Locks Heath Infant & Nursery School

E-Safety Policy

Policy reviewed by staff	Review date
Spring 2 2026	Spring 2 2027

This policy should be read in conjunction with the following policies:

- IT and Computing Policy
- Staff Acceptable Use of IT Policy
- Social Media Policy
- Anti-bullying Policy
- Child Protection & Safeguarding Policies

Policy Statement

This e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – pupils, all staff, governing body, parents and volunteers.

CPOMS – system of recording E-Safety concerns for any child(ren) at the school. There is a dedicated category of recording on this online system.

At Locks Heath Infant & Nursery School, the safeguarding of pupils is considered extremely important. As we use technology and the Internet across all areas of the curriculum in school and as children have increased ease of access to devices connected to online material and games outside of school, online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is as such:

- To ensure that the whole school community has the knowledge to stay safe online.
- To ensure risks are identified, assessed and lessened (where possible) in order to reduce any harm to the child or liability to the school.

A copy of this policy will be available for parents to access via the school website.

Roles & Responsibilities

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they have delegated review of this policy to the headteacher and the staff at the school.

Safeguarding governor(s) will be appointed to ensure aspects of this policy are checked and challenged as part of the wider governance of safeguarding. These governors will ensure they keep up to date with emerging risks and threats through technology use

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the E-Safety Officer as indicated below.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipients, i.e. pupils, all staff, senior leadership team and governing body.
- Parents will be signposted to various resources and websites regarding e-safety as part of the school's preplanned communication strategy and in response to incidents where children may be at increased risk. Parents will also have the opportunity to attend an E-Safety workshop within our local cluster of schools.
- The designated E-Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All E-safety incidents are dealt with promptly and appropriately.

E-Safety Officer

The day-to-day duty of the e-Safety Officer is devolved to the Computing subject coordinator. As Designated Safeguarding Lead (DSL), the Headteacher (along with Deputy Designated Safeguarding Leads ((DDSLs)) who are the Assistant Headteacher and Home School Link Worker) also has a responsibility to recognize and act on any concerns raised around E-Safety through CPOMS, overseeing and ensuring appropriate responses to recorded incidents and reporting concerns to children's services where appropriate.

The E-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Work with the Headteacher, Assistant Headteacher and Home School Link Worker to plan reactive strategic actions to incidents that arise throughout the year.
- Work with the Headteacher, Assistant Headteacher and Home School Link Worker to frequently review the E-Safety Parent communication strategy to ensure it is kept up to date and effective in reducing the number of recorded E-Safety incidents on CPOMS.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.

- Work with the school's IT provider to carry out monitoring exercises to check the effectiveness of the school's filtering system, bringing any issues to the attention of the Headteacher immediately.
- E-Safety concerns involving children accessing inappropriate content at school and / or at home: Ensure staff know what to report and ensure the appropriate audit trail is in place on CPOMS in order for the DSL and DDSLs to able to monitor occurring themes.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.

ICT Technical Support Staff

Technical support staff for Locks Heath Infant & Nursery School are Drift IT Ltd, and are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any e-safety technical solutions such as Internet filtering are operating correctly, working with the E-Safety Officer to assess the effectiveness of this service.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the E-safety Officer and Headteacher.

All Staff

The boundaries of use of ICT equipment and services in this school are given in the Acceptable Use of IT Policy for staff; any deviation or misuse of IT equipment or services will be dealt with in accordance with the school's code of conduct and disciplinary procedures.

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident involving children reporting that they have accessed inappropriate content in school or outside of the school site must be reported to the E-Safety Officer and the DSL / DDSLs via CPOMS immediately.
- Other E-Safety incidents where staff are reporting issues with inappropriate use of the school's IT equipment or internet access should be reported to the E-Safety Officer (and an e-safety Incident report is filled out, see Appendix I), or in their absence to the Headteacher. If you are unsure, the matter is to be raised with the E-Safety Officer or the Headteacher to make a decision.
- Staff should report directly to the Headteacher should an issue or allegation occur that the E-Safety Officer has undertaken inappropriate use of the school's IT equipment or internet access.
- Staff should report directly to the Chair of Governors (a.governor@locksheath-inf.hants.sch.uk) should an issue or allegation occur that the Headteacher has undertaken inappropriate use of the school's IT equipment or internet access.
- The reporting flowcharts (Appendix IV) outlined within this e-safety policy are fully understood, and are accessible should an incident occur.
- Confidential files are secure and protected to ensure access is only granted to those who are authorised.
- Staff login passwords are regularly changed, and that passwords are not shared to ensure confidentiality of files and information.

