Moat Farm Infant School

Lavender Farm Nursery

eSafety Policy

To be used in conjunction with:

Social Media Policy
Email Acceptable Use Policy
Internet Acceptable Use Policy
Password Security Policy
Mobile Phone and Camera Policy
Internet Filtering Policy

Author	Alan Care
Updated	July 2016
Review Date	July 2017
Governor approval	September 2016

The purpose of the e-safety policy.

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to e-safety. The policy relates to other policies including ICT/Computing curriculum, Internet Access, Bullying, Child Protection and Health and Safety.
This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both on and off the school site.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Background and Rationale

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child’s education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual’s consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator / Officer
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator / Officer.
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator / Officer.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

E-Safety Coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority

- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, (Examples of suitable log sheets are attached)
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / Governors meetings where appropriate
- reports regularly to Senior Leadership Team

Network Manager / ICT Technical staff (including contracted staff from outside school)

The Network Manager / ICT Technical Staff is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- To aid the E-Safety Co-ordinator in the monitoring and development of school ICT/Computing policy.
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Internet Provider is informed of issues relating to the filtering applied by the provider
- the school's filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Filtering Policy Template" for good practice document)
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Officer /Head teacher / Senior Leader / Head of ICT / ICT Co-ordinator / Class teacher / for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Coordinator / Head teacher / Senior Leader / Head of ICT / ICT Co-ordinator / Class teacher / for investigation / action / sanction
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities

- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated person for child protection / Child Protection Officer should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

It is important to emphasise that these are child protection issues, not technical issues. Technology provides additional means for child protection issues to develop.

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Pupils should know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for accessing the school website / VLE / in accordance with the relevant school Acceptable Use Policy

Teaching and learning

Why Internet use is important

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

Internet use will enhance learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
Pupils will be educated in the effective use of the Internet in research, in an age appropriate way including the skills of knowledge location, retrieval and evaluation

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly.
From September 2016 Trustnet will be the schools Internet Service Provider and Email Provider.

- Security:
    - Fully managed Firewalls
    - Sophus antivirus
    - Webscreen 2.0 Web Filtering
    - Mailprotect – Email Filtering
    - Email and Internet activity actively monitored and reported

School Website

The school website will comply with all DfE, Ofsted and Local Authority guidelines for content.

Publishing pupil's images and work

Only photographs/work that have parental permission to include their pupils will be used.
Pupils' full names will not be used anywhere on the website.

Managing emerging technologies

Emerging technologies will be examined for educational benefit by SLT before use in school is allowed.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Should unsuitable material appear on a school computer the school will manage and investigate on a case by case basis.

Handling e-safety complaints

The Headteacher will deal with complaints of Internet misuse.
Any complaint about staff misuse must be referred to the Headteacher.
Complaints of a child protection nature must be dealt with in accordance with school Child Protection Procedures.

Community use of the Internet

All use of the school internet connection by community and other organisations shall be in accordance with the e-safety policy.

Introducing the e-safety policy to pupils

E-safety rules will be discussed with the pupils at the start of each year.
E-safety posters will be posted next to all computers within classrooms and in a prominent place in the ICT suite, so that all users can see them.
Pupils will be informed that network and Internet use is monitored and appropriately followed up.
Pupils will receive e-safety lessons and will be constantly reminded of online safety.

Staff and the e-Safety policy

All staff will have access to the School e-Safety Policy and its importance explained.
Staff should be aware that Internet traffic will be monitored.
Discretion and professional conduct is essential.
Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy through the School Website, newsletters, and parents' evenings.

