"Sun Hill Junior School is committed to fostering a safe and secure learning environment in which pupils and adults feel valued and respected and can flourish."

Sun Hill Junior School

ICT & E-safety policy

Name of School	Sun Hill Junior School
Date of Policy Issue/Review	January 2021/January 2023
Name of Responsible Manager/Headteacher	Sue Griffiths (HT & DSL)
Chair of Governors	Katy Toms
Date approved by Governors if statutory:	

Introduction

New technologies provide many educational and social benefits, and we aim to equip our pupils to develop safe and responsible online behaviours to protect them wherever and whenever they go online. We will do this by schooling our pupils with the skills, confidence and knowledge they need to do this.

Aims:
• To raise children's awareness of technology in the world today.
• To teach the children to use and understand a wide range of technology.
• To use a variety of technology, including the internet to enhance and improve work in all areas of the curriculum.

This document outlines the systems and processes in place at Sun Hill Junior School in order to establish and reinforce safe and responsible online behaviours. These guidelines are set out under the following headings:

- **Curriculum**
- **Teaching and Learning**
- **Education**
- **Pupils**
- **Staff**

- **Monitoring and Review Procedures**
- **Parental Support**
- **Key Responsibilities**
- **The Role of the E-Safety Co-ordinator**
- **End User E-Safety Agreements**
- **Further Information**
- **Appendices**

Glossary of terms:

ICT: *Information and Communication Technology*
MAT: *Multi Academy Trust*
LSA: *Learning Support Assistant*
PICS: *Personal Internet and Cyber Safety*
DfE: *Department for Education*
DSL: *Designated Safeguarding Lead*
DDSL: *Deputy Designated Safeguarding Lead*

Curriculum:

- ICT skills will be taught in computing lessons and used across the curriculum.
    - To equip pupils with the confidence and capability to use and express themselves and develop their ideas through, technology throughout their later life.
    - To enhance learning using computational skills.
    - To develop an understanding of how to use technology safely and responsibly at a level suitable for the future workplace and as active participants in a digital world.
    - To respond to new developments in technology.

- Computing lessons meet the requirements of the National Curriculum programmes of study and provide a relevant, challenging and enjoyable Computing curriculum for all pupils.
    - To use computational thinking and creativity to understand and change the world.
    - To reinforce deep links with mathematics, science, design and technology, and the wider curriculum
    - To learn the core the principles of computer science, including how digital systems work, and how to put this knowledge to use through programming.

Teaching and Learning:

The aims of Computing are to equip children with the skills to use technology to become independent learners, so the teaching style we adopt is as active and practical as possible. Often we give children direct instruction on how to use hardware or software, but equally there are

opportunities for individuals or groups of children to use computers and technology to help them in whatever they are trying to study.

We recognise that children may have widely differing prior experience of information technology. This is especially true when some children have access to IT equipment at home, while others do not. We provide suitable learning opportunities for all children by matching the challenge of the task to the ability and experience of the child. The units studied in Computing are planned to build upon prior learning. While we offer opportunities for children of all abilities to develop their skills and knowledge in each unit, we also build planned progression into the scheme of work, so that the children are increasingly challenged as they move up through the school. Similarly we aim to provide a range of devices including laptops and chromebooks for children to use.

Education:

Benefit of using the internet in education

- access to world-wide educational resources including museums, arts and galleries;
- vocational, social and leisure, in school and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments,
- educational materials and effective curriculum practice;
- collaboration across support service and professional associations;
- improved access to technical support;
- exchange of curriculum and administration data;
- access to learning wherever and whenever convenient.
- access to learning platforms
- improved communication with parents and children of the school community

Enhancing Learning

- Our internet access includes filtering appropriate to the age of the pupils. Pupils are taught what internet use is acceptable and what is not, and given clear objectives for internet use.
- Appropriate and efficient use of search engines is part of our Computing curriculum and internet access is planned to enrich and extend learning activities. During 'lockdown' or extended periods when children are not in school, we are able to deliver the entire curriculum as necessary through our learning platform – Google classroom

Evaluating internet content

- We will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law: https://www.copyrightservice.co.uk/copyright/p01_uk_copyright_law for further details of copyright.
- As part of the computing curriculum and safety lessons, children are taught to be appropriately discerning of websites and online content.

