**At Knights Enham Schools we provide…**

Inclusive and ambitious learning experiences where our school community feels safe and motivated to achieve their best.

**'Together We Achieve'**

# E-Safety Policy

**(Based on a model policy from Hampshire County Council)**

**Approved: November 2024**

***Review: November 2025***

## Contents

## 1. Introduction

ICT (or computing) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.
Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Knights Enham Schools, we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile Internet technologies provided by the school (such as laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, and portable media players, etc).

## 2. Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Computing Lead Teacher in our school is **Miss Williams**. All members of the school community have been made aware of who holds this post. It is the role of the Computing Lead to keep abreast of current issues and guidance through organisations such as Hants LA, Becta, CEOP (Child Exploitation and Online Protection) and 'Childnet.'
Senior Management and Governors are updated by the Head/Computing lead and all Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's Acceptable Use Agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home/school agreements, and behaviour/pupil discipline (including the anti-bullying policy and PSHE).

*E-Safety skills development for staff*

- Our staff receive regular information and training on E-Safety issues in the form of updates at staff meetings and correspondence from the Computer Lead.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.)
- All staff are encouraged to incorporate E-Safety activities and awareness into their curriculum areas.

*Managing the school E-Safety messages*

- We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The E-safety policy will be introduced to the pupils at the start of each school year.
- E-safety posters will be prominently displayed in every classroom.

**3. E-Safety in the Curriculum**

Computing and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

- The school has a framework for teaching internet skills in Computing/ PSHE lessons.
- The school provides opportunities within a range of curriculum areas to teach about E-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum.
- Pupils are aware of the relevant legislation when using the Internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as 'Childline'.

**4. Password Security**

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-Safety Policy.
- Users are provided with an individual network, email and Learning Platform log-in username.

- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended.
- Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer).
- In our school, all Computing password policies are the responsibility of the Computing Lead and all staff and pupils are expected to comply with the policies at all times.

**5. Data Security**

The accessing and appropriate use of school data is something that the school takes very seriously.

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the Headteacher.
- Any data taken off the school premises must be carefully stored and used and kept as securely as possible.

**6. Managing the Internet**

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.
All use of the Hampshire schools Internet is filtered and logged by EdComputing, and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school will provide supervised access to Internet resources (where reasonable) through the school's fixed Internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

*Infrastructure*

- School Internet access is controlled through the Hampshire Local Authority's web filtering service.
- Knights Enham Schools is aware of its responsibility when monitoring staff communication under current legislation and takes into account; current GDPR regulations, Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and Internet activity can be monitored and explored further if required.
- The school does not allow pupils access to Internet logs.
- The school uses management control tools for controlling and monitoring workstations via passwords and user permissions.

- If staff or pupils discover an unsuitable site, the screen must be switched off, closed and the incident reported immediately to the Computing Lead (Mrs T Cole).
- It is the responsibility of the school, by delegation to EdICT and the designated school network supervisor, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software & are encrypted. It is not the school's responsibility, nor the Computing Lead's, to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first.
- Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the Headteacher or Computing Lead.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed. The Headteacher will inform the technician for support.

**7. Managing other Web 2 technologies**

Web 2, (where users publish to the web, including social networking sites), if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking sites to pupils within school.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile, home phone numbers, school details, email address, specific hobbies and interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the Hampshire designated Learning Platform approved by the Head Teacher.

## 8. Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as tablets, gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

*Personal Mobile devices (including phones)*

- The school discourages staff to bring in personal mobile phones and devices for their own use. Where mobile phones are brought in, they must remain on silent, stored away out of visible sight and used discretely outside of teaching hours and away from children, unless it is an emergency where this has been agreed by the Headteacher. Under no circumstances does the school allow a member of staff to contact a pupil. The school staff may only contact parents/ carer using their personal device in an emergency, when acting in loco parentis.
- Where an allegation is made against a member of staff concerning the use of mobile phones or cameras, the allegation procedure must be followed in the school safeguarding policy.
- Pupils are not allowed to bring personal mobile devices/phones to school without the permission of the Headteacher.
- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- No mobile device can be connected to the school's wireless network.

