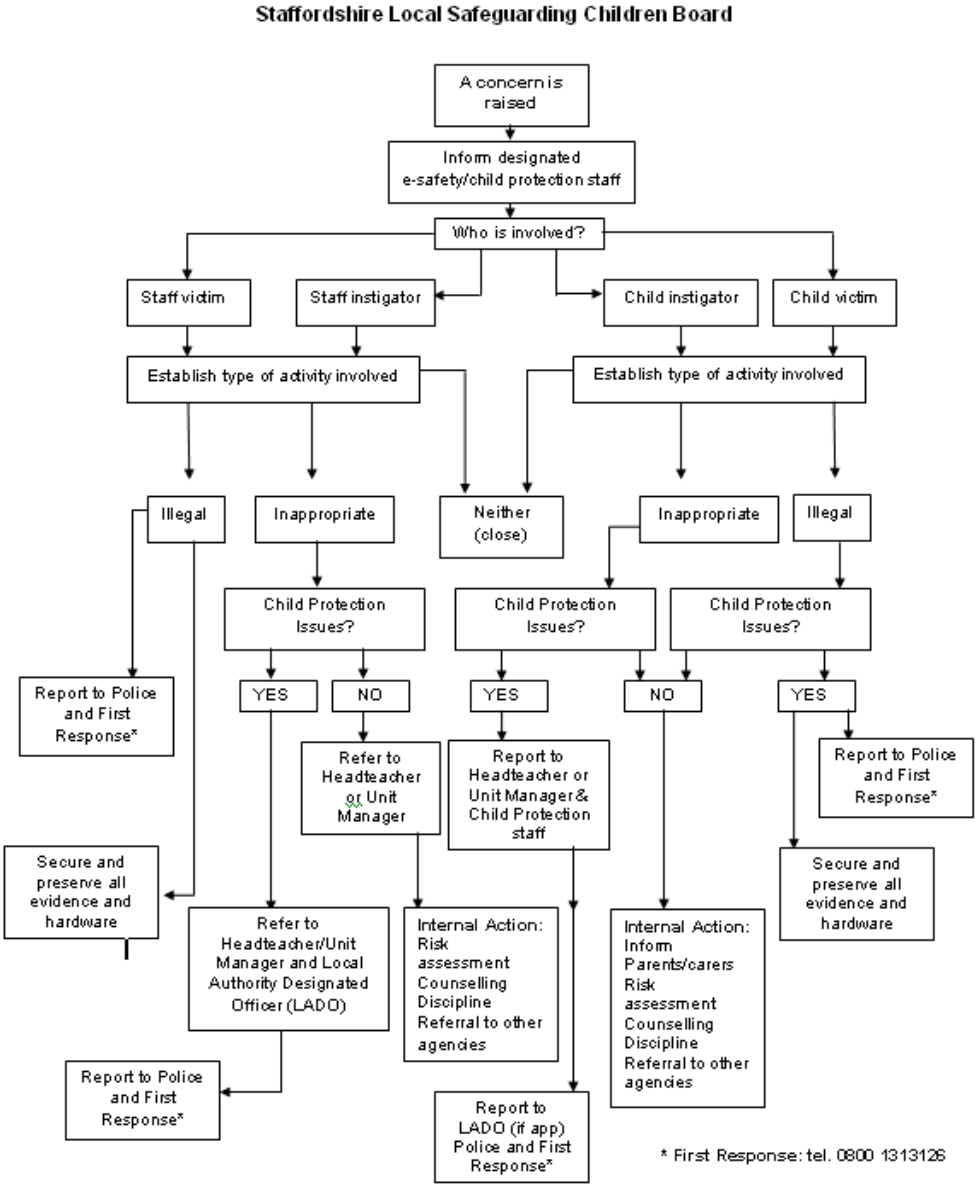
Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

The flow chart from the Staffordshire Safeguarding Children's board– below and http://www.staffsscb.org.uk/e-SafetyToolkit/IncidentResponse/ should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event contact the Staffordshire Safeguarding Children's Board

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Head of Key Stage	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		P	P √	P					
Unauthorised use of non-educational sites during lessons			√						
Unauthorised use of mobile phone / digital camera / other handheld device			√						
Unauthorised use of social networking / instant messaging / personal email			√						
Unauthorised downloading or uploading of files			√						
Allowing others to access school network by sharing username and passwords			√						
Attempting to access or accessing the school network, using another student's / pupil's account			√						
Attempting to access or accessing the school network, using the account of a member of staff			√						
Corrupting or destroying the data of other users			√						
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			√						
Continued infringements of the above, following previous warnings or sanctions			√						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			√						
Using proxy sites or other means to subvert the school's filtering system			√						
Accidentally accessing offensive or pornographic material and failing to report the incident			√						
Deliberately accessing or trying to access offensive or pornographic material			√						
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			√						

Staff Actions / Sanctions

Incidents:		Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		P√	P	P				√
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		√				√		
Unauthorised downloading or uploading of files		√				√		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		√				√		
Careless use of personal data eg holding or transferring data in an insecure manner		√				√		
Deliberate actions to breach data protection or network security rules		√				√		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		√				√		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		√				√		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		√				√		
Actions which could compromise the staff member's professional standing		√				√		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		√				√		
Using proxy sites or other means to subvert the school's filtering system		√				√		
Accidentally accessing offensive or pornographic material and failing to report the incident		√						
Deliberately accessing or trying to access offensive or pornographic material		√						√
Breaching copyright or licensing regulations		√				√		
Continued infringements of the above, following previous warnings or sanctions		√						√