Pupils:

- Each pupil has their own unique logon for Google classroom and drive access storing work electronically. It is the class teacher's responsibility to monitor work children are storing in these folders. The network co-ordinators are also able to access and view these folders.
- The following guidelines will be shared with the children throughout their life in the school.
    - Children must never logon to the network as another individual nor save nor delete work in any location other than that to which they have been directed by a member of staff.
    - No work or message produced will be derogatory about any other pupil or member of staff
    - Pupils must not knowingly damage school equipment or online content
    - Pupils will only print once and only if given permission from a member of staff – pupils are unable to print directly from chromebooks.
    - Pupils will only use the computers / chromebooks during lesson time and all devices are unavailable to pupils at break or lunchtime unless under direct supervision of a member of staff.
    - Pupils who break these rules will have their access to the school network, online platform (Google Classroom) and equipment limited or removed.

Introduction to pupils

- Pupils will be informed that network, Google Classroom (including Gmail and Drive) and all internet use is monitored. E-safety rules are reinforced termly, through the Cyber Ambassador scheme, participation in Safer Internet day and in computing lessons. Pupils will be taught as an e-safety unit at the beginning of each academic term in addition to the ongoing safety messages of computing lessons. E-safety lessons will be delivered through assemblies, PSHE, circle time, ICT and Computing.

Inclusion

- All pupils, regardless of race, gender, disability or cultural background have a basic entitlement to Internet use to enhance their learning across the curriculum. Adults working with children who have access to the Internet should ensure equality of access for all and monitor use so that no one group dominates an activity.

Rules for Internet and Computer Safety at School

The following rules will be discussed with all pupils at the start of each academic year.

Children using the school's devices will be expected to follow these rules:

- I will only use the internet when I am being supervised by an adult.

- I will not try to access my home email account from school and will only use my Sun Hill Gmail (Google Classroom) account.
- I will not do anything that might cause damage to computers, chromebooks, tablets, iPads, or any other equipment or data stored on computers.
- I will respect the copyright of other people's work and will not copy, alter or download anything that belongs to someone else, without their permission.
- I will respect other people's work and not use other people's passwords or interfere with their work or files.
- I will not print work without permission from the class teacher or LSA
- I will use the internet responsibly and will not try to access inappropriate websites.
- I will report any concerns I have about online content immediately to an adult.

Personal Internet and Cyber Safety:

The following rules will be discussed with all children and form part of our Computing Curriculum at the start of each academic year. Parents may also be offered the chance to attend a Perins MAT e-safety briefing by a police officer from Hampshire Constabulary

1: Do not give out personal details or photographs.
2: Don't take other people at face value – they may not be what they seem.
3: Never arrange to meet someone you've only ever previously met on the Internet.
4: Always stay in public area of chat where there are other people around.
5: Don't open an attachment or downloaded file unless you know and trust the person who sent it.
6: Never respond directly to anything you find disturbing – save or print it, log off and tell an adult.

The Hampshire Constabulary PICS, Guide for Parents and Children and further information can be found at www.thinkuknow.co.uk

The Acceptable Use Policy: Information & Guidelines for Parents (appendix C) will also be sent to parents at the beginning of each academic year.

Staff:

All staff can use the school network and online Sun Hill Google for Education platform. The school network can be used at any time that staff are on the premises and certain staff may also be able to 'remote in'.

All staff Network and Google for Education use is subject to the following provisions:

- Do not store or create inappropriate or offensive data such as pornographic, racist and other such offensive materials
- No photos or videos to be taken using personal devices. If taking videos/photos with school devices, staff must check the children's permission criteria held in the school office and delete the photo/video as soon as reasonable.
- Users are responsible for all data created or downloaded onto the school network

- No other user should have his or her data compromised through deliberate acts of any member of staff
- All Staff MUST adhere to the GDPR regulations
- Staff have a limited right to professional materials created or stored on the school network. Data that is created for professional reasons shall remain the property of the school and the creator. However if the school wishes to share this data outside of the school then the creator must give his or her written permission. If the creator wishes to share materials made then they have a perfect right to do so. If a person leaves then a copy of all work created for the school such as planning must be left for the school to use or adapt in perpetuity within the school but must not be shared outside the school without the creator's written permission.
- Copyright of material is respected
- Use of personal devices and school equipment for personal reasons is limited to a time when a member of staff is not teaching or supervising pupils.
- Staff should have their personal phones on silent or switched off and out of sight (e.g. in a drawer, cupboard or handbag) during class time or when in contact with children. (*for further information please see the Mobile Phones in School policy*)

Any breach of these provisions will be dealt with according to the severity of the breach. If the breach is a breach of law the police will be called in straight away and all evidence will be preserved. This may result in the school network being unavailable for use while investigations are carried out. If the breach is less severe school disciplinary action would result through established channels.

