINITION

2.1 DfE guidance offers the following definition of cyber-bullying:

The use of Information & Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else.

2.2 Cyberbullying can take a number of different forms: threats and intimidation, harassment or 'cyberstalking' (e.g. repeatedly sending unwanted texts or instant messages), vilification/defamation, exclusion/peer rejection, impersonation, unauthorised publication of private information/images and 'trolling' (abusing the internet to provoke or offend others online).

It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. It can include sharing of nudes and semi-nudes.

2.3 Examples include:

- Threatening behaviour
- Trolling
- Blackmailing, including revenge porn
- Grooming on-line
- Fake profiles
- Hacking accounts
- Tagging photos with defamatory or negative comments

3. RAISING AWARENESS

3.1 The School educates pupils both in the proper and responsible use of e-communications and about the serious consequences of cyber-bullying and will, through Lifeskills, in computing lessons and assemblies, continue to build resilience in students to protect themselves and their peers online. Parents are educated through Lifeskills evenings and through resources from the Wellbeing Hub.

3.2 The School also recognises that it must 'take note of bullying perpetrated outside School which spills over into the School'. Under powers granted by the EIA 2006, the School is able to respond to cyberbullying carried out by pupils beyond the confines of the School. If staff discover that a child or young person is at risk as a consequence of online activity, this will be dealt with as a child protection issue and a referral may be made to external agencies including the police and Child Exploitation and Online Protection Unit (CEOP).

3.The School provides safeguarding training, of which e-safety is a part, so all staff know how to respond effectively to reports of cyber- bullying or harassment and offers more specialised training for key staff (see school document GUIDANCE FOR STAFF ON RESPONDING TO A SHARING OF NUDES AND SEMI-NUDES images or videos.

3.4 In instances where alleged bullying involves pupils from other schools, clubs or external groups, the School will liaise as necessary with appropriate staff from these organisations.

4. CYBERBULLYING AND THE LAW

4.1 The School fully recognises its duty to protect all of its members and to provide a safe, healthy environment for everyone.

4.2 Pupils are entitled to freedom of expression and respect for their private lives, provided they do not infringe the rights of others. Infringement includes libel and slander (defamation), bullying, harassment and victimisation, inciting hatred on racial, religious or homophobic grounds (hate crimes), breach of confidentiality, breach of copyright or the School's trade mark, child pornography and a wide range of other criminal offences. There are a number of offences (both civil and criminal) that may be committed in the course of cyber-bullying. Some may be covered by more than one piece of legislation:

4.3 The Education and Inspections Act 2006 (EIA 2006) outlines powers which relate more directly to cyberbullying. Headteachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off the school site. The Act also provides a defence in confiscating items such as mobile phones from pupils.

4.4 There is not a specific law which makes cyberbullying illegal but it can be considered a criminal offence under several different acts including Protection from Harassment Act (1997), Malicious

Communications Act (1988), Communications Act (2003) Obscene Publications Act (1959) and Computer Misuse Act (1990). (See Appendix 4)

4.5 The consequences of being prosecuted for such offences may be far-reaching. Convictions for some of these offences may also affect the ability of the offender to enter a career working with children or "vulnerable adults".

4.6 The law of defamation is also relevant. Someone who publishes material which is damaging to the reputation of an individual or a company may be sued for compensation.

4.7 Young people who use their mobile phones or other devices to record physical attacks can be prosecuted as accessories to serious criminal offences.

5. STRATEGIES TO PREVENT CYBER-BULLYING

5.1 The Head of Senior School is always informed of incidents involving cyber-bullying (as any bullying incident) and delegates responsibility for anti-bullying work to the Deputy Head Pastoral (DSL and Heads of Year. The Head of Computing is also the RMS e-safety Coordinator. The Head of Cadogan House deals with incidents of cyber bullying in the Prep Department.

