MICKLEOVER PRIMARY SCHOOL

Name of Policy: E- Safety Policy

Date of Policy: June 2018

Member of Staff responsible: Erica Clennell

Review date: June 2019

Signature: _____ **Chair of Governors**

Date Approved: _____

At Mickleover Primary School

We are:

Motivated to learn

Proud of our achievements

Successful and skilled for life

E-Safety Policy

Our E-Safety Policy has been based on the e-Safety Policy developed and discussed at a Derby City ICT Network meeting. The e-Safety Policy relates to other policies including those for Information Communication Technology (ICT), bullying and child protection.

ROLES AND RESPONSIBILITIES

Governors

The role of the E-Safety Governor will include;

- Regular meetings with the E-safety officer
- Regular monitoring of E-Safety incident logs
- Reporting to relevant governors

Headteacher and Senior Leaders

- The Headteacher (E-Safety Officer) has a duty of care for ensuring the safety of members of the school community
- The SMT are aware of procedures to be followed in the event of a serious E-safety allegation being made against a member of staff.
- The Headteacher (E-safety officer) is responsible for ensuring that relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Officer.
- Receive reports of E-safety incidents and create a log of incidents to inform future E-safety developments
- Provide, as part of the induction process, all new staff (including those on university/college placement and work experience) with information and guidance on the e-safety policy and the school's acceptable use policies.

School Business Manager/Technical Staff

- Ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- Ensure that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- Liaise with school technical staff.
- That they keep 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/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher for investigation and action.

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of E-safety matters and of the current E-safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy.
- They are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems.
- They know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the E-safety and acceptable use policies

- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current 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
- When carrying out internet searches, the children will use Google safe search, swiggle.org.uk or yahoo for kids
- Staff and pupils must always keep their passwords private, must not share it with others, orleave it where others can find it.
- All staff have their own unique username and private password to access the school system. Staff are responsible for keeping their password private.

Child Protection/ Designated Safeguarding Officer

- should be trained in E-safety issues and be aware of the potential for serious child protection/safeguarding 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

Pupils

Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy. They:

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand 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

Some parents and carers have only a limited understanding of E-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Parents and carers will be encouraged to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Their children's personal devices in the school (where this is allowed)

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/VLE. The school will also seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters
- School notice boards
- The school website has direct links to Internet Service Providers' advice on how to set parental settings and to the Child Exploitation and Online Protection Centre (CEOP) website
- Parents/Carers evenings and events

TEACHING AND LEARNING

Why the Internet and digital communications are important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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. They will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-safety is therefore an essential part of the school's E-safety provision. Children and young people need the help and support of the school to recognise and avoid E-safety risks and build their resilience.

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

Pupils will be taught the importance of cross-checking information before accepting its accuracy.

Pupils will be taught how to report unpleasant Internet content e.g. blowing the whistle on the school's VLE, using the Child Exploitation and Online Protection (CEOP) Report Abuse icon or Hector Protector.

MANAGING INTERNET ACCESS

Maintaining information system security

Local Area Network (LAN) security issues include:

- Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. Misuse of the network will result in disciplinary actions being taken.
- Workstations are secured against user mistakes and deliberate actions.
- The Server is located securely and physical access restricted.
- The server operating system is secured and kept up to date.
- Virus protection for the whole network is installed and current, using Sophos anti-virus protection and automatic updates
- Wireless access to the school network is protected by a network key.

Wide Area Network (WAN) security issues include:

- All Internet connections are connected via the Learning Derby network to ensure adequate filtering and security protection are in place.
- Firewalls and switches are configured to prevent unauthorised access between schools.
- The security of the school information systems will be reviewed regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Personal data transported on Portable media must be encrypted or password protected.
- Portable media may not be used by pupils without specific permission followed by a virus check. (Staff using portable media are encouraged to virus check their media regularly.)
- Unapproved system utilities and executable files will not be allowed in pupils work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.

E-mail

The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff e-mail addresses take the form of initialsurname@mickleover.derby.sch.uk. Any digital communication between staff and pupils or parents/carers must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.
Pupils can send or receive emails through the Learning Platform. Pupil e-mail is a walled garden as default which means they cannot e-mail people beyond school. Wider access may be given for specific projects in school.
Pupils may only use approved e-mail accounts. Pupils must immediately tell a teacher if they receive any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
E-mail sent to external organisations should be written carefully as this is the same as sending a letter on school headed paper.
The forwarding of chain e-mail is not permitted.

Social networking and personal publishing

We are aware that bullying can take place through social networking.
The schools will block/filter access to social networking sites.
Newsgroups will be blocked unless a specific use is approved.
Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, Instant Messenger and e-mail addresses, full names of friends, specific interests and clubs etc.
Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
Pupils will be advised to use nicknames and avatars when using social networking sites.
Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
Blogs or wikis used for educational purposes will be delivered through the learning platform once it is introduced and permissioned to specific users or groups of users.
Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others. Pupils will be advised not to publish specific and detailed private thoughts.

