# Sywell CEVA Primary School

# Online-Safety & Acceptable Use Policy

*'Working Together in God's Hands'*

## Policy Statement

The purpose of the Acceptable Use Policy is to clearly identify for the whole school community:

i) the steps taken in school to ensure the safety of pupils when using the internet, e-mail and related technologies

ii) the school's expectations for the behaviour of the whole school community whilst using the internet, e-mail and related technologies within and beyond school

iii) the school's expectations for the behaviour of staff when accessing and using data.

For clarity, the Online-safety policy uses the following terms unless otherwise stated:
**Users -** refers to staff, governing body, school volunteers, students 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** – students, all staff, governing body, parent.

Safeguarding is a serious matter; at Sywell CEVA Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as online-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 twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk-free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Sywell CEVA Primary School website; upon review all members of staff will sign as read and understood both the online-safety policy and the Staff Acceptable Use Policy. (Appendix 1) A copy of the Students Acceptable Use Policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet. (Appendix 2)

Head teacher name: Mrs Russell Lunn Signed:

Chair of Governors: Mrs Annette Ray Signed:

Review Date: June 2017 Next Review: June 2018

# Policy Governance (Roles & Responsibilities)

### Governing Body

The governing body is accountable for ensuring that our school is deploying the policy:

- Review this policy at least annually and in response to any online-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of online-safety at the school who will:
    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Head teacher in regards to training, identified risks and any incidents.

### Head teacher

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

The Head teacher will ensure that:

- Online-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated Online-Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All online-safety incidents are dealt with promptly and appropriately.

### Online-Safety Officer

The day-to-day duty of Online-Safety Officer is Russell Lunn
The Online-Safety Officers 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.
- Review this policy regularly and bring any matters to the attention of the Head teacher.
- Advise the Head teacher, governing body on all online-safety matters.
- Engage with parents and the school community on online-safety matters at school and/or at home.
- Deliver a termly programme of Online Safety assemblies
- Plan and implement an Online Safety and Digital Citizenship curriculum across all year groups
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the online-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical online-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make themselves aware of any reporting function with technical online-safety measures, i.e. internet filtering reporting function; liaise with the Head teacher and responsible governor to decide on what reports may be appropriate for viewing.

**ICT Technical Support Staff**

Technical support staff 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 online-safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the online-safety officer and Head teacher.
    - The IT System Administrator password is to be changed on a monthly (30 day) basis.

**All Staff**

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 Head teacher.
- Any online-safety incident is reported to the Online-Safety Officer and an Online-Safety Incident report is made (Appendix 3). If a member of staff is unsure, the matter is to be raised with the Online-Safety Officer to make a decision.
- The reporting flowcharts (Appendix 4) contained within this online-safety policy are fully understood.

**Visitors and Volunteers**

All visitors and volunteers should refer any online safety concerns to the school Designated Safeguarding Leads as explained in the school’s Safeguarding leaflet.

**All Pupils**

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

Online-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school:

- pupils are taught the SMART rules (KS2) and SID’s Top Tips (FS and KS1) within Online Safety lessons and assemblies
- a hyperlink to CLICK CEOP is found on the school website and pupils are made aware of this in KS2

**Parents and Carers**

Parents play the most important role in the development of their children; the school contributes towards parents' awareness as appropriate to help them to have the skills and knowledge they need to ensure the safety of their children outside the school environment. Through parents' evenings and school newsletters, the school will keep parents up to date with new and emerging online-safety risks and will involve parents in strategies to ensure that students are empowered.

Parents are regularly reminded of the hyperlink to CLICK CEOP on the school website, to provide them with a reporting mechanism in the event of any cause for concern relating to any child regarding their Online Safety.

## Technology

Sywell CEVA Primary School uses a range of devices including PC's, laptops and iPads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

**Internet Filtering** – we use Schools Broadband that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is 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 Computing Coordinator, online-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head teacher.

**Passwords** – all staff and students will be unable to access any networked device without a unique username and password. Staff passwords will change on a termly basis or if there has been a compromise, whichever is sooner. The Computing Coordinator and IT Support will be responsible for ensuring that passwords are changed.

**Anti-Virus** – All capable devices will have anti-virus software. This software will be updated monthly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Head teacher if there are any concerns. All USB peripherals such as keydrives are to be scanned for viruses before use.

