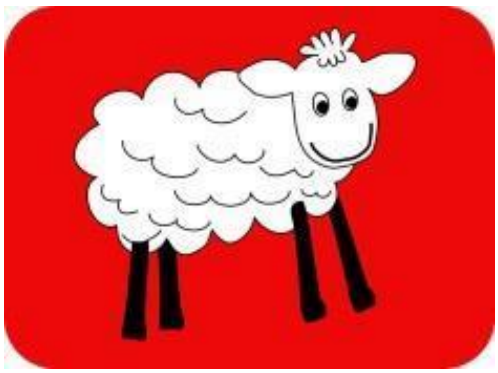


Sheepy Magna Church of England Primary School

E-Safety Policy

Headteacher: Alison Field

_____

~~Safeguarding~~ Governor: ~~Bob Amour~~

_____

Last Reviewed – June~~May~~ 2025~~3~~

Next Review Date – June~~May~~ 2026~~5~~



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, volunteers, church community.

Safeguarding is a serious matter; at Sheepy Magna CE Primary 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 Sheepy 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.



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 Head Teacher in regards to training, identified risks and any incidents.
  - Be a member of the Health, Safety and Wellbeing~~Safety~~ Committee

~~Currently this governor is: Bob Armour~~[1]

Head Teacher

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 recipient, i.e. pupils, all staff, senior leadership team, governing body and 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 Gavin King and Gemma Rose~~Stephanie Mitchell~~.[2]

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 themselves~~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.

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 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. Passwords for staff will be a minimum of 8 characters. The IT System Administrator password is to be changed on a half termly 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 Headteacher.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Pupils
The boundaries of use of ICT equipment and services in this school are given in the Pupil 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; pupils will be given the appropriate advice and guidance by staff. This includes online safety and peer on peer abuse. Similarly all pupils 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 and school newsletters 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. [3]

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

Technology
Sheepy School uses a range of devices including PC's, laptops, iPads and cameras. 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 RM SafetyNet 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 Office 365 for Education software that helps to prevent 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 – All school devices that hold personal data (as defined by the Data Protection Act [4]2018) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB key drives) 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.

Passwords – all staff and pupils will be unable to access devices such as staff IPads and PCs without a unique username and password. CESG/GCHQ guidance advises against regularly changing passwords and instead advises that passwords should only be changed if a compromise is suspected and indicted. 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 keydrives (if you allow them) 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; pupils upon their parents signing and returning their acceptance of the Acceptable Use 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 is not permitted. Pupils are permitted to use the school email system when it is deemed necessary for aspects of the curriculum. At such a point they are given their own email address.

Photos and videos – Digital media such as photos and videos are covered in the schools' Acceptable Use Policy and Staff Behaviour Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year, issued by the office; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; Sheepy 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 Sheepy 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.

- Blogging – used by staff and students in school.
- Twitter – used by the school as a broadcast service (see below).
- Facebook – 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 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 license 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 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, Sheepy School will have an annual programme of training which is suitable to the audience.

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. At Sheepy, we teach E-Safety on an annual basis with an E-Safety day. In conjunction with this, pupils and parents are reminded and updated termly. Pupils are taught about E-Safety during their IT lessons. The e-safety curriculum covers the 4 C's (content, contact, conduct, commerce).

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. 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.

Acceptable Use Staff and Volunteers

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be safe and responsible users of the internet and other digital technologies.
- that school ICT systems and users are protected from accidental or deliberate misuse.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work and improve opportunities for learners and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to minimise the risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of its ICT systems including email and other digital communications technologies.
- I understand that this agreement also apply to use of school ICT systems out of school (eg laptops, email, VLE etc).
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will keep my usernames and passwords private and will not try to use anyone else's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, to the appropriate person in school.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, delete or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner.
- I will ensure that when I take or publish images of pupils or parents/colleagues, I will do so with their permission and in accordance with the school's policy. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify pupils by name, or other personal information.
- I will not use chat and social networking sites in school.

- I will only communicate with pupils and parents / carers using official school systems and in a professional manner. I will not share any personal information with a pupil (including personal phone numbers or email address). Nor will I request or respond to any personal information from a young person unless it is appropriate as part of my professional role.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies:
When I use my personal hand held / external devices in school (PDAs / laptops / mobile phones / USB devices etc), I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that when connecting these devices to school ICT systems, they are protected by up to date anti-virus software and are free from viruses.
I will not use personal email addresses on the school ICT systems.
I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
I will ensure that my data is regularly backed up, in accordance with relevant school policies.
I will not try to upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others (eg child sexual abuse images, criminally racist material, adult pornography etc). I will not try to use any programmes or software that might allow me to bypass the filtering / security systems intended to prevent access to such materials.
Unless I have permission, I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
I will not install or attempt to install programmes of any type on school systems, nor will I try to alter computer settings, unless this has been authorised by ICT Technical Support Staff.
I will not disable or cause any damage to school equipment, or the equipment belonging to others.
I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where personal data is electronically transferred outside the secure school network, it must be encrypted.
I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems both in and out of school and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Signed …….. Print name…….

Acceptable Use Pupils

Rationale

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users as far as their age and understanding will allow for.

Pupil Acceptable Use Agreement for EYFS/KS1

This is how I stay safe when I use computers:

I will ask a teacher if I want to use the computers.

I will only use activities that a teacher has told or allowed me to use.

I will take care of the computer and other equipment.

I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Parent / Carer Signature

As the parent / carer of the above pupil, I understand that the school has discussed the Acceptable Use Agreement with my son / daughter as part of whole school commitment to e-Safety both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet.
I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-Safety.