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or Local Authority.
- They do not allow “friend” access to their personal social networking spaces to pupils, former pupils under 18 years old, or minors. They should ensure that communications with minors comply with their professional role. Abuse of this may result in disciplinary action being taken.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Cyberbullying

Cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online. The school recognises that both staff and pupils may experience cyberbullying and will commit to preventing any instances that should occur. We regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to that they post online. The school will commit to creating a learning and teaching environment which is free from harassment and bully. We have a zero tolerance policy for cyberbullying, and any incident will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.

Managing filtering

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-Safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by ICT Leaders who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every 30 days.
- Network administrator passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader.
- The head teacher is responsible for ensuring that software licence logs are up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installation.
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored.
- Requests for filtering changes must go through the head teacher.
- The school has provided differentiated user-level filtering (allowing different filtering levels for different groups of users).
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed procedure is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.

Asset Disposal

Details of school-owned hardware will be recorded in an Asset Register. All redundant equipment will be disposed of through Lead IT. This will include a certificate to ensure that all have been disposed of appropriately.
All redundant equipment that may have held personal data will have storage forensically wiped.

Publishing pupils’ images and work

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

- Staff and volunteers are allowed to take digital images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published
- Pupils' work can only be published with the permission of the pupil and parents or carers.
- Teachers should delete images from mobile devices regularly.

Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Managing emerging technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed with SLT permission .	Not allowed	Allowed	Allowed at certain times	Allowed with SLT permission	Not allowed
Mobile phones may be brought to school	✔ (*1)						✔ (*2)	
Mobile phones on desk (on silent/ vibrate)			✔					✔
Personal use of mobile phones in lessons.				✔				✔
Use of mobile phones in social time	✔							✔
Taking photos on mobile phones/ cameras			✔					✔
Use of school mobile devices eg tablets, gaming devices	✔					✔		

*1 Mobile phones should be out of sight and on silent

Staff should not use mobile phones for personal use unless in an emergency. Texting, emails and phone calls of a personal nature are not allowed during lesson times (except in emergency situations)

*2 Pupil's mobile phones to be left in the school office and collected at hometime

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Please refer to the schools Data Protection policy for details. Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using secure password protected devices.
- The data must be securely deleted from the device once it has been transferred or its use is complete

POLICY DECISIONS

Introducing the e-safety policy to pupils

E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
Pupils will be informed that network and internet use will be monitored and appropriately followed up. A programme of training in e-Safety will be developed, based on the school's Rising Stars Computing Scheme and using materials from CEOP.
E-Safety training will be embedded within the Personal Social and Health Education (PSHE) curriculum and reinforced regularly when children have access to the Internet in school.

Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained and discussed.
Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
ICT technician will be supervised by senior management and work to clear procedures for reporting issues.
Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

Parents and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Learning Platform.
The school will maintain a list of e-safety resources for parents/carers.
The school will ask all new parents to sign the consent form as part of the parent /pupil home/school agreement when they register their child with the school.
Internet issues will be handled sensitively, and parents will be advised accordingly.
A partnership approach with parents is encouraged. This will include parent evenings with demonstrations and suggestions for safe home Internet use.
Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents via parents meetings.

Authorising Internet access

All staff must read and sign the Staff Code of Conduct for ICT before using any school ICT resource. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
Parents will be asked to give consent as part of the home school agreement.

Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources before being allowed to access the internet from the school site.

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 computer connected to the school network. Neither the school nor DCC can accept liability for any material accessed, or any consequences of Internet access. The school will audit ICT use regularly to ensure the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

Should an E-Safety incident occur or a concern is raised the flowchart in Appendix 4 should be followed and the 'Reporting E-Safety Concerns Proforma' in Appendix 3 should be completed.

Other Incidents
It is expected that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy take place, through careless, irresponsible or deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated, encrypted computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated, SLT will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following internal response or discipline procedures.
- Involvement by Local Authority or other organisations if required.
- Police involvement and/or action if required.