*School provided Mobile devices (including phones)*

• The sending of inappropriate text messages between any member of the school community is not allowed.
• Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
• Where the school provides mobile technologies such as phones and laptop for offsite visits and trips; these devices should be used.

## 9. Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private.
Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Head Teacher or line manager where there are any concerns.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.
- Staff must inform (the e-Safety co-ordinator/ line manager) if they receive an offensive e-mail.
- Pupils are introduced to email as part of the Computing Scheme of Work.

## 10. Safe Use of Images Taking of Images and Film

- Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.
- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Head Teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones to record images of the others. Cameras on field trips may be used provided the pupil abides by the AUP on having permission from the subject and the supervising member of staff to take the image.

*Publishing pupil's images and work*

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, e.g. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

*Storage of Images*

- Images/films of children are stored on the school's network
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the permission of the Head Teacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/Learning Platform.
- All staff have the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

**11. Misuse and Infringements**

*Complaints*

Complaints relating to E-Safety should be made to the Computing lead or the Head Teacher. Incidents should be logged and the school flowchart for Managing an E-Safety Incident should be followed (see appendix).

*Inappropriate material*

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Computing lead.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Computing lead, depending on the seriousness of the offence; investigation by the Head Teacher/ Local Authority, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).
- Users are made aware of sanctions relating to misuse or misconduct. All staff have read and signed the AUP and the children have signed an age appropriate version of our AUP.

## 12. Equal Opportunities

*Pupils with additional needs*

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' E-Safety rules.
However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues.
Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children and young people.

## 13. Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting
E-Safety both in and outside of school. We regularly consult and discuss E-Safety with parents/carers and seek to promote a wide understanding of the benefits related to Computing and associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g., on school website).
- The school disseminates information to parents relating to E-Safety where appropriate in the form of;

➢ Information and celebration evenings
➢ Posters
➢ Website/Learning Platform postings
➢ Newsletter items
➢ Learning platform information

## 14. Writing and Reviewing this Policy

This Policy works in conjunction with the Acceptable Use Policy.

*Staff and pupil involvement in policy creation*

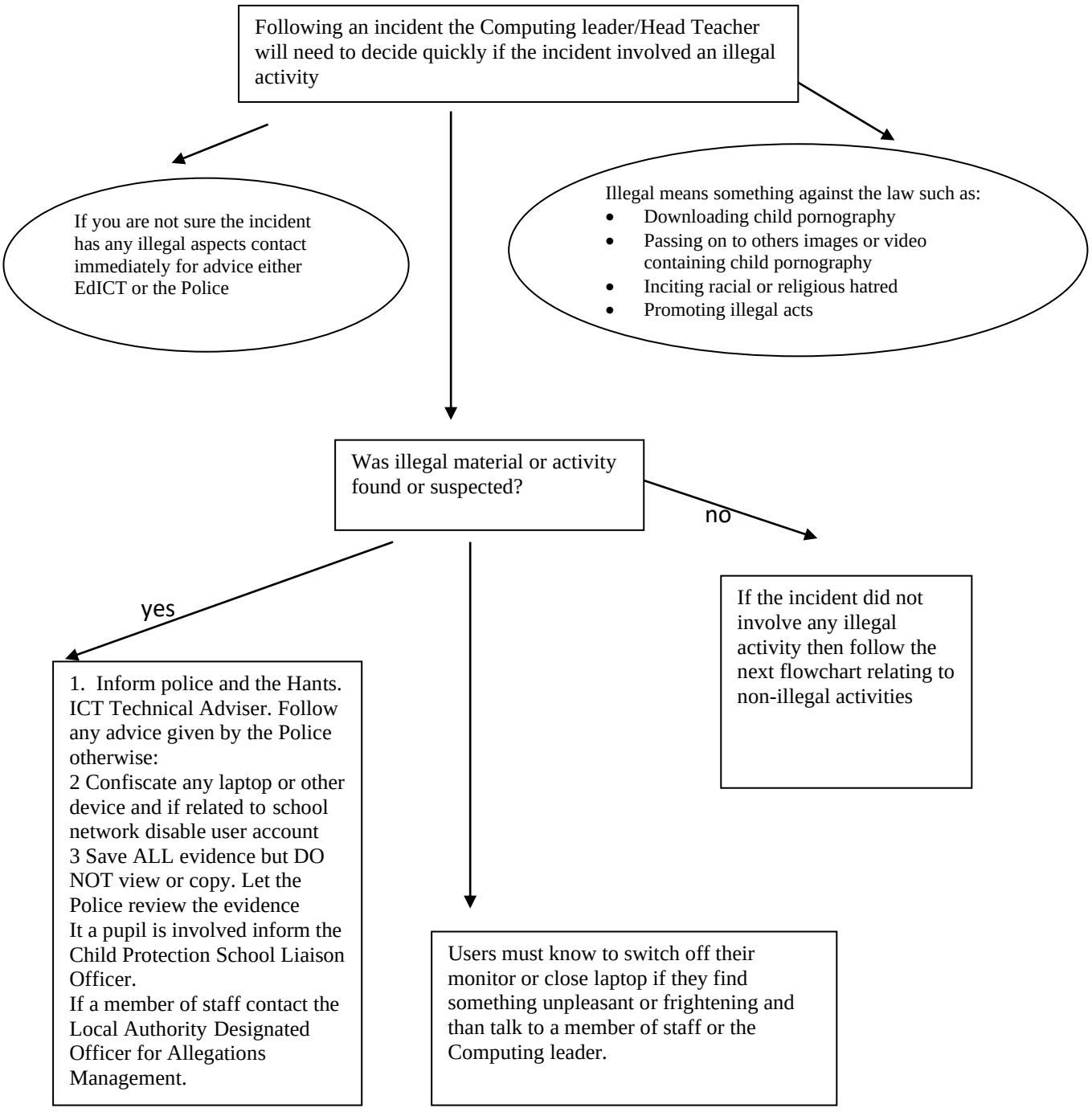
- Staff and pupils are involved in reviewing the E-Safety policy through staff meetings, assemblies individual class work and school council.