5.2 The Deputy Pastoral Head (DSL) will take overall responsibility for the co-ordination and implementation of cyberbullying prevention and response strategies by ensuring:

- that all incidents of cyberbullying both inside and outside school are dealt with effectively and will be managed and/or escalated in line with the procedures set out in the School's Anti-bullying Policy, Behaviour Policy and Safeguarding Policy.
- that all policies relating to safeguarding, including cyberbullying are reviewed in partnership with the Head of Senior School and updated regularly.
- that all staff know that they need to report any safeguarding issues including cyberbullying to the Designated Safeguarding Lead. Formal safeguarding training occurs each September with regular updates as appropriate. Staff receive weekly safeguarding updates via the NSPCC CASPAR bulletin. Staff are required to undertake differentiated safeguarding courses according to their roles at RMS.
- that training is given (Prevent Duty) so that staff feel confident to identify children at risk of being drawn into terrorism, to challenge extremist ideas and to know how to make a referral when a child is at risk.
- that parents/carers are informed and attention is drawn to the cyberbullying policy so that they are fully aware of the School's responsibility relating to safeguarding pupils and their welfare.
- that all staff are aware of their responsibilities by providing clear guidance for staff on the use of technology within school and beyond.

5.3 The Deputy Head Pastoral will:

- ensure that all pupils are given clear guidance on the safe and positive use of technology, both in school and beyond, including how to manage their personal data and how to report abuse and bullying online.
- Monitor that Heads of Year are following up with daily smoothwall notifications.
- provide annual training, with the Head of Lifeskills, for parents/carers on online safety and the positive use of technology.
- ensure the pupils are aware of and have signed School's Digital user and iPad/laptop home school agreements
- provide additional training for staff and pupils on online safety and the above policies and procedures where required.
- plan and deliver a curriculum on online safety in computing lessons which builds resilience in pupils to protect themselves and others online.

The e-safety coordinator will plan a curriculum and work with the Head of Lifeskills and tutors in delivering a curriculum on online safety which builds resilience in pupils to protect themselves and others online.

5.4 Technical staff play a key role in maintaining a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments. RMS trains its staff to respond effectively to reports of cyber-bullying or harassment and has procedures in place to respond (Appendix 4). IT staff have completed additional online safety courses and all staff undertake additional training as required.

5.5 The Network Manager will:

- ensure adequate safeguards are in place to filter and monitor inappropriate content and alert the Designated Safeguarding Lead to safeguarding issues. The School uses Smoothwall to filter all internet access. Smoothwall records access to prohibited sites which enables the Network Manager to report issues to D S L
- ensure that visitors to the School are given clear guidance on the use of technology in school. Visitors may be given highly restricted guest accounts which will not allow any access to personal data and any misuse of the system will result in access to the system being withdrawn.

5.6.1 The Director of Finance & Operations will:

- ensure the School manages personal data in line with statutory requirements. The School is aware of its duties under the Data Protection Act (1998) and the 2018 General Data Protection Regulations (GDPR) . Careful consideration will be given when processing personal information so that the individual's privacy is respected where it needs protection. Access to the personal information will only be given to those who need it. The principles of the Data Protection Act and GDPR will be applied when processing, collecting, disclosing, retaining or disposing of information relating to a pupil or member of staff.

5.7 The School Governors will:

- appoint a governor in charge of digital safety who will work with the DSL to ensure the policies and practices relating to safeguarding including the prevention of cyberbullying are being implemented effectively. The current governor for digital safety is Ms Sharron Shackell.

6. PREVENTION STRATEGIES FOR PUPILS

6.1 Any pupil who has reason to believe that they or another pupil may be the victim of cyber-bulling should speak to any member of staff without delay. (See Appendix 2)

6.2 In building resilience within its students RMS:

- expects all pupils to adhere to its acceptable use policies for the safe use technologies. Certain sites are blocked by our filtering system and our IT Department monitors pupils' use.
- supports anti-bullying week.
- imposes both disciplinary and restorative sanctions for the misuse, or attempted misuse of the internet which may include specially prepared, mandatory support sessions and pupils are made aware of the serious sanctions at stake.
- issues all pupils with their own personal school email address. [Access to sites such as "hotmail" is not allowed].
- supports the European Commission's Safer Internet Programme and in particular their 'Web We Want' initiative.
- offers guidance on the safe use of social networking sites and cyberbullying in Lifeskills lessons.
- offers guidance on keeping, names, addresses, passwords, mobile phone numbers and other personal details safe.
- does not permit the use of mobile phones by pupils below Sixth Form during the school day by pupils having Yondr pouches.
- Sixth can use their phones in Hind House.

