# ONLINE SAFETY POLICY
# MARCH 2022

**Policy Originator**: Headteacher

**Status:** Non-statutory **Review Period:** 3 Years

**Date:** March 2022 **Next review date:** March 2025

Online Safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for **behaviour, safeguarding, anti-bullying, data handling and photography.**

**Using this policy**

Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been approved by governors.

The online safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones and tablets.

The online safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

1. **Introduction**

In line with current expectations the school has a computer system which gives the children access to the Internet.

Usually, the resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times, they will be able to move beyond these, to sites unfamiliar to the teacher.

The problems and issues that have been highlighted by the media concern all schools. Whilst some of the media interest is hype, there is genuine cause for concern that children might access unsuitable material accidentally.

The purpose of this policy is to:

- Establish the ground rules we have in school for using the Internet
- Describe how these fit into the wider context of our discipline and PSHCE policies
- Demonstrate the methods used to protect the children from sites containing pornography, racist or politically extreme views, misogynistic, misandrist concerns and violence.

The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians.

We feel that the best recipe for success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

## 2. Teaching & Learning: Using the Internet for education

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils

The benefits include:

- access to a wide variety of educational resources including books, art galleries, museums and a range of enhanced learning sites
- rapid and cost-effective world-wide communication
- gaining an understanding of people and cultures around the globe
- staff professional development through access to new curriculum materials, experts' knowledge and practice
- exchange of curriculum and administration data with LA/DfE
- social and leisure use

The school will provide an age-appropriate online safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. The school intends to teach pupils about the vast information resources available on the Internet, using it as a planned part of some lessons. Staff will review and evaluate resources available on web sites appropriate to the age range and ability of the pupils being taught. The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Initially, the pupils may be restricted to sites which have been reviewed and selected for content. They may be given tasks to perform using specific web sites.

As pupils gain experience, they will be taught how to use searching techniques to locate specific information for themselves. Comparisons will be made between research from different sources of information, (e.g. newspapers, books, www). We hope pupils will begin to learn that it can sometimes be appropriate to use the Internet, as opposed to other sources of information, in terms of: the time taken, the amount of information found, the usefulness of information located.

At times, information, such as text, photos, etc. may be 'downloaded' from the Internet for use in pupils' work. Tasks may be set to encourage pupils to view web sites and to search for information.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be made aware that Shalford Infant & Nursery School has its own website which contains information about school activities and learning.

## 3. Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform online policy.
- The security of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- Physical monitoring of the internet by staff will ensure children are accessing appropriate content.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

## 4. Pupils access to the Internet

Our school uses RM as the internet provider and their age-related filtering system, which will minimise the chances of pupils encountering undesirable material. Any school will normally only allow children to use the Internet when there is a responsible adult present to supervise, however, it is unrealistic to suppose that the teacher's attention will always be directed toward the computer/smartboard/ipad screen.

Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils the expectation we have of pupils.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use – child friendly search engines will be used for children to search the internet e.g. www.safesearchkids.com.
- Pupils will be taught how to report unpleasant Internet content
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be shown how to publish and present information appropriately to a wider audience without giving out personal details or information which may identify them.

## 5. Expectations of pupils using the Internet

- At Shalford Infant & Nursery School we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access.
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally they are expected to report it immediately to a teacher or teaching assistant, so that the Service Provider can block further access to the site.
- Pupils must ask permission before accessing the Internet and before printing anything material which they have found.
- Computers and tablets should only be used for schoolwork, unless permission has been granted otherwise.
- At Foundation Stage and Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials
- Complaints of internet misuse will be dealt according to the school behaviour policy. Complaints of a safeguarding nature must be dealt with in accordance with school safeguarding procedures. Pupils and parents will be informed of consequences and sanctions for pupil's misusing the internet and this will be in line with the school's behaviour policy.
- Appropriate elements of the online safety policy will be shared with children.
- Online safety rules will be posted in all networked rooms.

- Children will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of online safety issues and how best to deal with them will be provided for children through the Computing and PHSE curricula.

**6. Social networking & personal publishing**

- Social networking sites and newsgroups will be blocked unless a specific use is approved
- Pupils are advised never to give out personal details on any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils

**7. Staff use of the Internet**

It is important that teachers and support staff are confident enough to use the Internet in their work. The School Online Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies.

Abuse of the Internet or email by any school employee is a serious matter that could result in disciplinary procedures. Email sent via the school proxy server is monitored for inappropriate content and attachments. If staff have doubts as to the legitimacy of any aspect of their Internet use in school they should discuss this with their line manager to avoid any possible misunderstanding.

All staff, including administration, premises manager, governors and helpers should be included in appropriate awareness raising and training annually. Internet use should be included in the induction of new staff.