*Review Procedure*

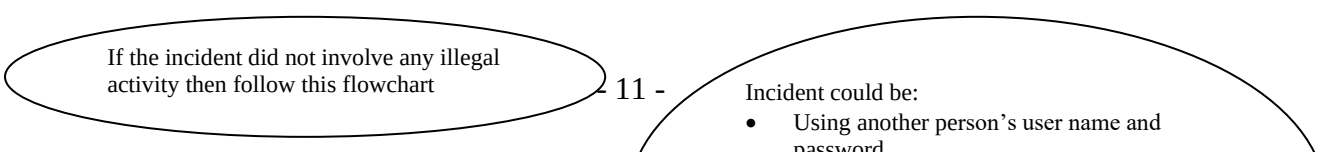
There will be an on-going opportunity for staff to discuss with the Computing lead any issue of E-Safety that concerns them.
This policy will be regularly reviewed and consideration given to the implications for future whole school development planning.
The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

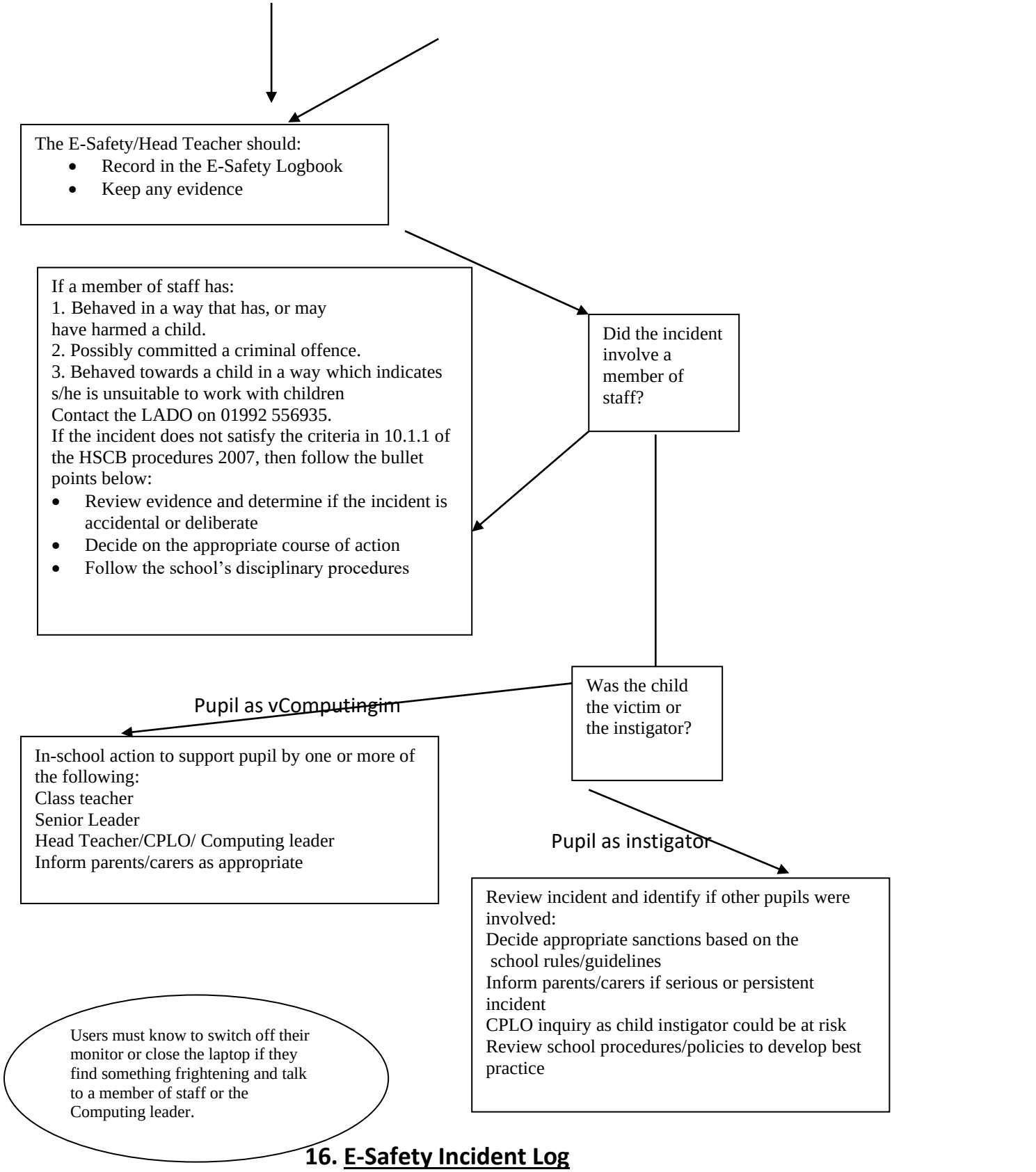
## 15. Flowchart for Managing an e-Safety Incident

## Knights Enham Schools Flowchart to support decisions related to an illegal Incident
For Headteachers, Senior Leaders and Computing Lead




## Managing an e-Safety Flowchart Incident
For Headteachers, Senior Leaders and Computing Lead






## 16. E-Safety Incident Log

Incidents of all e safety incidents to be recorded by the Computing Lead (Mrs Coles) and Headteacher (Mr Whitehouse). The incident log will be monitored by the Headteacher and discussed with the Computing

Lead, Senior Leaders and the Chair of Governors. This can also be recorded on Cpoms and means to identify patterns.

| Date & Time | Name of pupil of member of staff | Male or Female | Room/ Location of computer | Details of Incident (including evidence) | Actions & Reasons |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# 17. Be SMART on the Internet poster

**E-Safety Rules to be displayed in every classroom**


## 18. CURRENT LEGISLATION

*ACTS RELATING TO MONITORING OF STAFF EMAIL*

***Data Protection Regulations (GDPR) 2018***

Guidance to support schools with data protection activity, including compliance with the General Data Protection Regulation (GDPR). This guidance will help schools develop policies and processes for data management, from collecting and handling the data through to the ability to respond quickly and appropriately to data breaches.
https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

*Data Protection Act 1998*

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/actsl998/19980029.htm

*The Telecommunications (Lawful Business Practice)*

(Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

*Regulation of Investigatory Powers Act 2000*

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

*Human Rights Act 1998*

http://www.hmso.gov.uklacts/actsl 998/19980042.htm

*OTHER ACTS RELATING TO ESAFETY*

*Racial and Religious Hatred Act 2006*

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

*Sexual Offences Act 2003*

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs. For more information
www.teachernet.gov.uk

*Communications Act 2003 (section 127)*

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on convComputingion, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

*The Computer Misuse Act 1990 (sections 1 —3)*

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

*Malicious Communications Act 1988 (section 1)*

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

*Copyright, Design and Patents Act 1988*

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

*Public Order Act 1986 (sections 17 —29)*

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

*Protection of Children Act 1978 (Section 1)*
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convComputinged of such an offence may face up to 10 years in prison.