If content being reviewed includes images of Child Abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- Incidents of 'grooming' behaviour
- The sending of obscene materials to a child
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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:

Pupils	Actions								
Incidents:	Refer to class teacher	Refer to Phase Leader	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)		✔	✔	✔					
Unauthorised use of non-educational sites during lessons	✔							✔	
Unauthorised use of mobile phone/digital camera/other mobile device			✔					✔	
Unauthorised use of social media/ messaging apps/personal email			✔		✔			✔	
Unauthorised downloading or uploading of files	✔		✔					✔	
Attempting to access or accessing the school network, using another 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 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			✔			✔			
Accidentally accessing offensive or pornographic material and failing to report the incident	✔		✔		✔	✔		✔	
Deliberately accessing or trying to access offensive or pornographic material			✔		✔			✔	✔

Staff	Actions							
Incidents:	Refer to line manager	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)		✔	✔	✔				
Inappropriate personal use of the internet/social media/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 message that is regarded as offensive, harassment or of a bullying nature	✔	✔						
Using personal email/social networking/instant messaging/text messaging to carry 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	✔	✔						
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		✔	✔		✔	✔		✔

APPENDIX 1
STAFF CODE OF CONDUCT FOR ICT

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff, governors, volunteers and students are aware of their professional responsibilities when using any form of ICT. All staff, governors, student and volunteers are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the E-Safety Officer.

- I will only use the school's email/Internet /Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords or codes provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number or personal email address, to pupils or parents(unless prior permission given by SLT for school trips.)
- I will ensure that I am not in contact with any pupils at Mickleover Primary School on Social Networking sites including Facebook and Twitter.
- I will only use the approved, secure school email system (..@mickleover.derby. sch.uk) for any school business.
- I will ensure that any pupil or personal data is kept securely on an encrypted device and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will only install hardware or software on a school laptop for educational purposes.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils will only be taken on school devices.
- Images of pupils will only be stored on the school network or school encrypted devices.
- Parental consent is required to publish any images on the school website or distributed outside school.
- I understand that my use of the Internet on school devices, eg laptops, i-pads etc and other related technologies can be monitored by the Headteacher and ICT Leader.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the E-Safety Coordinator.
- I will not disclose information about Mickleover Primary School on social media.
- I will uphold public trust by maintaining high standards of ethics and behaviour within and outside school as stated in teachers' Standards.
- I will support and promote the school's E-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I agree to follow this code of conduct and to support the safe use of ICT throughout the school.
- I will ensure that my chosen password on my memory stick complies with industry standard which is 8 characters, at least one Upper case letter and one numeric. Ideally with a symbol too ie %$*£! **I will not use my children's names or my place of birth or Password1 etc.**

  The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. The school will not be liable for the loss or damage to any personally-owned devices that are brought into school.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: …… Capitals: …… Date……

Signed: …… Capitals: …… Date……

Signed: …… Capitals: …… Date……

APPENDIX 2
ICT ACCEPTABLE USE POLICY- PUPILS

This policy applies to all pupils at Mickleover Primary School. Mickleover recognises the importance of digital technologies as a powerful learning tool in school. We also recognise the importance of the correct use of technology both in and out of school and need to make clear the expectations of acceptable use and the consequences of not following the code of practice. The current ICT Acceptable Use Policy (AUP) is published on the School Website and is available from the school office. All pupils and their parents are required to follow the ICT AUP Pupil Agreement. Should a pupil fail to abide by this AUP he/she will be dealt with in line with the school Behaviour Policy. All illegal activities will be reported to the Head teacher and if necessary to the local Safeguarding Children's Authority and Social Services.

Pupil Usernames and Passwords

- Pupils must not disclose their username or password to anyone else.
- Pupils must not allow anyone else to use their account and should not use anyone else's account.
- Pupils must log off a device when they finish using it.
- Data must be kept in accordance with the Data Protection Act.
- Pupils must not disclose any personal information to another person.

Hardware/Software

- All pupils have a responsibility towards the care and safe-keeping of any digital devices or computers.
- Pupils are not permitted to download or install any software or apps on school devices.
- Pupils should report all faults on school devices to a member of staff.
- Pupils should report any content causing concern immediately to an adult.

Internet Use

- All use of the internet within school hours should be to enhance learning.
- Pupils must not search for, send or forward any sites containing offensive, obscene, violent or dangerous material.
- Pupils should report any inappropriate content immediately to the adult responsible for them at the time.

Social Networking and Cyber-bullying/Online Bullying

It is important that children understand the risks of Social Networking, know how to stay safe in this environment and how to avoid making themselves vulnerable to a range of issues including identity theft, bullying, harassment, grooming and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment due to an inappropriate personal profile or inclusion on another's profile.

- Access to social networking sites is not allowed in school on any devices.
- Pupils are not permitted to have Mickleover Primary School staff as contacts on social networking sites.
- If incidents of cyber-bullying through social media come to the attention of school, we have a duty of care to deal with it. This is the case even if the cyber-bullying is taking place out of school.
- Mickleover Primary School will not tolerate any form of bullying including electronic or online bullying.

Child Exploitation and Online Protection (CEOP) The Child Exploitation and Online Protection centre provides useful guidelines and advice for teachers, parents and children. Thinkuknow.co.uk is the CEOP Centre's online safety centre. You will find advice and tips for children and adults.