All staff, including teachers, supply staff, teaching assistants and support staff should read the School Online Safety Policy and its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

**8. Home usage & parental support**

Internet use in pupils' homes continues to increase rapidly and many pupils have unrestricted access to the Internet at home. The school aims to help parents plan appropriate, supervised use of the Internet by helping them to understand more about online safety themselves via online safety workshops for parents and regular online safety information via the school newsletter. Details of sites offering support and guidance on home Internet use are available on the school website. Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters and on the school web site. The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

**9. How will ICT system security be maintained?**

The school ICT systems will be reviewed regularly with regard to security. Strategies will be discussed with the Learning Partners Academy Trust and the LA, particularly where relating to the wireless network, firewall configurations and anti-virus software.

- All users must act reasonably. Loading non-approved software could cause major problems. Good password practice is required including logout after use
- Cabling should be secure and wireless LANs safe from interception
- Servers must be located securely and physical access restricted
- The server operating system must be secured to a high level
- Virus protection for the whole network must be installed and current (this must include arrangements for teacher laptops to be periodically updated)

- The network manager will ensure that the system has the capacity to take increased traffic caused by Internet use
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Leader (headteacher).
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

**10. School website**

- A website can promote the school and link to other good sites of interest.
- The point of contact on the Website should be the school address, school email and telephone number. Staff or pupils' home information will not be published.
- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school website or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children.
- Pupils' full names will not be used anywhere on the website, and particularly not associated with photographs. Parents or carers will have the opportunity to opt out of publication of photographs of their children on the school website at the point of enrolment.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

**11. Email use in school**

- Pupils and staff may only use approved e-mail accounts on the school system
- Only school approved email accounts should be used for email by pupils. This will only occur under direct supervision by an adult and as part of a directed task.
- .Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Incoming e-mails should be treated as suspicious and attachments not opened unless the author is known. Staff to pupil email communication must not take place.
- Emails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. The forwarding of chain messages is banned. In the school context, email should not be considered private and the school and the Learning Partners Academy Trust reserve the right to monitor email.

**12. Mobile phone and handheld device use in school**

- Mobile phones and personally owned mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Mobile phones and personally owned devices will not be used in any way during lessons or formal school time and should be switched off or silent at all times. Bluetooth communication should be 'hidden' or switched off.
- If a staff member is expecting a personal call which is urgent and needs to be answered they may leave their phone with the School Office to answer on their behalf or seek specific permissions to use their phone at other than their break times or after school.

- Staff use of mobile phones during the school day will normally be limited to the lunch break and after school. The school reserves the right to search the content of any mobile or handheld device on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- All visitors to school are requested to keep their phones on silent.
- Staff should not use personally owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties such as contacting pupil's parents, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- No pupils should bring his or her mobile phone or personally owned device into school. Any device brought into school will be confiscated.

**13. Protecting personal data**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998
- Should any pupils encounter any offensive materials online accidentally they are expected to report it immediately to a teacher or teaching assistant, so that the Service Provider can block further access to the site.
- The Teacher or Teaching assistant should record the incident on the school's safeguarding system, CPOMS, which is then reviewed by the designated Safeguarding Lead. Relevant parents will be informed. All incidents are monitored by a member of the Senior Leadership Team.
- The Head teacher and DSL should use the flow chart (Appendix 3) along with the screening tool and the Surrey Child Protection Procedures to determine next steps in supporting the child involved in the incident. Schools' DSL will be conversant with these and the processes for referral.
- Should any pupils encounter any cyber bullying by other pupils in the school, this should be recorded on CPOMS by the staff member to which the information was disclosed, in line with our Anti-Bullying Policy. Staff should be aware that concerns can occur both online and offline simultaneously.
- The Designated Safeguarding Lead will inform the head teacher/deputy head of the incident recorded on CPOMS.
- The head teacher will interview all concerned and will add further action to CPOMS.
- Class teachers and support staff (as appropriate) will be kept informed.
- Parents will be kept informed.
- Appropriate disciplinary action will be taken.
- The log of online incidents will be monitored and reviewed regularly to ascertain whether any changes need to be made, e.g. to the school's online safety policies, anti-bullying policies, training, curriculum content.

Appendix 1

# ICT ACCEPTABLE USE POLICY/CODE OF CONDUCT
# March 2022

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff and visitors are aware of their responsibilities when using any form of ICT. All staff and visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Online Safety Leader.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, smart watches, email, 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 school ICT system for a purpose not permitted by its owner.
- I will only use the school's email / Internet / network and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will ensure that all electronic communications with parents and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.
- I will not install any hardware of software without the permission of the IT technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without the permission of the parent/carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will report any incidents of concern regarding children's safety to the Online Safety Leader, a Designated Safeguarding Lead or the Headteacher.
- I will ensure that electronic communications with pupils, parents and ex-pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will support the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure my school laptop (where applicable) has a secure password on it. I will only use an encrypted USB pen.
- I will not use my own camera to take photos of children and I will not store/download any photos of children at my house on other devices or storage systems.