- Staff should endeavor to keep up to date with the latest and emerging risks and dangers associated with the online world. NSPCC recommend using this site to keep up to date with these: https://www.net-aware.org.uk/
- Staff should also keep up to date with the school website links connected to e-safety – these can be found here: https://www.locksheathinfant.com/useful-links/

All Pupils

E-Safety is embedded into our curriculum through taught units of work and regular PSHE. Our pupils will be proactively taught the learning values through their learning as well as day to day learning across the school. These values are expected of the children regardless of which platforms they are communicating with. Pupils will be given the age-appropriate advice and guidance by staff on a regular basis, for example before each IT lesson. Similarly all pupils will be fully aware how they can report areas of concern whilst at school or outside of school, by following the 'SMART' initiative (Appendix V).

Parents and Carers

Parents play a vitally important role in the development of their children and as such the school will endeavour to ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, workshops, school newsletters and information, and material available via the school website, the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that pupils are empowered. Parents will also receive a copy of 'SMART' poster (Appendix V). Parents will be signposted to e-safety workshops held within the local cluster of schools.

Technology

Locks Heath Infant School uses a range of mobile devices. In order to safeguard the pupil and in order to prevent loss of personal data we adopt the following assistive technology:

Internet Filtering – we use software provided by Hampshire County Council's School's Broadband, which provides a service designed for children. It includes a 'firewall', which prevents access to inappropriate websites (determined by the age of the user) and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The software is called '***Netsweeper***' and this is overseen and controlled on behalf of the school by ***Drift IT*** who currently have the school's IT contract. The IT Coordinator, E-Safety Officer and IT Support are responsible for working together to ensure that the filtering is appropriate and that any issues are brought to the attention of the Headteacher, who will then report to Hampshire County Council. Hampshire School's Broadband will provide periodical reports for the IT Coordinator and E-Safety Officer – these will be used to assess appropriate use of web searches by staff and children.

Email Filtering – we use software provided by Hampshire County Council's School Broadband, that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script that could be damaging or destructive to data; spam email such as a phishing message.

Portable hard drives/memory sticks – staff will ensure that confidential files are not kept on portable hard drives and memory sticks, and, wherever possible, such devices will be password protected.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated regularly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

Safe Use

Internet – Locks Heath Infant & Nursery School view the use of the Internet in school is a privilege, not a right. Any unacceptable use of the internet will be dealt with by staff accordingly.

Email – All staff must ensure that the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Photos and videos – Digital media such as photos and videos are covered in the schools' Acceptable Use of IT Policy, and is re-iterated here for clarity. All parents wishing images of their child(ren) to be used by school staff for any publishable or online media content must give their permission. Non-return of the permission form will be assumed as non-acceptance.

Social Networking – Locks Heath Infant School is fully aware of social networking within today's society. However, all staff and volunteers must take caution when using social media. The schools' Acceptable Use of IT Policy and Social Media Policy outline the use of Social Networking in more detail and give staff the necessary guidance and expectation.

Incidents – E-Safety incidents where children are directly involved or have seen or been exposed to inappropriate content, must be recorded on CPOMS by the staff member who received or became aware of the disclosure. Any other e-safety incident is to be recorded on an incident log, and brought to the immediate attention of the E-Safety Officer, or in their absence the Headteacher. See Appendix IV for a flow chart outlining what to do in an incident. The E-Safety Officer will assist you in taking the appropriate action to deal with the incident.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Locks Heath Infant & Nursery School will have an annual programme of training which is suitable to the audience. The same material will be available for the parents to access via the school website and workshops run by the local cluster of schools.

E-Safety for pupils is embedded into the curriculum; whenever IT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupil's learning. It is recommended that each time before using the internet, pupils are reminded of the 'SMART' posters (Appendix V), which should be displayed in each classroom and room with IT facilities.