*Obscene Publications Act 1959 and 1964*
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

*Protection from Harassment Act 1997*
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

*Education and inspections act 2006*
An Act to make provision about primary, secondary and further education and about training; to make provision about food or drink provided on school premises or in connection with the provision of education or childcare; to provide for the establishment of an Office for Standards in Education, Children's Services and Skills and the appointment of Her Majesty's Chief Inspector of Education, Children's Services and Skills and make provision about the functions of that Office and that Chief Inspector; to provide for the amendment of references to local education authorities and children's services authorities; to amend section 29 of the Leasehold Reform Act 1967 in relation to university bodies; and for connected purposes.

**19. Covid-19 appendix to E-Safety Policy**

At this time of national crisis, it is more important than ever that Knights Enham Schools provides a safe environment for children; this includes **online safety**. This appendix has been written using the governments guidance: **Children and online safety away from school** and the **guidance from the UK Safer Internet Centre on safe remote learning.**

*Roles and Responsibilities*
Staff are responsible for all links and signposting that they recommend on the school website. These sites must be in keeping with the school's ethos.
This policy appendix, supported by the school's Acceptable Use Agreements for staff, governors, visitors and pupils Covid-19 appendix, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policy: Covid-19 Appendix to Child Protection Policy.

*E-Safety skills development for staff*
- Our staff receives regular information and updates via email about sites and safe signposting that have been checked by the schools Headteacher or the Computing Co-ordinator.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety through the Covid-19 appendix child protection policy and know what to do in the event of misuse of technology.
- All staff are encouraged to incorporate E-Safety activities and awareness into their home-learning page.

*Managing the school E-Safety messages*

- We endeavour to embed E-Safety messages across the school website and on home- learning pages.
- The Covid-19 appendix E-safety policy will be shared with parents and children.

*E-Safety in the Curriculum*

Computing and online resources are increasingly used across the curriculum. We believe safety is essential for the resources that we are promoting on our school website especially during this home-learning period.

- Safe links and websites are linked via the school's Home School Learning page on the website.
- Staff will not suggest web links that infringe copyright and will respect other peoples' information, images, etc.
- Pupils are aware of the impact of online bullying and links will be sign-posted from the school's home-learning pages.

*Password Security*

- All users must read the Covid-19 appendix Acceptable Use Agreement and the school's Covid-19 appendix E-Safety Policy.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and Learning Platforms, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are secure if they are being used in a public domain or on a family computer.
- Due consideration should be given when logging into the Learning Platform as to the browser/cache options (shared or private computer).

*Managing the Internet*

- Staff members will provide links via the school website to Internet resources.
- Staff will not recommend social media pages as the legal age limit to use these pages is 13.
- Staff will discourage the use of social networking sites such as TikToc, House Party, Zoom etc. as these sites are open to hacking and inappropriate content.

*Managing the website*

- The school does not recommend to the pupils any social networking sites.
- Pupils and staff should be mindful to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- We recommend when signing up to online support, that this is carried out in the parent's name and they have full access to the site via a family password.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are encourage to report incidents of bullying to the school via email, this will still be investigated.

*Mobile technologies*

- It may be necessary to communicate with parents and children via personal equipment. If this is the case the Headteacher should be informed before the communication takes place and informed of it content. Every available precaution should be made to safeguard personal equipment, e.g. a staff member's personal phone number.
  If at all possible, the member of staff should contact the Headteacher or admin team to communicate with a family via the school's email system instead.
- Accessing the school admin site for the website via a personal device such as a mobile or a tablet should only be carried out in a secure way and passwords should not be stored automatically on these devices.

*Safe Use of Images / Taking of Images and Film*

- Parents sending images of their child into school via email, consent to these pictures being shared on newsletters and the school website.

*Parental Involvement*

- This update to the E-safety policy will be share electronically with parents.