Name of Pupil

Signed (parent)

Date

Pupil Acceptable Use of ICT Agreement for KS2

<u>These are the rules I agree to follow when using any digital technology:</u>

- I will ask permission from a teacher before using ICT equipment and will use only my own login and password.
- To protect myself and other pupils, if I see anything I am unhappy with or receive messages I do not like, I will immediately close the page and tell a teacher or adult.
- I will not access other people's files or send pictures of anyone without their permission.
- I will not bring CDs or memory sticks into school unless I have permission and they have been checked to ensure that they are virus free.
- I will only e-mail people I know, or that my parent/teacher has approved and the messages I send will be polite and sensible. I will not give my home address or phone number, or arrange to meet someone I have met online.
- When I am using the internet to find information, I will check that the information is accurate as I understand that the work of others may not be truthful.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- I will not use my mobile phone in school for any reason.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- If I am involved in incidents of inappropriate behaviour that involve members of the school community (e.g. cyber-bullying, using images/information without permission), the school will take action according the Behaviour Policy.
- I understand that if I do not follow these rules I may not be allowed to use ICT in school and my parents/carers may be contacted.

I have read and understood these rules and agree to follow them:

Name of Pupil Date

Parent / Carer Countersignature

As the parent / carer of the pupil I know that my child has signed this Acceptable Use Agreement and has received, or will receive, e-Safety education to help them understand the importance of safe use of digital technology– both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the Internet and digital technologies at home and will inform the school if I have concerns over my child's e-Safety.

Name of Parent/Carer Signed

Date



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:**
Signature (Governor)		**Date:**

Risk Log

No.	Activity	Risk	Likelihood	Impact	Score	Owner

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



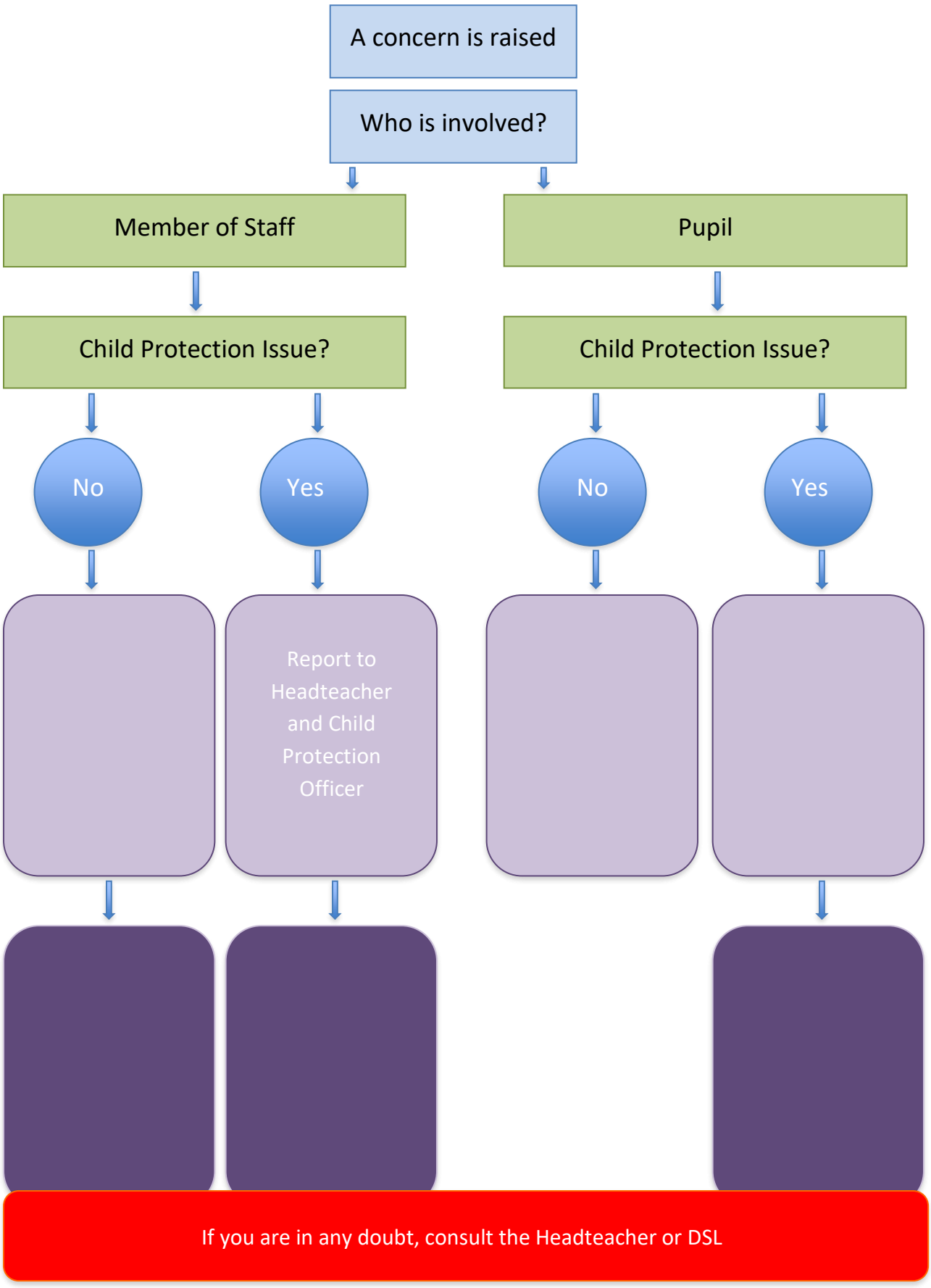
Risk Assessment

Risk No.	Risk
LIkelihood	
Impact	
Risk Assessment	
Risk Owner/s	
Mitigation	

Approved / Not Approved (circle as appropriate) **Date:**

Signed (Headteacher) : **Signed (Governor) :**

Inappropriate Activity Flowchart



Illegal Activity Flowchart