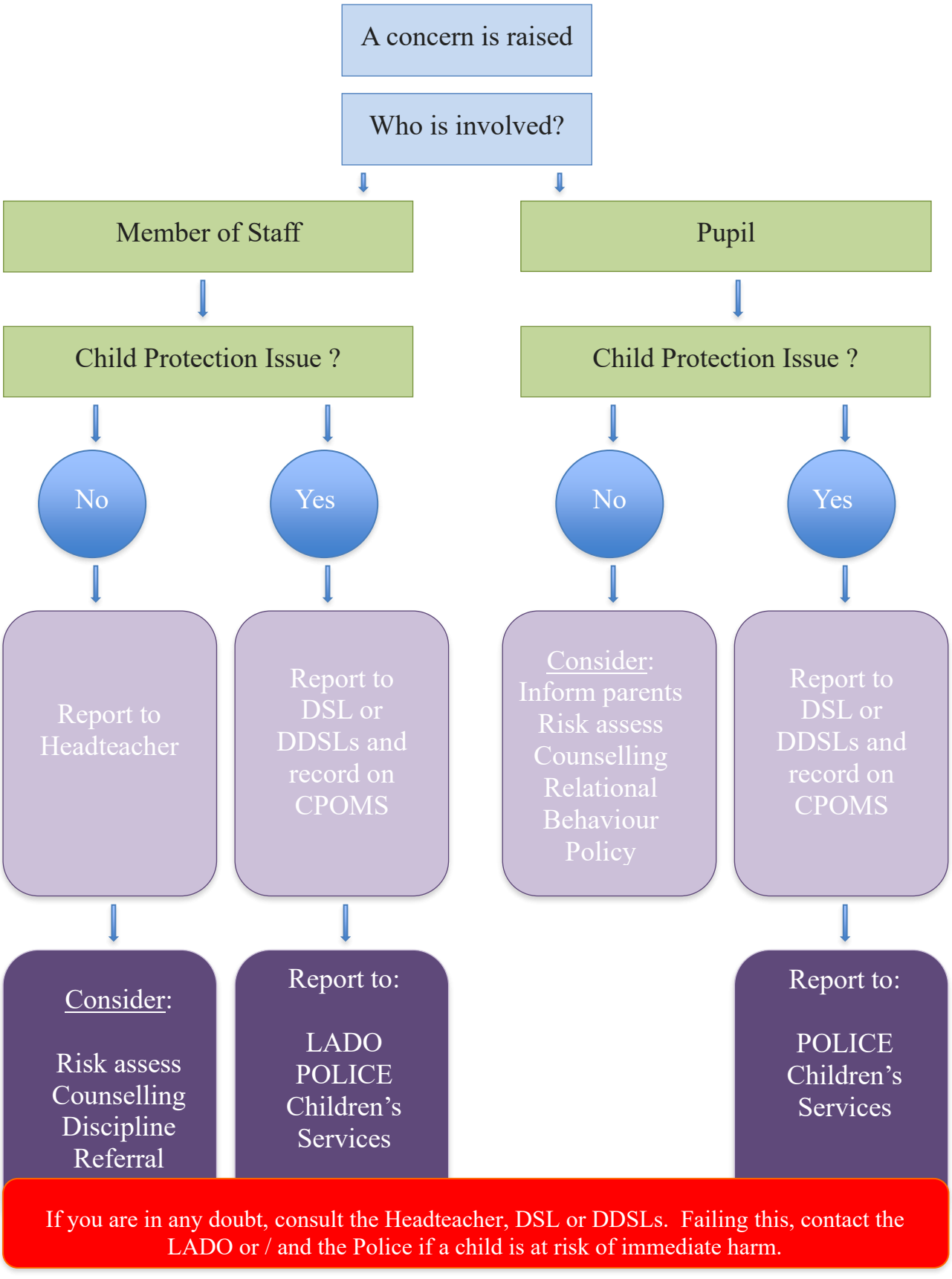
As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The E-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and the responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