6.3 RMS pupils are taught to protect themselves when using the internet in Computing lessons and as part of their Lifeskills programme. The UKCCIS has produced a digital code as an easy way to remember**: Zip it, Block it, Flag it.**

6.4 Pupils are advised to:

- Zip it: keep your personal stuff private and think about what you say and do online
- Block it: block people who send nasty messages and don't open unknown links and attachments
- Flag it: flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

7. STRATEGIES FOR PARENTS/GUARDIANS

7.1 The School seeks to work closely with parents and carers in promoting a culture of e-safety.

7.2 The School will always contact parents/carers with any worries about a pupil's online behaviour, and parents and carers are encouraged to share any worries about this issue with the School.

7.3 The School recognises that not all parents and guardians may feel equipped to protect their child/ward when they use electronic equipment at home. The School therefore, arranges discussion evenings for parents/guardians when external specialists advise about the potential benefits and hazards of this exploding technology, and the practical steps that parents/guardians can take to minimise the potential dangers to their children/wards. Parents have access to the Wellbeing Hub and there are information links on the Parent Portal. Both of these offer a wealth of information. Parents are also encouraged to use the Vodafone Parent Magazine.

Guidance for all members of RMS

Appendix 1 - GUIDANCE FOR STAFF

If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below.
If the incident is of a sexualised nature, please follow the Nude and Semi-nude Policy and speak to DSL/DDSL as soon as possible; as outlined in that policy staff are not to take a screenshot of any nude or semi-nude of a child, nor should they share it to their iPad or any device.

Mobile Phones/Tablets/Computers

- Ask the pupil to show you the mobile phone/tablet/screen
- Where possible ask the pupil to save the material
- Where possible print off the offending material straight away
- Note clearly everything, on the screen relating to an inappropriate text message or image, to include the date, time and names - You may take a screen shot on an iPad or device (but not if the image is a nude or semi-nude)
- Make a transcript of a spoken message, again record date, times and names
- Tell the pupil to save the message/image
- Follow the protocol of any bullying incident and log the incident on CPOMS.
- Make sure there are no omissions
- Follow the protocol for any bullying incident
- Guidance can be found: NSPCC_online_abuse_and_bullying_prevention_guide_3.pdf (publishing.service.gov.uk)

Appendix 2 - GUIDANCE FOR PUPILS

Key messages

- Your online world will follow you offline. What you say or do online can be seen forever
- How you behave, upload or share may be seen by your Online Abuse and Bullying Prevention Guide 6 parents, friends, teachers, lecturers or future employers and you can lose control of how its shared and by whom very quickly
- Some behaviours are illegal, make sure you know the facts or you could end up breaking the law
- Your behaviour online and your behaviour offline should be the same. Your online behaviour should reflect your offline behaviour – you shouldn't behave differently simply because you're online
- If you are worried about anything you have seen or done online you can speak to ChildLine on 0800 1111 or www. childline.org.uk

If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, your tutor, your housemistress, your Head of Year or the Deputy Head Pastoral but can be any member of staff.

- Do not answer abusive messages but log and report them
- Do not delete anything until it has been shown to your Form Teacher, parents/guardian, Head of Year (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying)
- Do not give out personal details
- Never reply to abusive e-mails or messages
- Never reply to someone you do not know

GUIDANCE FOR PARENTS

It is vital that parents and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying. RMS informs parents of the cyber-bullying policy and the procedures in place to deal with cyber-bullying.

- Parents can help by making sure their child understands the School's policy and, above all, how seriously RMS takes incidents of cyber-bullying
- Parents should also explain to their child legal issues relating to cyber-bullying
- If parents believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything
- Parents should contact the School as soon as possible. If the incident falls in the holidays RMS reserves the right to take action against bullying perpetrated outside the school which spills over into the school and/or including pupils at other schools.

