Mickle Trafford Village School

E-Safety Policy

Date of policy	Spring 2022
Date for Review	Spring 2023
Signed Headteacher	
Signed Chair of Governors	

School E-Safety Policy

New technologies have become integral to the lives of children in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times. The requirement to ensure that children 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. Our E-Safety policy should help to ensure safe and appropriate use. 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, remote learning, 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.

Mickle Trafford Village 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.

Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- DfE (2021) 'Keeping Children Safe in Education'
- Data Protection Act 2018
- DfE (2020) 'Keeping children safe in education'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'

Role and Responsibilities

The **governing board** is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an **annual** basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training (including online safety) at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.

The **headteacher** is responsible for:

- Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.

- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the **DSL and governing board** to update this policy on an **annual** basis.

The **E-Safety Co-ordinator** is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.

- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the **governing board** about online safety
- Working with the **headteacher and governing board** to update this policy on an **annual** basis.

ICT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the **headteacher**.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

- Adhering to this policy, the **Acceptable Use Agreement** and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

Writing and reviewing the E-Safety policy

The school have an E-Safety Coordinator

The E-Safety policy and its implementation will be reviewed annually

Teaching and learning

Online safety is embedded in the whole curriculum; however, it is particularly addressed in the following subjects:

- Computing (Mr Andrews Online)
- PSHCE
- JigSaw Well-being
- Health Education

Why the use of the Internet is important

- The Internet is an essential part 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 embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Pupils use the internet widely outside school and need to learn how to evaluate Internet information ad take care of their own safety.

How Internet use will enhance learning

- Developing effective practice in Internet use for teaching and learning is essential as the quantity of information is often overwhelming.
- Pupils will be educated in the effective use if the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- 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.

- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.

Pupils will be taught how to evaluate Internet content

It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts to filter. To protect the pupils the following safeguards are in place:

- The school will work with the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Coordinator.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are taught what to do if they experience material that they find distasteful, uncomfortable or threatening. In such circumstances they close the page and report the incident immediately to the teacher
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Coordinator.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- All curriculum laptops and I-pads are securely centrally stored.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Mobile phones will not be used during school time and staff will store their mobiles in their cupboards.

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. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Publishing content including pupil’s images and work

The school website is an excellent medium for communicating with families both current and prospective as it can celebrate pupil’s work, promote the school and publish resources for projects. However publication of information should be considered from a personal and school security viewpoint as a school, we publish images in the more secure area of our site which is only accessible by password

- The contact details on the website should be the school address, email and telephone number. Staff or pupils’ personal information will not be published
- Photographs that include pupils will be selected carefully.
- Pupils’ full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil’s work can only be published on the school website unless the parent/carer has refused permission of the pupil and parents.
- Pupil’s work can only be published on the school’s Tapestry with the permission of parent/carers.

Social networking and personal publishing

- The schools firewall will block or filter access to social networking sites and pupils will be advised not to use these at home.
- Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged children.
- Pupils will be advised never to give out personal details or to place photos of any kind which may identify them and/or their location.

- Pupils should be advised not to publish specific and detailed private thoughts.
- School is aware that bullying can take place through social networking.
- Staff are advised that they should consider the consequences and possible repercussions of any information that they make available online, for example, networking sites. Particular care should be taken in the posting of photographs, videos and information related to the school, staff and pupils which may result in bringing the school into disrepute.

Responding to Specific online Safety Concern

Cyber-bullying

All staff are made aware that cyber-bullying can take place outside the classroom and can have an effect on children within the school setting. If staff become aware of this they must report it to the designated lead who will discuss the matter with parents and monitor actions taken to prevent this happening again.

Parents are encouraged to actively seek advice and guidance from school if they have any concerns relating to cyber-bullying. Parents will be encouraged to record and evidence any instances which cause concern.

Upskirting

Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.

A "specified purpose" is namely:

- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear).
- To humiliate, distress or alarm the victim.
- "Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.
- Upskirting is not tolerated by the school.

Incidents of upskirting are reported to the **DSL** who will then decide on the next steps to take, which may include police involvement, in line with the **Child Protection and Safeguarding Policy**.

Youth produced sexual imagery (sexting)

Youth produced sexual imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 18 is illegal.

All concerns regarding sexting are reported to the **DSL**.