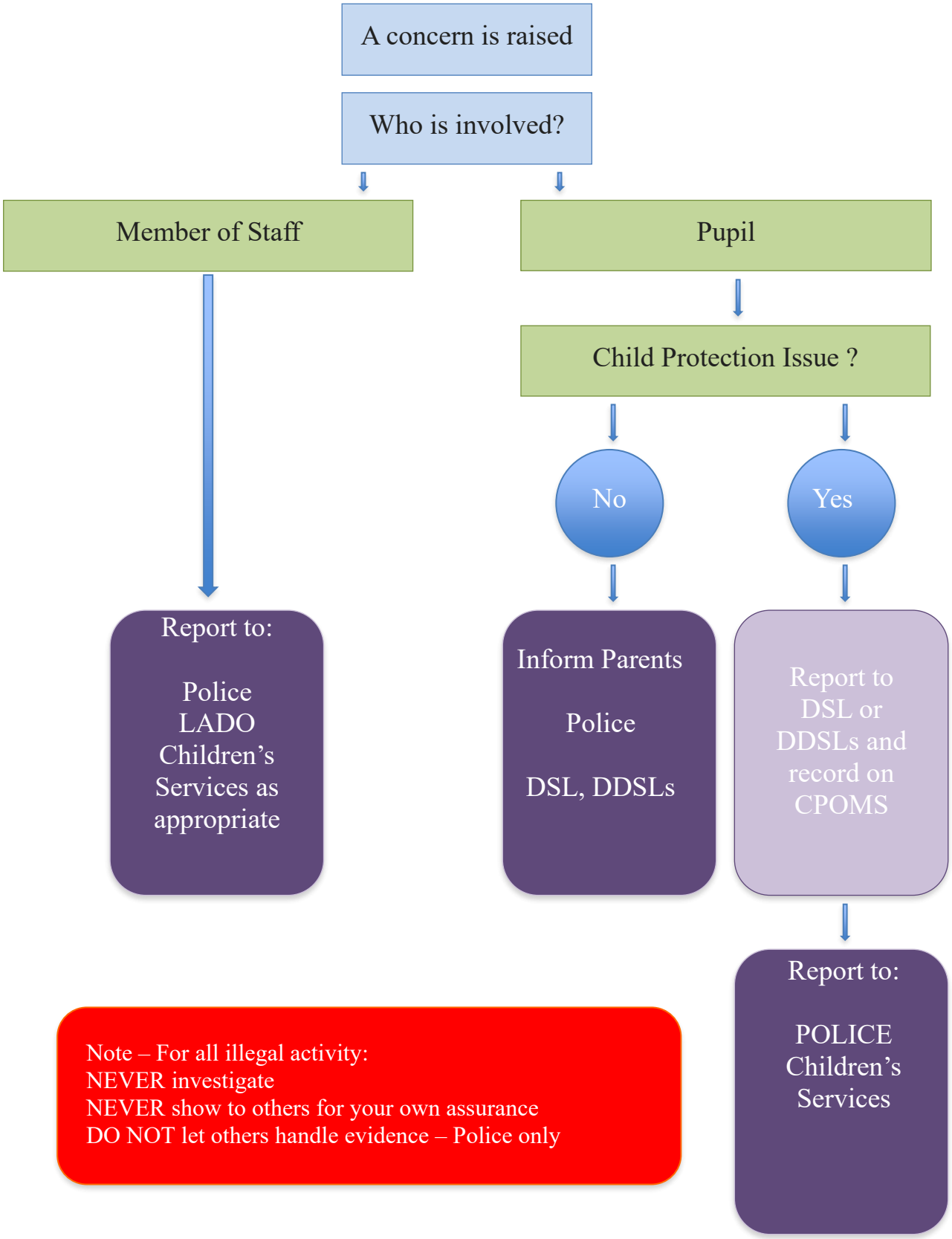
Appendix I
E-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*
	When:	**When:**
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)		
Review Date:		
Result of Review:		
Signature (Headteacher)		**Date:**

Appendix IV
Inappropriate Activity Flowchart



Appendix IV (cont.)
Illegal Activity Flowchart



Appendix V

Our internet safety rules

Note: This poster is to be displayed at all times in classrooms and other rooms which have IT facilities. It is recommended that staff refer to this poster prior to any IT use.