Teaching E-Safety

E-safety lessons and assemblies include modules within the computing curriculum that teaches children how to keep themselves safe from online bullying, radicalisation, and other forms of child exploitation.

Monitoring and Review Procedures

The Head Teacher and nominated board member will monitor the use of the Internet to ensure that practices and procedures are maintained to ensure e-safety for all.

This policy sits within the School Safeguarding Policies and as such will be reviewed regularly. It can also be found on the school website.

Sun Hill Junior School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from internet use. The school will record any incidents involving technology at home or in school on CPOMS to establish if the e-safety policy is adequate, and its implementation appropriate, any concerns will be reported to the Head Teacher and The Perins MAT Data and Communications Manager. Consequently, a key strategy for minimising risk is to ensure that children are taught about Internet Safety and how to keep themselves safe online.

The school believes this policy to be good practice as adapted from DfE guidelines, but will review this policy regularly as technology adapts and grows

• Where photos of children are published on the school web site (with parental permission) the children will not be identified in any way unless with express permission by parents or carers.
• Where photos of children are published on the school web site the children will be fully clothed (i.e. No swimming photos)
• Where children's work is published on the school website it will be identified by first name and year group only unless with express permission by parents or carers.

Parental Support

Parents' attention will be drawn to the school's e-safety policy in newsletters, the school prospectus and on the school website. E-safety letters will be sent home. Parent information evenings will be offered by either Sun Hill Junior School or Perins MAT. E- Safety will also form a regular part of our Anti- Bullying strategy.

Social Media Guidelines

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that many are signed up either with or without parental knowledge.

As a school we will monitor the use of social networking and ensure it is part of our curriculum. Children will be given an initial experience of chat rooms through Google Classroom stream where it can be monitored and is protected. We will also ensure that parents are fully aware of how to minimise the risk if their children are using external sites. As a school, we do reserve the right to contact sites such as Facebook and ask them to remove our children's accounts.

Key Responsibilities

Key responsibilities of the Senior Leadership Team include:

- Developing, owning and promoting the e-safety vision to all stakeholders. Supporting the e-safety co-ordinator in the development of an e-safe culture. Making appropriate resources available to support the development of an e-safe culture.
- Receiving and regularly reviewing e-safety incident logs.
- Supporting the e-safety co-ordinator in the appropriate escalation of e-safety incidents.
- Taking ultimate responsibility for e-safety incidents.
- Keeping up to date with new e-safety threats to children.

Key responsibilities for teaching and support staff include:

- Contributing to the development of e-safety policies.
- Reading staff policies – and adhering to them.

- Taking responsibility for the security of systems and data.
- Having an awareness of e-safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies, emphasising positive learning opportunities rather than focusing on negatives.
- Embedding e-safety education in curriculum delivery wherever possible. Identifying individuals of concern and taking appropriate action.
- Knowing when and how to escalate e-safety issues.
- Maintaining a professional level of conduct in their personal use of technology, both within and outside school.
- Ensuring pupils have the correct permissions.
- Taking personal responsibility for their professional development in this area.
- Use strong passwords (a mixture of letters, numbers and characters), keep them private and change them regularly.
- Log off or lock workstations when left unattended.

Key responsibilities for children and young people include:

- Contributing to the development of e-safety policies.
- Reading pupil policies – and adhering to them.
- Taking responsibility for keeping themselves – and others – safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.
- Respecting the feelings, rights, values and intellectual property of others.
- Seeking help from a trusted adult if things go wrong, and supporting others who may be experiencing e-safety issues.
- Discussing e-safety issues with parents and carers in an open and honest way.

The Role of the E-safety Co-ordinator

The E-safety co-ordinator role is incorporated into the role of Designated Safeguarding Lead. The Technology Curriculum Team, School Office Manager, SENCo and ELSA may be called upon to assist them in their role to ensure that safeguarding issues are considered from the widest possible perspective.

End User E-safety Agreements

In order to meet with the requirements of this document, relevant e-safety agreements are distributed to pupils (Appendix A) and staff (Appendix B), and relevant information is shared with parents (Appendix C) To ensure rules are understood and agreed to, all user groups will be asked to sign and return a copy of their agreement.

Further Information

For further details about e-safety, visit these websites:

https://www.net-aware.org.uk/ NSPCC and O2 safety awareness website
www.childnet.com/kia - Childnet's interactive internet safety resource
www.digizen.org - A website providing information and advice to encourage responsible digital citizenship.
www.kidsmart.org.uk – a website for teachers, pupils and parents with games and activities alongside effective internet safety advice.
www.chatdanger.com – advice on how to stay safe while chatting online.
www.ceop.gov.uk - Child Exploitation and Online Protection website. CEOP is a police agency tackling child abuse on the internet. This website includes a unique facility that enables parents and young people to make reports of actual or attempted abuse online.

