E-Safety Policy

Policy Statement

For clarity, the e-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, parents.

Safeguarding is a serious matter; at St Ives Primary & Nursery School we use technology and the Internet extensively across all areas of the curriculum. 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 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 St Ives Primary & Nursery School website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. A copy of this policy and 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.

Headteacher Name: Signed:

Chair of Governors: Signed:

Review Date: March 2019 Next Review: March 2020

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-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 e-safety at the school who will:

  - Keep up to date with emerging risks and threats through technology use.
  - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
  - Attendance at E-safety Group meetings.

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 (or more than one), as indicated below.

The Headteacher will ensure that:

- E-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 e-safety Officer(s) 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 E-safety Officer is devolved to Eve Moore.

The E-safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself 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 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.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.

- Ensure any technical e-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 him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.
- Lead the E-safety Group.

ICT Technical Support Staff

(Note: if you outsource (buy-in) your technical support this policy must be brought to their attention and signed as if they are a member of 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 e-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 e-safety officer and Headteacher.
    - Passwords are applied correctly to all users regardless of age.

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 Headteacher.
- Any e-safety incident is reported to the e-safety Officer (and an e-safety Incident report is made), or in his/her 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.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Students

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.

E-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.

Parents and Carers

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

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded.

Technology

St Ives Primary & Nursery School uses a range of devices including PC's, laptops, 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 Netsweeper software 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 ICT Coordinator, e-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 Headteacher.

Email Filtering – we use Netsweeper software 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 (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – No data is to leave the school on an un-encrypted USB drive; all such devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of such a device) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office. *(Note: Encryption does not mean password protected.)*

Passwords – all staff and students will be unable to access a PC or laptop without a unique username and password. Staff and student passwords will change every 180 days or where there has been a compromise, whichever is sooner. The ICT 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 at least weekly 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. All USB peripherals such as USB drives 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 E-safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

All staff, students and parents of students are informed that Internet activity may be monitored in order to ensure as much as possible that users are not exposed to illegal or inappropriate websites, and to ensure as much as possible that users do not actively seek access to illegal or inappropriate websites.

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 is not permitted.

Photos and videos – Digital media such as photos and videos are covered in the schools' Admissions Form, and is re-iterated here for clarity. All parents must sign the relevant section of the Admissions Form if they agree for their child to be present in photographs/videos that are published on the school website or other digital media. If a parent has not agreed this, then that child's photograph/video must not appear on such media.

Social Networking – there are many social networking services available; St Ives Primary & Nursery School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within St Ives Primary & Nursery School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Twitter – used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school Admissions Form) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools 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 e-safety incident is to be brought to the immediate attention of the e-safety Officer, or in his/her absence the Headteacher. The e-safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

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, St Ives Primary & Nursery School subscribe to the National Online Safety programme which provides annual e-learning for members of staff, governors and parents.

e-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. St Ives Primary & Nursery School subscribe to the National Online Safety programme of study and will teach important e-safety messages through these resources.

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 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.

E-safety Group

The E-safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring of the E-safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.
Members of the E-safety Group will assist the E-safety Officer with:

- the production / review / monitoring of the school E-safety Policy / documents.
- the production / review / monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.
- mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

PREVENT – A Community Safeguarding Programme

Prevent is about safeguarding people and communities from the threat of terrorism. Prevent is 1 of the 4 elements of CONTEST, the Government's counter-terrorism strategy. It aims to stop people becoming terrorists or supporting terrorism. At the heart of Prevent is safeguarding children and adults and providing early intervention to protect and divert people away from being drawn into terrorist activity.

If you see or hear something that could be terrorist related, call the Police Hotline on 0800 789 321.

If you are concerned about someone in your community, please contact the local police force by dialing 101 or if you require urgent police assistance, dial 999.

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the e-safety Policy. Once you have read and understood both you must sign this policy sheet *(it may be easier and tidier to have a separate single sheet that all staff sign).*

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 e-safety incident, reported to the e-safety officer and an incident sheet completed. Users are reminded that Internet activity may be monitored.