Following a report of sexting, the following process is followed:

- The DSL holds an initial review meeting with appropriate school staff
- Subsequent interviews are held with the pupils involved, if appropriate
- Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the pupil at risk of harm
- At any point in the process if there is a concern a pupil has been harmed or is at risk of harm, a referral will be made to children's social care services and/or the police immediately
- The interviews with staff, pupils and their parents are used to inform the action to be taken and the support to be implemented
- When investigating a report, staff members do not view the youth produced sexual imagery unless there is a good and clear reason to do so.
- If a staff member believes there is a good reason to view youth produced sexual imagery as part of an investigation, they discuss this with the headteacher first.
- The decision to view imagery is based on the professional judgement of the DSL and always complies with the **Child Protection and Safeguarding Policy**.
- Any accidental or intentional viewing of youth produced sexual imagery that is undertaken as part of an investigation is recorded.
- If it is necessary to view the imagery, it will not be copied, printed or shared.

Online abuse and exploitation

Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.

The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.

All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the **DSL** and dealt with in line with the **Child Protection and Safeguarding Policy**.

Online hate

The school does not tolerate online hate content directed towards or posted by members of the school community.

Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved, e.g. **Staff Code of Conduct and Anti-Bullying Policy**.

Online radicalisation and extremism

The school's filtering system protects pupils and staff from viewing extremist content.

Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the **Child Protection and Safeguarding Policy** and **Prevent Duty Policy**.

The school website

The **headteacher** is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information relating to staff and pupils is not published on the website.

How will mobile phones be used?

If a child must bring their mobile phone to school, it must be switched off and handed to the class teacher or the office until the end of the day and left at the owners own risk.

Parents and visitors are reminded not to us their mobile phones to take photos or videos of other people's children during school trips and events.

How will interactive watches be used?

Many watches now have the facility to track exercise and count steps throughout the day. These watches are permitted in school unless they have a facility to take photographs. For safeguarding reasons, children cannot wear watches which allow them to film or photograph other children at school.

Handling E-Safety complaints

Prompt action will be required if a complaint is made regarding any member of our community and the facts of the case will be established

- A minor transgression of the rules may be dealt with be the teacher
- 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

Introducing the E-Safety policy to pupils

- E-Safety rules will be discussed with the pupils at the start of each year.
- Children will be reminded of these rules regularly to raise awareness and the importance of safe and responsible internet use.
- E-Safety posters will be agreed with the children and displayed in all classrooms, so that all users can see them.
- When first logging into PCs or Laptops, children will be taught about e-safety.
- Pupils are informed that network and Internet use is monitored and appropriately followed up.
- Pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- The children receive E-Safety lessons and are constantly reminded of online safety.
- Pupils are taught to be critically aware of the content they access online, including recognition of bias and extreme or commercial content. They are guided to validate the accuracy and reliability of information.
- The online E-Safety coordinator maintains and passes on knowledge of current concerns to be included within learning experiences.
- Y5 E-Safety officers present regular updates in assembly and implement a number of competitions throughout the year.
- Key Online Safety messages are reinforced through assemblies (lead by E-Safety Coordinator), Safer Internet Week (February), Cyber Bullying Day (June) anti-
- bullying week (November) and throughout all teaching.

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 could be monitored and traced to the individual user.
- 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 E-Safety and the school's policy through newsletters and the website
- Raising awareness through activities planned by pupils
- E-Safety parent information evenings will be held every 2 years run by our staff and community police officer
- Providing and maintaining links to up to date information on the school website
- Parents are sent a copy of the **Acceptable Use Agreement** at the beginning of each year, and are encouraged to go through this with their child to ensure that their child understands the documents and the implications of not following it.

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.
- Pupils should only invite known friends and deny access to others

Remote learning

All remote learning is delivered in line with the school's **Pupil Remote Learning Policy**.

All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are only carried out where necessary.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

All staff and pupils using audio communication must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the **SLT**, in collaboration with the **SENCO**.

Pupils not using devices or software as intended will be disciplined in line with the **Behavioural Policy**.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

The school will communicate to parents in writing about any precautionary measures that need to be put in place if their child is learning remotely using their own/familyowned equipment and technology, e.g. ensuring that their internet connection is secure.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.
- The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