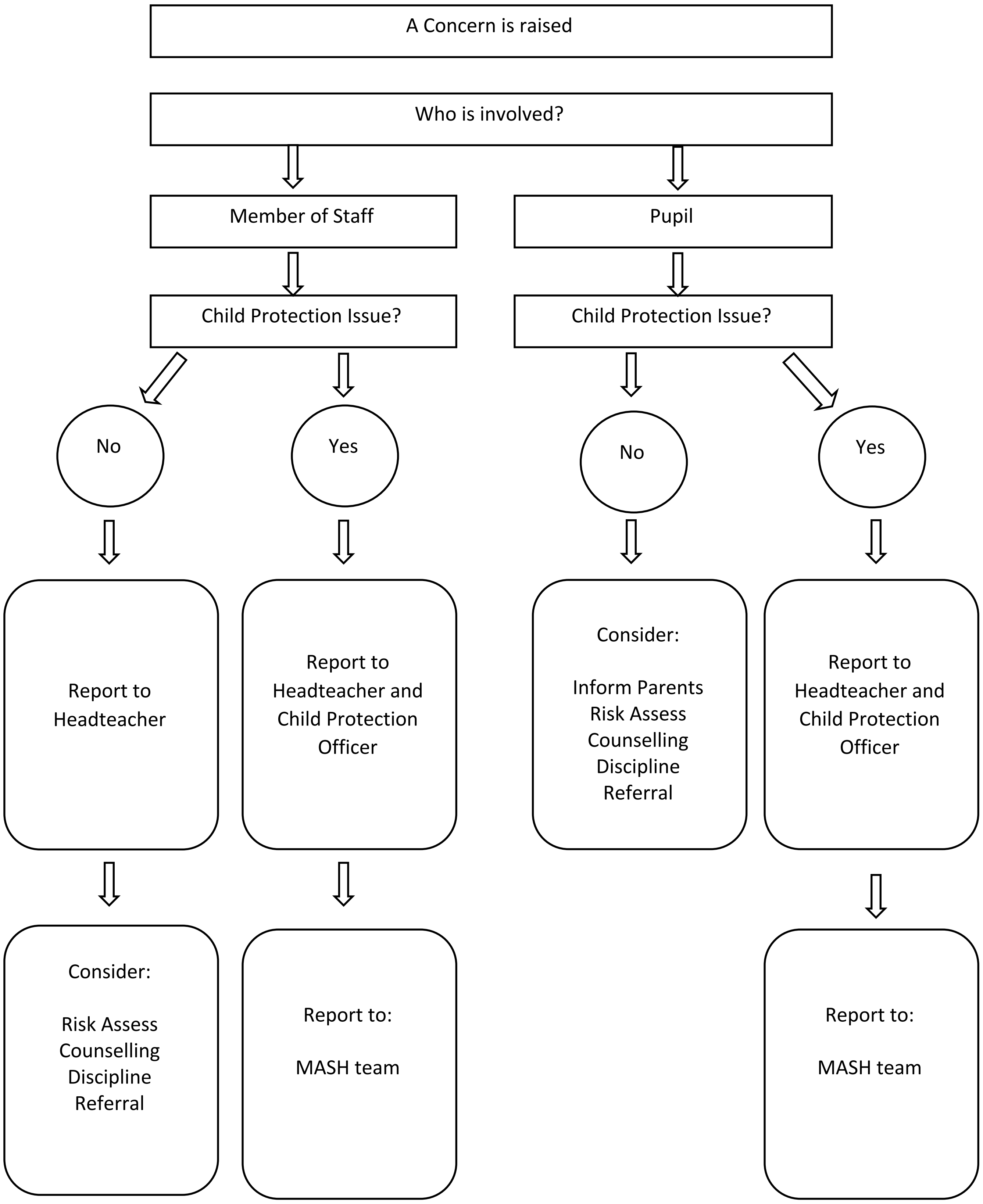
If using the internet at home:

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
Pupils must be made aware of how they can report abuse and who they should report abuse to.
Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.

eSafety Incident Log

<table>
<tr><td>Number:</td><td colspan="3">Reported By: (name of staff member)</td><td colspan="2">Reported To: (e.g. Head, e-Safety Officer)</td></tr>
<tr><td></td><td colspan="3">When:</td><td colspan="2">When:</td></tr>
<tr><td colspan="6">Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)</td></tr>
<tr><td colspan="2">Review Date:</td><td colspan="4"></td></tr>
<tr><td colspan="6">Result of Review:</td></tr>
<tr><td colspan="2">Signature (Headteacher)</td><td></td><td colspan="2">Date:</td><td></td></tr>
<tr><td colspan="2">Signature (Governor)</td><td></td><td colspan="2">Date:</td><td></td></tr>
</table>

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 Child Protection Officer

Report to:

MASH team

Pupil

Child Protection Issue?