Social networking – is allowed in school in accordance with the e-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 – If it is necessary for you to take work home, or off site, you should ensure that your device (USB drive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted USB drive.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

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 Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the e-safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to the Drift IT 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.

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

NAME :

SIGNATURE : **DATE :**

Acceptable Use Policy – Students

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

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

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

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 – let my teacher know if anybody asks me for personal information.

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

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

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 – that Internet activity may be monitored.

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

Signed (Student) :

Date :

Letter to Parents:

Dear Parent/Guardian

Use of the Internet in school is a vital part of the education of your son/daughter. Our school makes extensive use of the Internet in order to enhance their learning and provide facilities for research, collaboration and communication.

You will be aware that the Internet is host to a great many illegal and inappropriate websites, and as such we will ensure as far as possible that your child is unable to access sites such as this. We are able to do this using advanced software known as an Internet filter. This filter categorizes websites in accordance with their content; the school allows or denies these categories dependent upon the age of the children.

The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school; in order to ensure that there have been no attempts of inappropriate Internet activity we may occasionally monitor these logs. If we believe there has been questionable activity involving your child we will inform you of the circumstances.

At the beginning of each school year we explain the importance of Internet filtering to your child. Furthermore, we explain that there has to be a balance of privacy and safety; we also inform them that we can monitor their activity. All children are given the opportunity to ask questions and give their viewpoint. We would like to extend that opportunity to you also; if you have any questions or concerns please come and see us.

Yours sincerely

Mrs L Crossley
Headteacher

I have read this letter and understand that my child’s Internet access could be monitored to ensure that there is no illegal or inappropriate activity by any user of the school network. I acknowledge that this has been explained to my child and that he/she has had the opportunity to voice their opinion, and to ask questions.

Name of Parent/Guardian –

Name of Child –

Signature - Date

E-safety Incident Reporting Log

St. Ives Primary & Nursery School

Date	*Time*	*Incident*	*Action Taken*		*Incident Reported By*	*Signature*
			What?	*By Whom?*		