## Safe Use

**Internet** – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this Online-Safety Policy and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy. Parents will discuss with their child in Key Stage 1 and sign the policy.

**Email** – All staff are reminded that emails are subject to Freedom of Information requests, and as such 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 to communicate with parents is not permitted. All teaching staff are provided with a an email address. In addition, then Headteacher, Senco and Bursar have individual school email accounts set up by the local authority that allow for the secure sharing of information.

**Photos and videos** – Digital media such as photos and videos are covered in the school's child protection policy and safeguarding policy, and is re-iterated here for clarity. Photographs are not permitted of the children by parents and friends of the school. Staff are advised against taking photographs or video of the children on their own personal devices either in school or when on visits. However, in exceptional circumstances, eg the battery dies on the school device, photographs can be taken on a personal device but must be downloaded straight away on the return to school and then deleted before the device is taken off the premises.

**Sharing** – the school uses a sharing service 'Seesaw' to share work with parent in KS1 and KS2. Sywell CEVA Primary School is fully supportive sharing services as a tool to engage and collaborate with learners, and to engage with parents and the wider school community.

Pictures of children will only be shared with parents via Seesaw if the permission slip has been returned to school completed.

**Notice and take down policy** – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

**Incidents** - Any online-safety incident is to be brought to the immediate attention of the Online-Safety Officer, or in his absence the Deputy DSL (Sonia Byrne).. The Online-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log. (See appendix 1 and 3) All children have been informed about the CEOP button as a way or reporting something they are not happy with.

## Online Safety Curriculum and Assemblies

**Curriculum Plan** – Online-Safety for students is embedded into the curriculum; whenever ICT 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 student's learning.

Over the course of the academic year, every year group in Key Stages 1 and 2 will experience 6 lessons of Online Safety and Digital Citizenship (one per half term). Children in the Foundation Stage will experience 3 lessons during the academic year. Each half term's lesson will sit within a school-based theme to ensure continuity across the school (See appendix 6). Several websites and a range of interactive content is used to support this delivery, which is communicated to parents via letters and emails. The overview of the Online Safety and Digital Citizenship Curriculum is published on the school website.

**Assemblies** – In addition to the taught curriculum, Online Safety Assemblies are delivered to pupils once every term. Pupils are split into two groups for the assemblies to ensure the content is age appropriate: Reception to Year 3 and Years 4 to 6. The content of the assemblies is communicated to parents via email and letter. It is also uploaded onto the school website for parents to access. The theme of the Spring Term assembly follows the theme of the annual Safer Internet Day from the UK Safer Internet Centre. The Autumn Term and Summer Term assemblies cover a range of different themes.

**Training** – 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, Sywell CEVA Primary School will have an annual programme of training which is suitable to the audience.

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

The Online-Safety Officer is responsible for organizing and offering training for the school year to the Head teacher and 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 Head teacher for further CPD.

# Appendix 1

## Acceptable Use Policy – Staff

**Note: All Internet and email activity is subject to monitoring**

You must read this policy in conjunction with the Online-Safety Policy. Once you have read and understood both you must sign this policy sheet.

**Internet access** - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an online-safety incident, reported to the Online-safety officer and an incident sheet completed.

**Social networking –** is allowed in school in accordance with the online-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks

**Use of Email –** staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

**Passwords** - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

**Data Protection –**On no occasion should data concerning personal information be taken offsite on an unencrypted device.

**Images and Videos** - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

**Use of Personal ICT** - use of personal ICT equipment is at the discretion of the Head teacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by the Online-Safety Officer. Use of mobile phones to take photos or video of the children is not advised unless it is an exceptional circumstance eg battery dies on school device. If this happens the photos must be downloaded straight away on the return to school and deleted before the device leaves the premises.

**Viruses and other malware** - any virus outbreaks are to be reported to the School Broadband Helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

**Online-Safety –** like health and safety, online-safety is the responsibility of everyone to everyone. As such you will promote positive online-safety messages in all use of ICT whether you are with other members of staff or with students.