Parents will find any of our Lifeskills parental information evenings beneficial.

ONLINE AT HOME

There is a wealth of information and advice for parents; important and useful information can be found on the following sites:
NSPCC_online_abuse_and_bullying_prevention_guide_3.pdf (publishing.service.gov.uk)

https://www.gov.uk/government/publications/child-safety-online-a-practical-guide-for-parents-and-carers

https://www.vodafone.co.uk/newscentre/app/uploads/2022/01/Digital-Parenting-Magazine-10th-Edition.pdf

Appendix 3 - Relevant Laws

Obscene Publications Act 1959 makes it an offence to "publish" an obscene article (which can include written material, photographs or films). Publishing includes circulating, showing or transmitting the article.

Protection of Children Act 1978 makes it an offence to take an indecent photograph (or film) of a child. A "child" is anyone under 18. The definition of "photograph" includes images on a mobile phone or stored on a computer and also includes "pseudo-photographs" where images have been manipulated. It is also an offence for someone to distribute or show such images or to have them in their possession with the intention of showing them to others.

Public Order Act 1986 makes it an offence to use threatening, abusive or insulting words, behaviour and images with the intention to cause harassment, alarm or distress. This can apply where a mobile phone is used as a camera or video.

Malicious Communications Act 1988 makes it an offence to send an indecent, grossly offensive or threatening letter, electronic communication or other article to another person with the intention that it should cause them distress or anxiety.

Computer Misuse Act 1990 makes hacking into computers an offence.

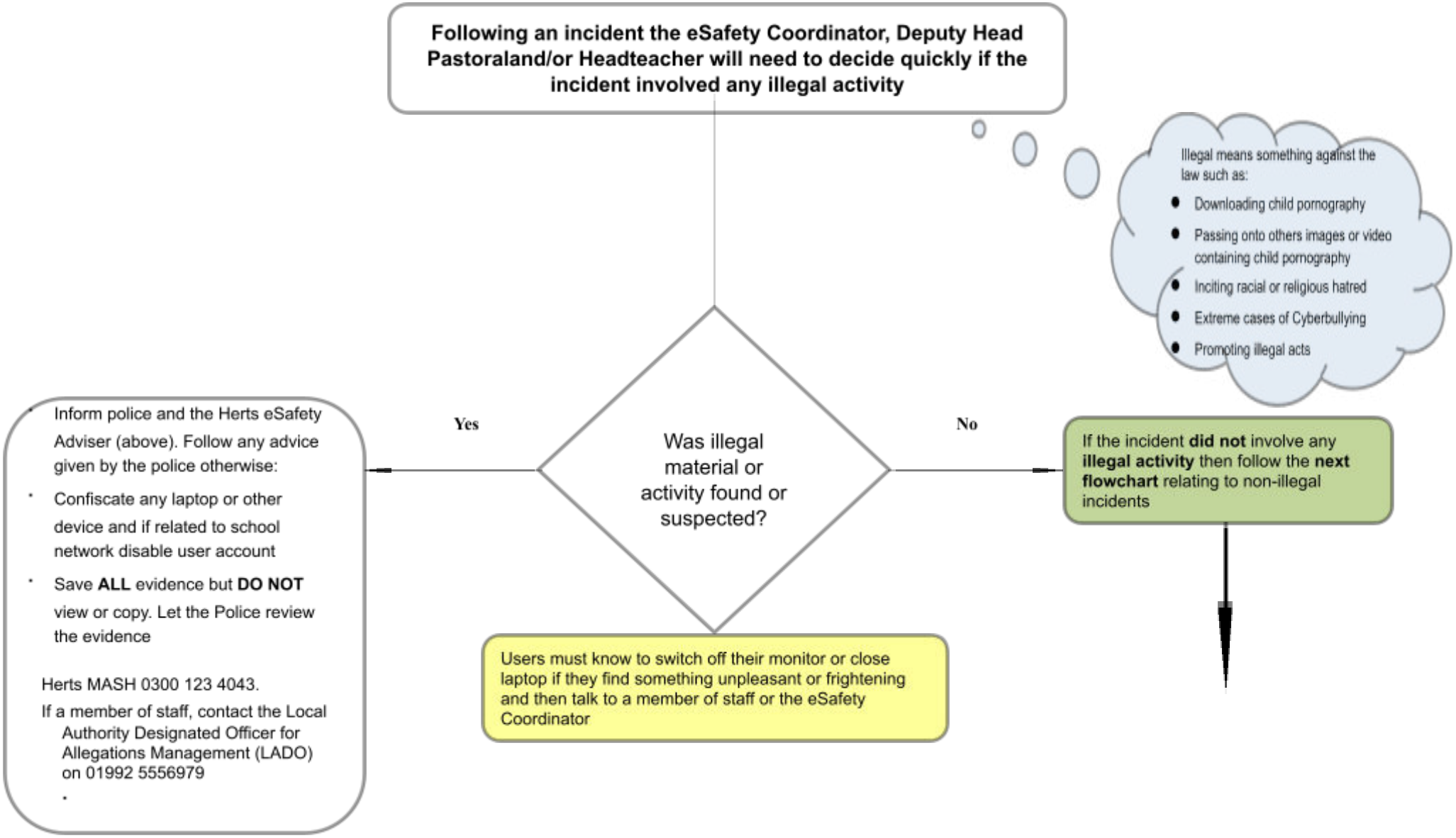
Protection from Harassment Act 1997 creates both civil and criminal offences of harassment. Harassment is defined as a course of conduct which causes alarm or distress on more than one occasion. It is also an offence to cause another person to fear, on at least two occasions, that violence will be used against them.