Appendix 2

# ICT Acceptable Use Policy for Visitors
# MARCH 2022

All visitors to Shalford Infant & Nursery School must adhere to our Acceptable Use Policy for visitors. This policy covers email, the internet and mobile devices, including smart watches.

**If you do not understand anything in this policy, please ask for clarification.**

- Mobile phones and other mobile devices are not allowed to be used on the school site. Smart watches must not be used for any other use than telling the time.

- Photographs or videos of pupils must not be captured by parents or visitors on the school site, without the express permission of the Headteacher.

- If granted permission to capture images of pupils, the images must not be shared (i.e. on social media) if they clearly show any pupil other than your own child.

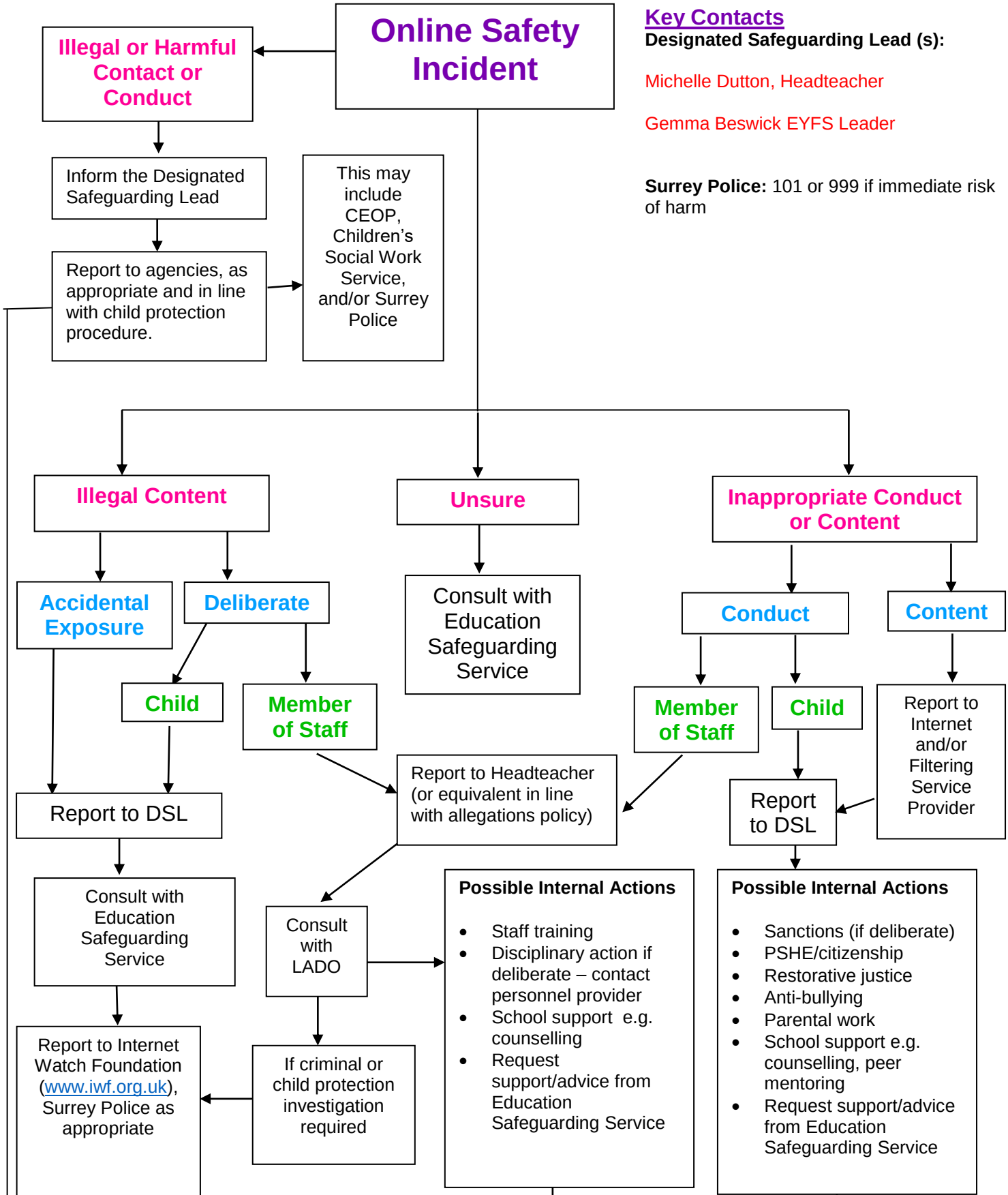
- Access to the school WiFi will not be granted to visitors. Requests to access the Guest WiFi will be considered based on visitor activities.

- Visitors who are granted access to our ICT network must not look at inappropriate materials such as pornography or extremist materials.

- If you witness anyone capturing images of a pupil at an inappropriate or not-permitted time, please report this to one of the Designated Safeguarding Leads immediately.

Appendix 3

# Responding to an Online Safety Concern



Record incident and action taken. Review policies and procedures and implement changes