**NAME:**

**SIGNATURE:**

**DATE:**

# Appendix 2

## Online Safety Rules

**I promise** to only use the school equipment for school work that the teacher has asked me to do.

**I promise** not to look for, or show other people, things that may upset them.

**I promise** never to use anybody else's user account and not to ask someone their password.

**I promise** to never click on any pop ups or adds or buy anything online.

**I will not** use other people's work or pictures without checking I have permission to do so.

**I will not** damage the equipment; if I accidentally damage something I will tell my teacher.

**I will not** share personal information online with anyone.

**I will not** download anything from the Internet unless my teacher has asked me to.

**I will not** copy other people's work from websites.

**I will** let my teacher know if anyone asks me for personal information.

**I will** let my teacher know if anybody says or does anything that is hurtful or upsets me.

**I will** be respectful to everybody online; I will treat everybody the way I want to be treated.

**I will** tell my teacher if I see anything that upsets me on the Internet.

**I understand** – that some people on the Internet are not who they say they are and some people can be nasty. I will tell my teacher if I am ever concerned in school or my parents if I am at home.

**I understand** – if I break the rules there will be consequences of my actions and my parents will be told.

Signed (Parent):

Signed (Student):

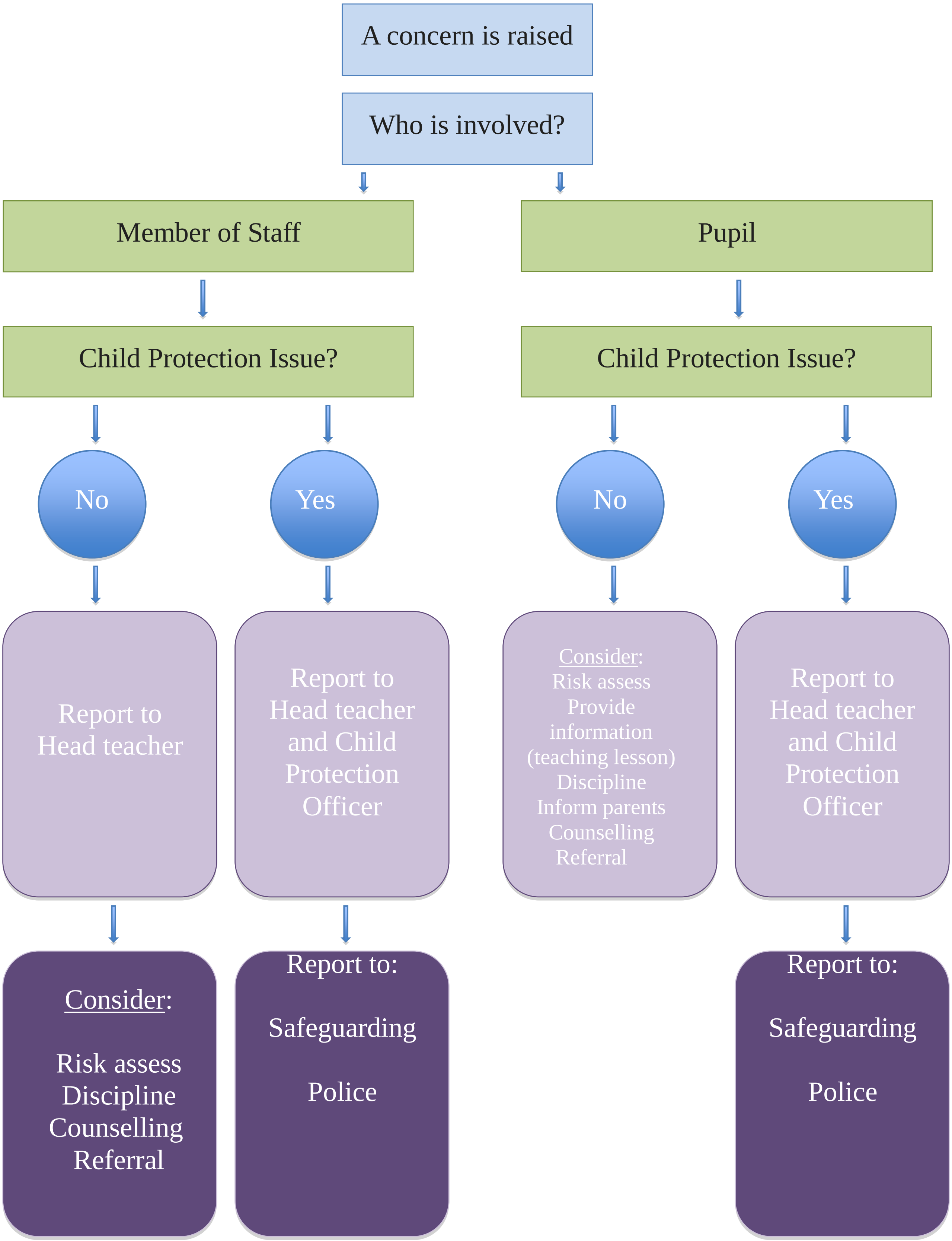
Date:

# Appendix 3

## Online-Safety Incident Log

| | | | |
|---|---|---|---|
| **Number**: | **Reported By:** *(name of staff member)* | **Reported To:** *(e.g. Head, Online-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 (Head teacher)** | | **Date:** | |
| | | | |
| **Signature (Governor)** | | **Date:** | |

# Appendix 4
## Inappropriate Activity Flowchart



A concern is raised

Who is involved?

Member of Staff

Child Protection Issue?

No

Report to Head teacher

Consider:

Risk assess
Discipline
Counselling
Referral

Yes

Report to Head teacher and Child Protection Officer

Report to:

Safeguarding

Police

Pupil

Child Protection Issue?

No

Consider:
Risk assess
Provide information (teaching lesson)
Discipline
Inform parents
Counselling
Referral

Yes

Report to Head teacher and Child Protection Officer

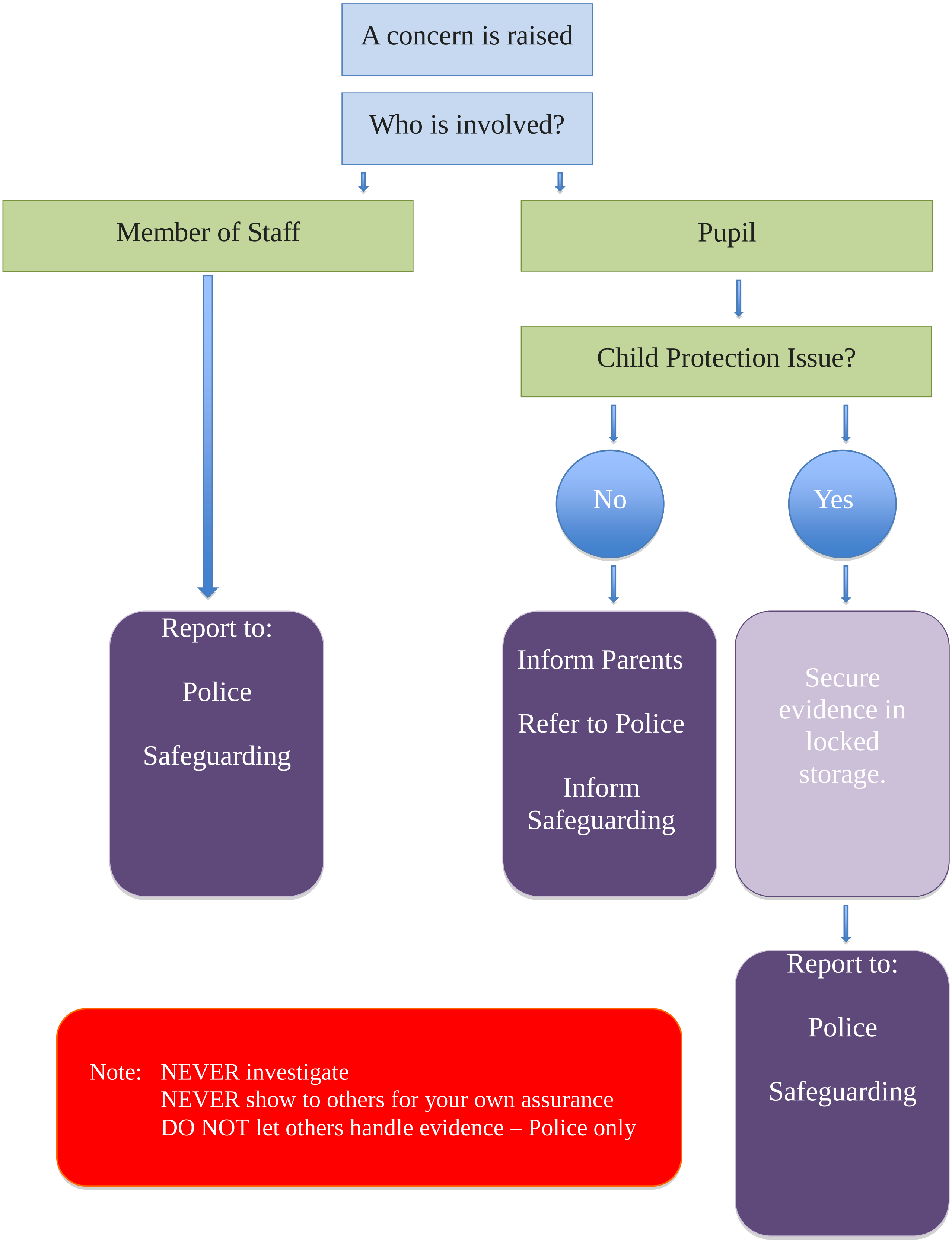
Report to:

Safeguarding

Police

If you are in any doubt, consult the Head teacher, Child Protection Officer or Safeguarding

# Illegal Activity Flowchart



A concern is raised

Who is involved?

Member of Staff

Pupil

Child Protection Issue?

No

Yes

Report to:

Police

Safeguarding

Inform Parents

Refer to Police

Inform Safeguarding

Secure evidence in locked storage.

Report to:

Police

Safeguarding

Note: NEVER investigate
NEVER show to others for your own assurance
DO NOT let others handle evidence – Police only

# Appendix 5

## Risk Log

| No. | Activity | Risk | Likelihood | Impact | Score | Owner |
|---|---|---|---|---|---|---|
| 1. | Internet browsing | Access to inappropriate/illegal content - staff | 1 | 3 | 3 | Online-Safety Officer<br>IT Support |
| 1. | Internet browsing | Access to inappropriate/illegal content - students | 1 | 3 | 3 | Schools Broadband<br>Online Safety Coordinator<br>DSL |
| 2. | Blogging | Inappropriate comments | 1 | 1 | 2 | All comments are viewed by staff first before being posted. |
| 2. | Blogging | Using copyright material | 1 | 2 | 2 | Staff are informed about copyright material and should know not to post it. |
| 3. | Email | Students sending and receiving inappropriate emails. | 1 | 3 | 3 | Emailing covered in the computing curriculum.<br>Online-safety curriculum covers messaging appropriately.<br>See section in policy on Emails. |

**Likelihood:** **How likely is it that the risk could happen (foreseeability)?**
**Impact:** **What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc?)**

**Likelihood and Impact are between 1 and 3, 1 being the lowest. Multiply Likelihood and Impact to achieve score.**
**LEGEND/SCORE:** **1 – 3 = Low Risk**
**4 – 6 = Medium Risk**
**7 – 9 = High Risk**

**Owner:** **The person who will action the risk assessment and recommends the mitigation to Head teacher and Governing Body. Final decision rests with Head teacher and Governing Body.**

# Appendix 6

## Overview of Online Safety and Digital Citizenship at Sywell CEVA Primary School

**Assemblies:**

3 assemblies per academic year will focus on Online Safety. These assemblies will be differentiated across the Key Stages. The content of the assemblies, with any associated videos and resources, will be shared with the parents by letter. This is to encourage them to continue to discuss the focus of the assemblies at home and to build a partnership of Online Safety between school and home.

**Digital Citizenship and Online Safety within PSHE:**

Over the course of the academic year, every year group in Key Stages 1 and 2 will experience 6 lessons of Digital Citizenship (one per half term). Children in the Foundation Stage will experience 3 lessons during the academic year.

Each half term's lesson will sit within a school-based theme to ensure continuity across the school. The 6 themes are:

| Term | Theme | Focus |
|---|---|---|
| Autumn 1 | Keep It Private | Knowing what information should be kept private |
| Autumn 2 | Believe It or Not! | Exploring the idea that not everything online is real or reliable |
| Spring 1 | Making Decisions | Developing the skill to know where to go for help |
| Spring 2 | My Online World | Understanding the role of technology in their own life |
| Summer 1 | Digital Citizens | Exploring their responsibilities as a Digital Citizen |
| Summer 2 | Online Friends | Knowing what make a good online friend and how to be one |

Resources from Common Sense Media: https://www.commonsensemedia.org/educators/scope-and-sequence