Communications Act 2003 makes it an offence to send a grossly offensive, obscene, indecent or menacing communication. There is also an offence of sending a message that is known to be false for the purposes of causing annoyance, inconvenience or needless anxiety.

Voyeurism (Offences) Act 2019 makes it an offence to take an image beneath someone’s clothing.

Appendix 4 Online-Safety Incident Flow Charts

Hertfordshire Flowchart to support decisions related to an illegal eSafety Incident
For Headteachers, Senior Leaders and eSafety Coordinators



If the incident **did not** involve and illegal activity then follow this flowchart

The eSafety Coordinator, Deputy Head and/or Headteacher should:

- **Record in the school Bullying Incident Log**
- **Keep any evidence**

Did the incident involve a member of staff?

Yes

If member of staff has:

- Behaved in a way that has harmed a child, or may have harmed a child.
- Possibly committed a criminal offence against or related to a child; or
- Behaved towards a child or children in a way that indicates they would pose a risk of harm if they work regularly or closely with children.

Contact the LADO on: **01992 556979** If the incident **does not** satisfy the criteria in **LSCBP procedures 2007**, then follow the bullet points below:

- Review the evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow the school disciplinary procedures (if deliberate) and contact school HR, Rachel Hurst or Christopher Williams at HfL on 01438 845111

No

Incident could be:

- Using another person's user name and password
- Accessing websites which are against school policy e.g. games, social networks
- Using a mobile phone to take video during a lesson
- Using the technology to upset or bully (in extreme cases could be illegal)

Was the child the victim or the instigator?

Pupil as victim

In – school action to support pupil by one or more of the following:

- Class teacher
- eSafety Coordinator
- Senior Leader or Headteacher
- Designated Safeguarding Lead for Child Protection (DSL)
- School PCSO

Inform parents/ carer as appropriate

If the child is at risk inform the police or Herts MASH immediately

Confiscate the device, if appropriate.

Pupil as instigator

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions and/ or support based on school rules/ guidelines
- Inform parents/ carers if serious or persistent incident
- In serious incidents consider informing Herts MASH as the child instigator could be at risk
- Review school procedures/ policies to develop best practice

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the eSafety Coordinator

Hertfordshire Managing an eSafety Incident Flowchart involving staff as victims