We recommend that parents/carers also read this policy and ensure they understand it, discuss it with their child and understand consequences of not complying with the policy.

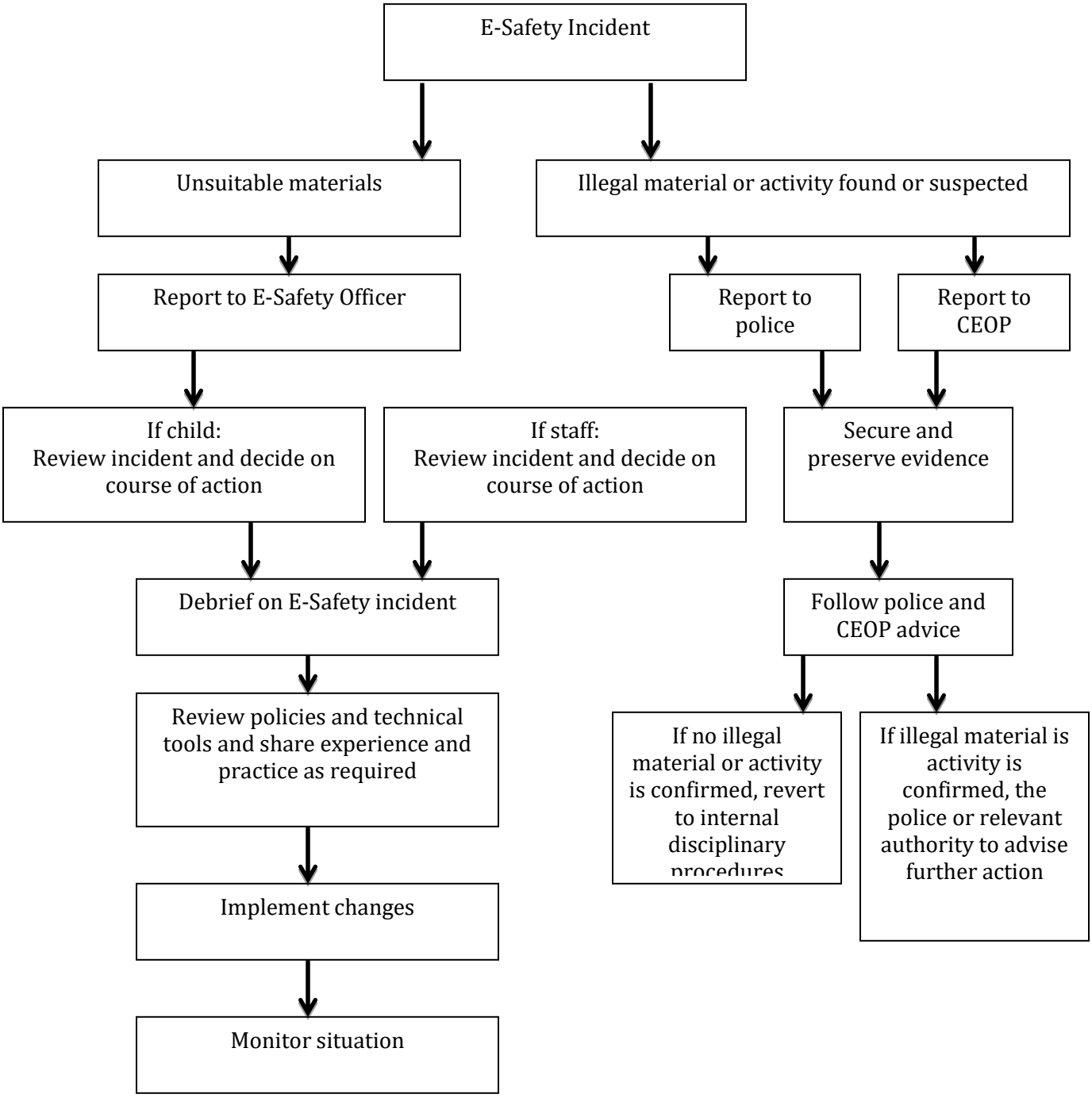
Appendix 3

Reporting E-Safety Concerns Proforma

Person Reporting Concern:		**Date:**	
Form Completed by:		**Role:**	
Indicate type of incident – please tick below.			
Website		**Safeguarding**	
Inappropriate website accessed		**Cyber Bullying**	
Inappropriate behaviour using ICT		**Sexual exploitation using technology**	
Illegal content accessed			
Inappropriate use of email or other technologies			
Deliberate misuse of school network			
Brief description of concern:			
Action taken:			
Signed:		**Date:**	

Appendix 4

Flowchart for Responding to E-Safety Incidents



This policy is linked to the following policies:

Safeguarding Policy
Behaviour Policy
PSHE Policy
Child protection policy
Anti-bullying Policy
Data Protection Policy