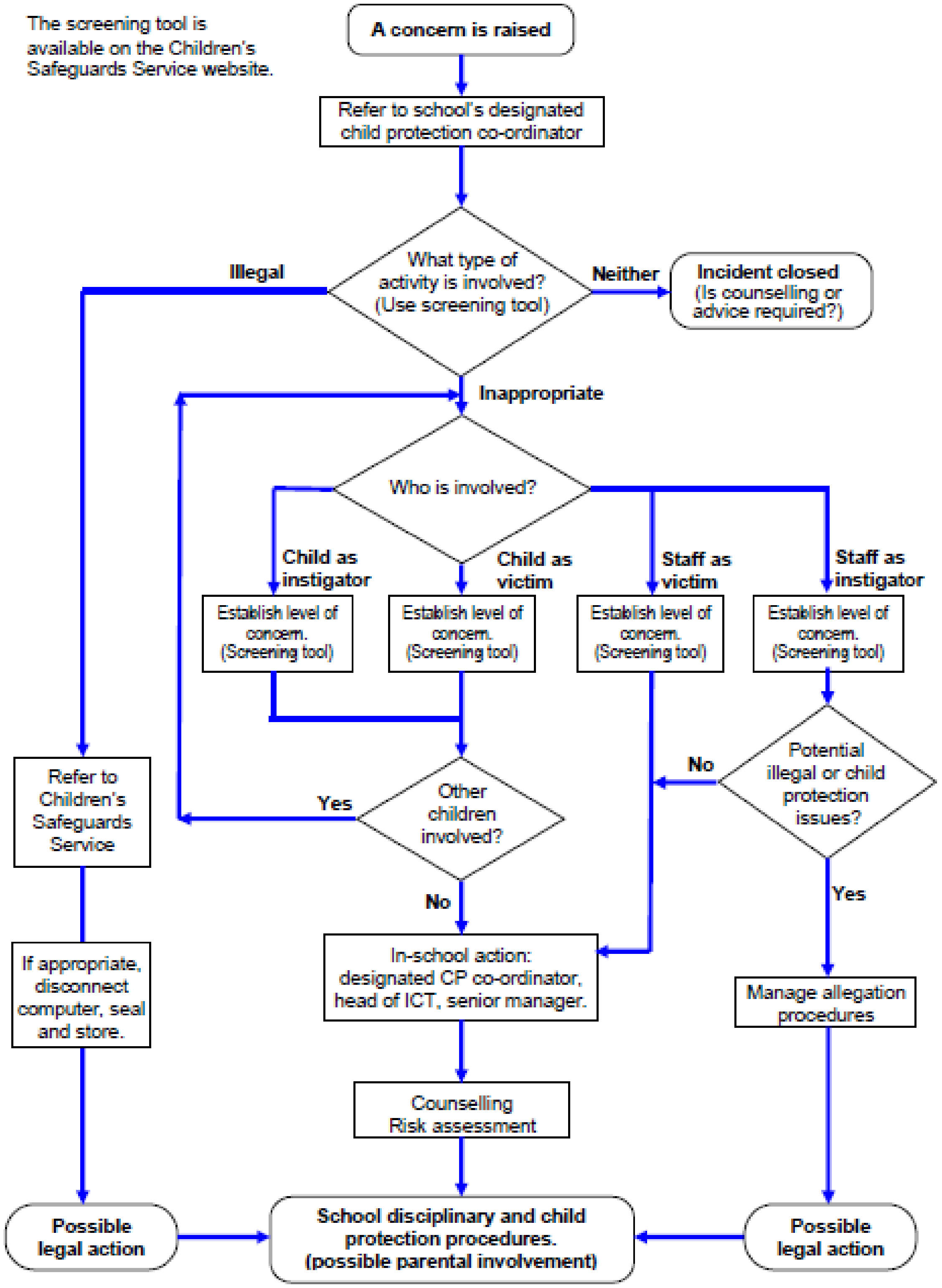
Reported by:	**Reported to:**
Date:	**Date:**
Incident description: (Describe what happened, involving which children and/or staff, and what action was taken)	
Review date:	
Result of review	

Signed **Headteacher**	**Date**
Signed **Governor**	**Date**

E-Safety Incident Log

Response to an Incident of Concern

The screening tool is available on the Children's Safeguards Service website.


A concern is raised
Refer to school's designated child protection co-ordinator
What type of activity is involved? (Use screening tool)
Illegal
Neither
Incident closed (Is counselling or advice required?)
Inappropriate
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Refer to Children's Safeguards Service
Yes
Other children involved?
No
No
Potential illegal or child protection issues?
Yes
If appropriate, disconnect computer, seal and store.
In-school action: designated CP co-ordinator, head of ICT, senior manager.
Manage allegation procedures
Counselling
Risk assessment
Possible legal action
School disciplinary and child protection procedures. (possible parental involvement)
Possible legal action