Risk Log

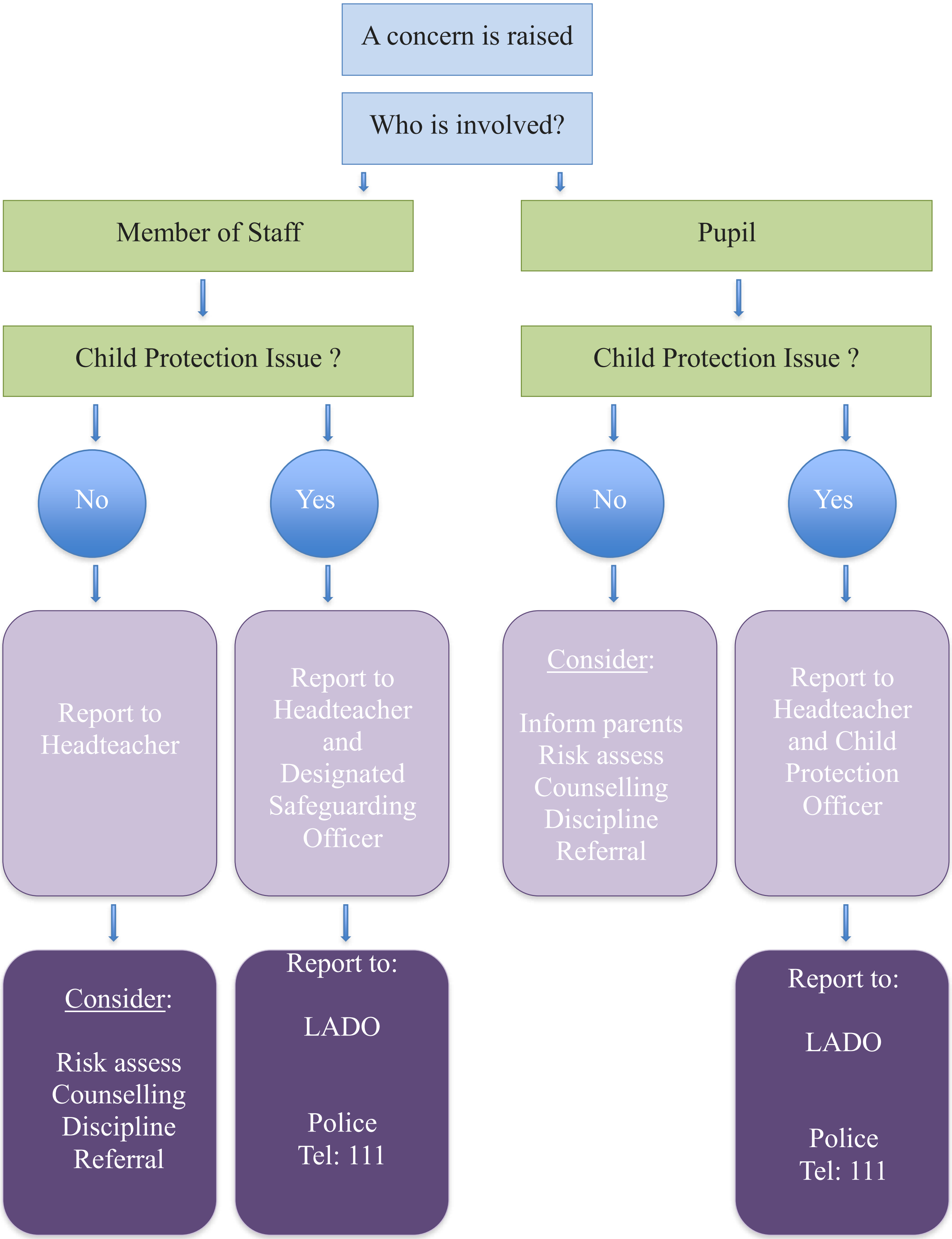
No.	Activity	Risk	Likelihood	Impact	Score	Mitigation	Owner
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	3	**3**	E-safety education of staff, E-safety policy.	E-safety Officer
2.	Internet browsing	Access to inappropriate/illegal content - students	3	3	**9**	E-safety education of students, internet filtering in place.	E-safety Officer
3.	Twitter	Inappropriate comments	2	1	**2**	E-safety education of staff, E-safety policy.	E-safety Officer
4.	Twitter	Using copyright material	1	2	**3**	Education of staff.	E-safety Officer
5.	Twitter	Publishing photographs of students without permission	1	3	**3**	Education of staff, list of pupils without permission.	E-safety Officer
6.	Student laptops	Students taking laptops home – access to inappropriate/illegal content at home	1	3	**3**	E-safety education of students/parents, Acceptable Use Policy agreement with students.	E-safety Officer
7.	Student iPads	Students taking iPads home – access to inappropriate/illegal content at home	1	3	**3**	E-safety education of students/parents, Acceptable Use Policy agreement with students.	E-safety Officer
8.	System Access	Unauthorised individuals access the restricted drives	1	3	**3**	E-safety (password) education of staff, E-safety policy.	E-safety Officer
9.	System Failure	Staff/students are unable to access the system	2	3	**6**	Drift IT Support.	E-safety Officer, Drift
10.	Server Failure	Data/documents are corrupted/lost due to server failure	1	3	**3**	Server back up, Drift IT Support.	E-safety Officer, Drift

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 recommend the mitigation to Headteacher and Governing Body.Final decision rests with Headteacher and Governing Body**

Inappropriate Activity Flowchart



A concern is raised

Who is involved?

Member of Staff

Child Protection Issue ?

No

Report to Headteacher

Consider:

Risk assess
Counselling
Discipline
Referral

Yes

Report to Headteacher and Designated Safeguarding Officer

Report to:

LADO

Police
Tel: 111

Pupil

Child Protection Issue ?