Appendix

A. Pupil E-safety Rules
B. Staff, Governor and Visitor Acceptable Use Agreement
C. Acceptable Use Policy: Information & Guidelines for Parents
D. Response to an incident of concern
E. Flowchart for managing an illegal e-safety incident
F. Flowchart for managing an e-safety incident to be managed in school

Appendix A

Pupil e-Safety Rules

- ☐ I will only use ICT in school for school purposes.
- ☐ I only use the internet at school with permission.
- ☐ I will not tell other people my ICT passwords.
- ☐ I will only open/delete my own files.
- ☐ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ☐ I will not deliberately look for, save or send anything that could be unpleasant or offensive. If I accidentally find anything like this I will close it and tell my teacher immediately.
- ☐ I will not give out my own or anybody else's details such as name, phone number or home address.
- ☐ I will only 'friend' people online that I know in person.
- ☐ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ☐ I will report anything I see, hear or receive online that is unkind, unpleasant or worrying, or if it is from someone that I don't know.
- ☐ I understand that if I do not follow these rules then my access to the Internet may be taken away or limited, and my parents may be told.

Signed…… Date……

Appendix B

Staff, Governor and Visitor Acceptable Use Agreement

This policy is designed to ensure that all staff and volunteers are aware of their professional responsibilities when using any form of ICT. All staff and volunteers are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the ICT or e-safety officer. Please sign and return this document, keeping a copy for your records.

- The school owns the computer network and can set rules for its use.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email and social networking, and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a computer or network for a purpose not permitted by the school.
- I understand that the irresponsible use of the network and internet will result in the loss of network or internet access, and the school may instigate additional sanctions. For serious breaches, the school may involve the police.
- I agree that network access must be made via the user's authorised account and password, and that passwords should be kept as confidential as possible.
- I understand that users may not install or run software on the network without permission from the network manager.
- I understand that all network and internet use at school must be appropriate to education.
- I agree that all copyright and intellectual property rights must be respected.
- I understand that all school e-mail messages shall be written carefully and politely, particularly as e-mail could be forwarded to unintended readers.
- I understand that anonymous messages and chain letters are not permitted using school e-mail addresses.
- I understand that I must take care not to reveal personal information to children or parents through email, personal publishing, blogs or messaging.
- I agree to use school managed messaging systems appropriately and politely.
- I understand that the school ICT systems may not be used for private purposes, unless the Headteacher has given specific permission.
- I agree that any inappropriate access to materials on the network, or on the internet using school computers at home, will be reported to the e-Safety Co-ordinator.

The school may exercise its right to monitor the use of the school's computer systems, where it believes unauthorised use of the school's computer system may be taking place, or that the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read and understood the Acceptable Use Agreement.

Signed……Role…… Date……

Appendix C

Acceptable Use Policy: Information & Guidelines for Parents

Dear Parent/Guardian,

ICT, including the use of the internet, has become an important part of learning at Sun Hill Junior School. We expect all children to be safe and responsible when using the internet and have developed a set of e-safety rules to support this.

A copy of the rules that the children are expected to follow at school is attached to this letter. Please take some time to read and discuss these with your child and return the slip at the bottom of this page to show that they have been understood and agreed. In order to keep your child as safe as possible when using the internet, I suggest that you agree similar rules for home use.

Full details of acceptable use and e-safety are contained in our positive ICT and e-safety Policy, which is available on our website or to read at the school office if required. If you have any concerns or would like further explanation, please do not hesitate to contact me.

Yours sincerely

Sue Griffiths

Head Teacher

Parent/ guardian signature

We have discussed this and …….....(child's name) agrees to follow the eSafety rules and to support the safe use of ICT at Sun Hill Junior School.

Parent/ Carer Signature …….…….…….

Class ……. Date ……

Appendix D

Response to an incident of concern

Internet technologies and electronic communications provide children and young people with the opportunity to broaden their learning experience and develop creativity in and out of school. However, it is also important to consider the risks associated with how these technologies are used.

Any e-Safety Policy should also recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for other users.

These risks to e-safety are, of course, caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents that may involve Child Protection Officers or the Police.

This section will help staff determine what action they can take within the school and when to hand the issue over to the school-based Designated Safeguarding Lead, the e-Safety Officer or the Police Liaison Officer.