No

Consider:

Inform Parents
Risk Assess
Counselling
Discipline
Referral

Yes

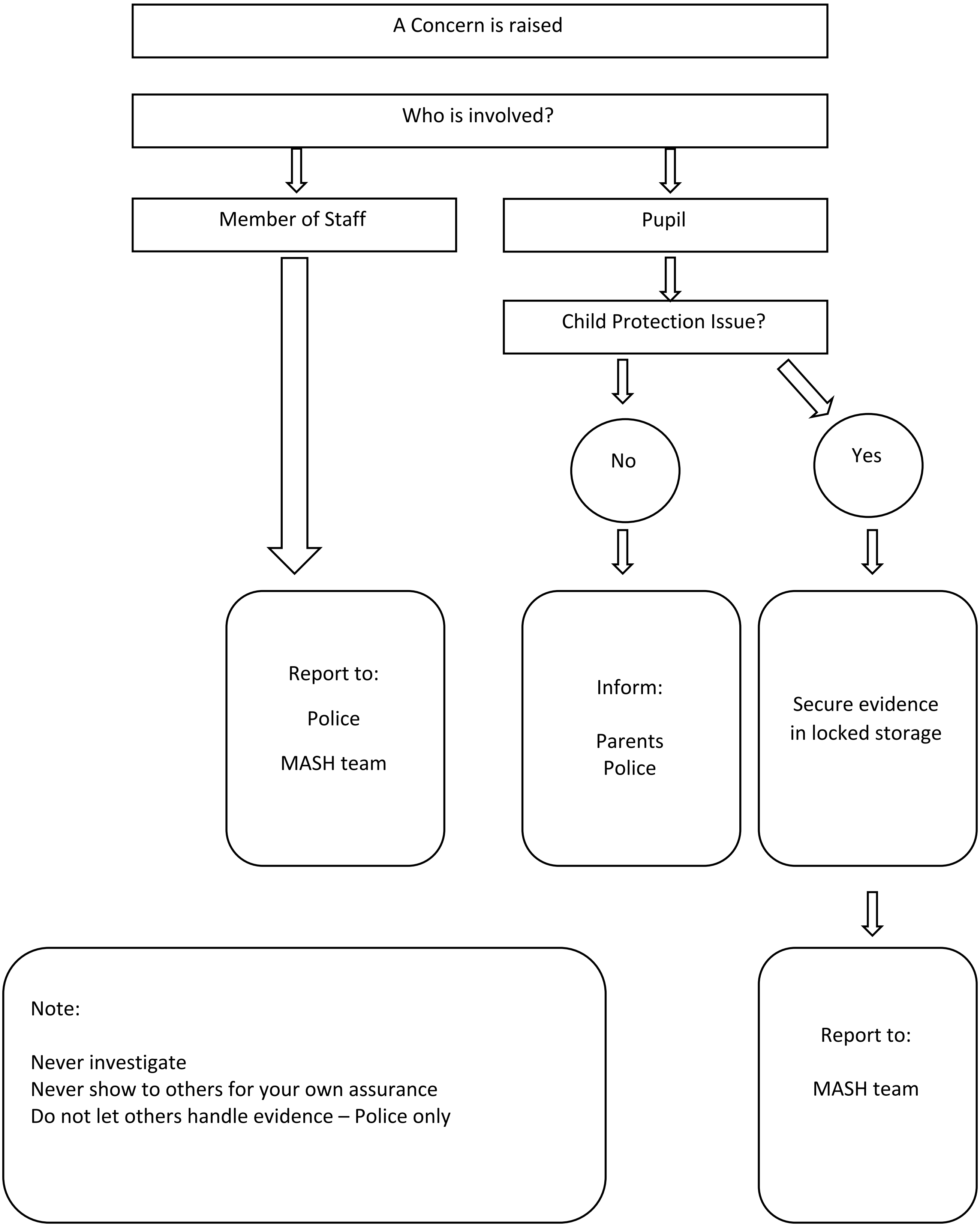
Report to Headteacher and Child Protection Officer

Report to:

MASH team

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:

Police

MASH team

Inform:

Parents
Police

Secure evidence
in locked storage

Report to:

MASH team

Note:

Never investigate
Never show to others for your own assurance
Do not let others handle evidence – Police only

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