No

Consider:

Inform parents
Risk assess
Counselling
Discipline
Referral

Yes

Report to Headteacher and Child Protection Officer

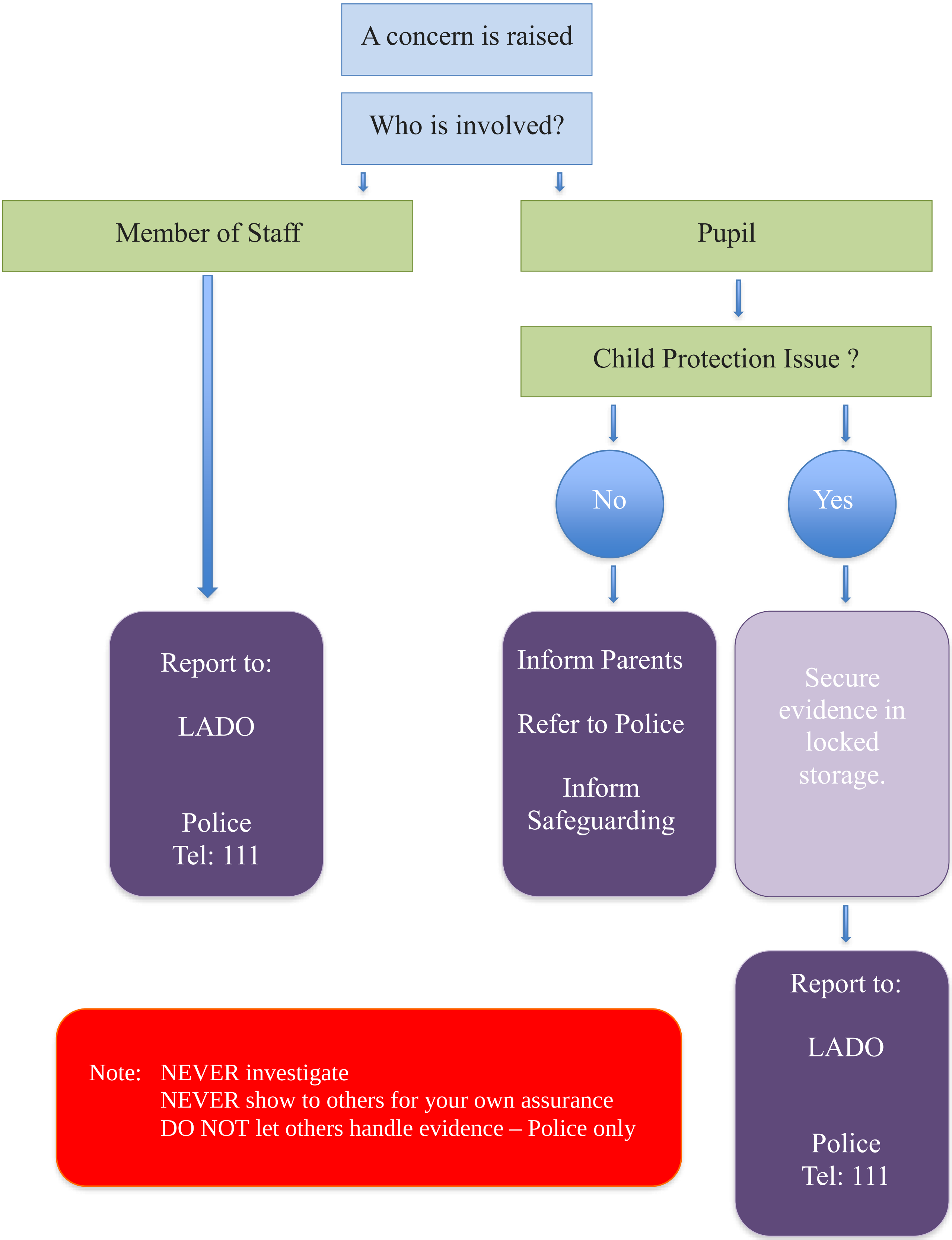
Report to:

LADO

Police
Tel: 111

If you are in any doubt, consult the Headteacher, 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:

LADO

Police
Tel: 111

Inform Parents

Refer to Police

Inform
Safeguarding

Secure evidence in locked storage.

Report to:

LADO

Police
Tel: 111

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