Electronic communication

- **Internet collaboration tools:** social networking sites and blogs
- **Internet Research**: web sites, search engines and Web browsers
- **Mobile Phones and personal digital assistants** (PDAs)
- **Internet communications:** e-Mail and instant messaging (IM)
- **Webcams and videoconferencing**

Risk Factors

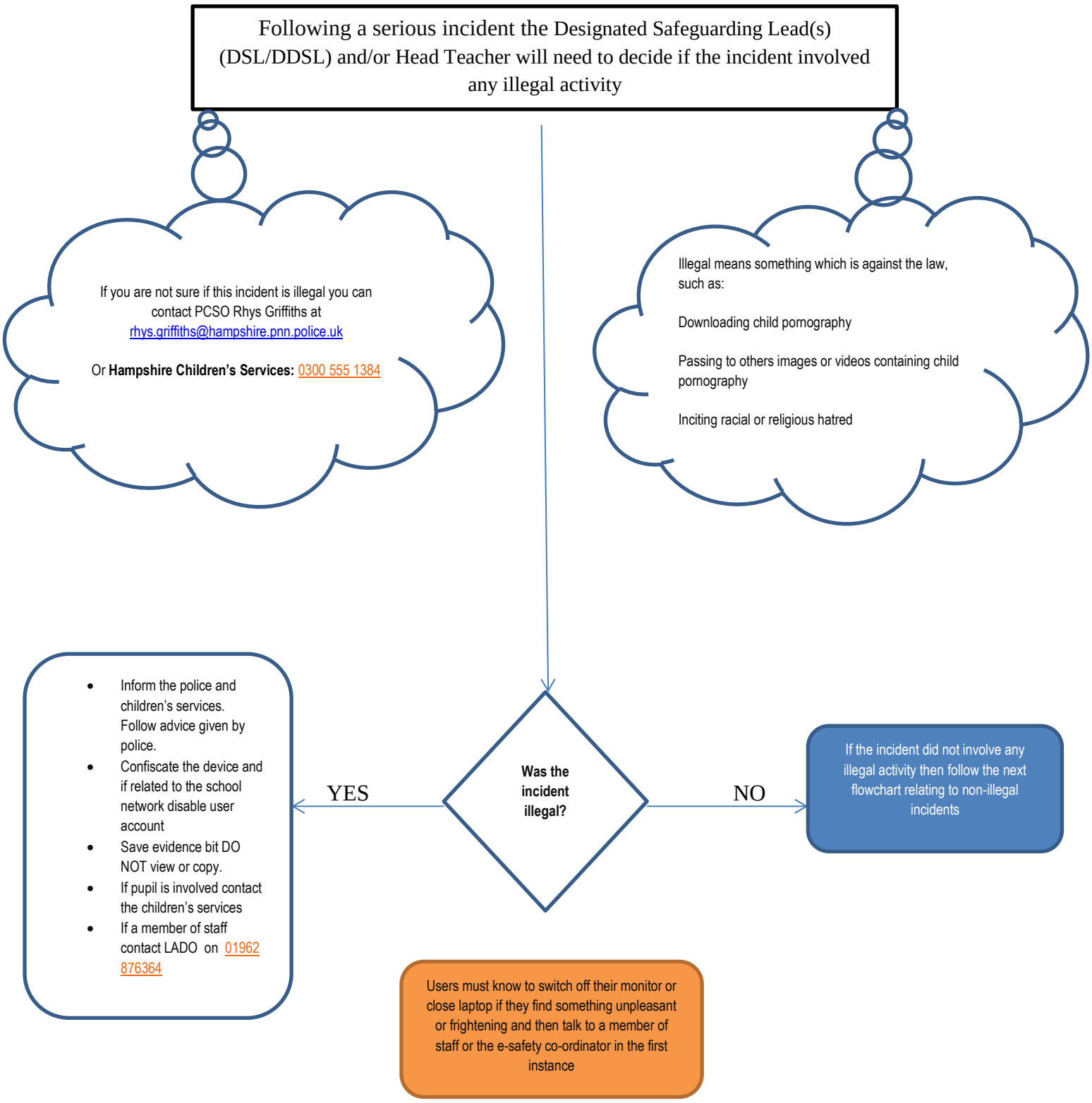
- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Identity theft
- Radicalisation
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information / images
- Hacking and security breaches

Response

The flowchart on the next page is illustrates the approach to investigating an incident of concern. This diagram should not be used in isolation and should always be discussed with a DSL or Head Teacher

Appendix E

Flowchart for managing an illegal e-safety incident



Appendix F

Flowchart for managing an e-safety incident to be managed in school