E-Safety Policy

This policy was re-adopted in March 2015
This policy will be reviewed in February 2016
ICT Coordinator's signature: ICT Manager's signature: Headteacher's signature: Safeguarding Governor's signature: Chair of Governor's signature:

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 and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and children to learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

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 helps to ensure safe and appropriate use. The development and implementation of our e-safety strategy involves all the stakeholders in our pupil's education from the Head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the children themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote child 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 for learning, safeguarding, ICT, acceptable use 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 our children's 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.

1. Aims and objectives

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

1.2 Aims of our E-Safety education are provided in the following ways:

- An E-safety programme is provided as part of Computing / PHSE / other lessons and is regularly revisited – this covers both the use of ICT and new technologies in school and outside school
- Key e-safety messages (CEOP THINKUKNOW resources) are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet are posted in all rooms and displayed on log-on screens (confirmation within Acceptable Use of Media Policy)
- Staff act as good role models in their use of Computing, the internet and mobile devices (confirmation within Acceptable Use of Media Policy)

2. Cyber-bullying

The extension of the use of mobile technologies, including the widespread use of mobile phones (generally with integrated cameras) by young people has lead to a new type of bullying-known as cyberbullying.
This may take the form of threats or abuse being sent by text, inclusive of multi-media messaging or phone calls. It may also take the form of pictures or videos taken without the permission of a young person or a member of staff and posted on the internet.

Our duty of care to our pupils means that we will implement the following cyber-bullying procedures:

- Bullying via mobile phones or the internet is included in our Anti-Bullying policy. This policy is regularly updated, and school staff have sufficient knowledge to deal with cyber-bullying.
- Our curriculum (e.g. THINKUKNOW resources and annual engagement through Safer Internet Day) teaches pupils about the risks of new communications technologies, the consequences of their misuse, and to use them safely.
- A clear expectation is set about the use of mobile phones at school by all stakeholders, including young people (confirmation within Use of Mobile Phones Policy). Permission for a pupil to have a mobile phone in school requires a written request from parents based on a genuine need for the phone to be in school. Once the Head teacher has given written permission the phone must be handed to the office at the beginning of the day, where it will be stored safely. It can be collected again at the end of the school day.
- Our internet filtering technologies are continually updated by the ICT Manager and harmful sites blocked through Netsweeper.
- We work with pupils and parents to make sure new communications technologies are used safely, taking account of local and national guidance and good practice.
- Action and sanction processes (Appendix 2.2 and 2.3) are in place to prevent images and information about pupils and staff being used outside school working with police and other partners when required.
- Servers and wireless systems are securely located and physical access restricted with encryption. Data is protected though encrypted hardware inclusive of hard drives, server support and memory sticks.

3. Stake holder Involvement

Many 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 the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).
The school provides information and awareness to parents and carers through:

- Letters, newsletters and information on school website
- Advice through parent consultation
- CEOP THINKUKNOW resources for parents

3.2 Education - Extended Schools

The school offers e-safety information through the school website, parent consultations, dedicated lessons, special events and staff training to ensure that staff, parents and children can together gain a better understanding of current issues. Messages around e safety are also targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering our children to stay safe while they enjoy these new technologies. When e-safety concerns are shared with the school, the Headteacher/DHT will meet with the relevant guardians to discuss possible e-safety risk and offer advice and/or support. Reported e-safety concerns will be logged and monitored in the schools E-Safety log.

3.3 Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal E-Safety training is renewed annually for all staff. An audit of the e-safety training needs of all staff is carried out regularly by the e-safety coordinator and/ or Computing Manager. (Some staff will identify e-safety as a training need within the performance management process).
- All new staff receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Policies
- This E-Safety Policy and its updates are presented to and discussed by staff in staff / team meetings / INSET days.
- The Computing/ E-Safety Coordinator and Computing Manager provide advice / guidance / training to individuals or groups as required.

3.4 Training – Governors

Governors take part in e-safety awareness sessions, with particular importance for those who are members of any sub committee / group involved in computing / e-safety / health and safety / child protection.

- Attendance at training provided by the Local Authority / National Governors Association / Child Protection Agency or other relevant organisation.
- Participation in school training / information sessions for staff or parents.
- Governor induction training.

3.5 Technical Support Providers – infrastructure / equipment, filtering and monitoring

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible, that procedures approved within this policy are implemented and that the Computing/ E-Safety Coordinator and Computing Manager are effective in carrying out their e-safety responsibilities.
The school works with external ICT Support Providers to ensure the following:

- Our school Computing systems are managed in ways that ensure that the school meets the e-safety technical requirements outlined in Local Authority E-Safety Policy and Ofsted E-Safety guidance.
- There are regular reviews and audits of the safety and security of our school ICT systems inclusive of proxy server access and filtering reports.
- Servers, wireless systems, cabling are securely located and physical access restricted with encryption.

- All staff have clearly defined access rights to school ICT systems.

(Details of the access rights available to groups of users is recorded by the Computing Manager and is reviewed, at least annually, by the Computing/E-Safety Coordinator).

- All users are provided with log-ons by the ICT Manager who monitors and maintains usage.
- The "master / administrator" passwords for the school ICT system, used by the Computing Manager are made available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- Staff are responsible for the security of their usernames and passwords, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by Netsweeper and maintained the Computing Manager.
- The school provides enhanced user-level filtering through the use of the Netsweeper filtering programme.
- In the event of the ICT Manager needing to switch off the filtering for any reason, or for any user, this is logged by the Computing Manager and the Head teacher
- Any filtering issues are reported immediately to the Computing Manager, Headteacher and/ or Netsweeper.
- Requests from staff for sites to be removed from the filtered list will be carefully considered by the Computing Manager and Computing Coordinator. If the request is agreed, this action will be recorded and logs of such actions shall be available from the Computing Manager.
- School Computing Manager to regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by the Computing Manager to control workstations and view child activity
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Computing Manager or e-Safety Coordinator. Request/urgent information slips are available to communicate incidents to the Computing Manager by pigeon hole or in person.
- When e-safety concerns are shared with the school, the Headteacher/DHT will meet with the relevant guardians to discuss possible e-safety risk and offer advice and/or support. Reported e-safety concerns will be logged and monitored in the schools E-Safety log.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place (Acceptable Use Policy) for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- An agreed policy is in place (Acceptable Use Policy) regarding the downloading of executable files by users
- An agreed policy is in place (Acceptable Use Policy) regarding the extent of personal use that users (staff / students / pupils) are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place (Acceptable Use Policy) that allows staff to or forbids staff from installing programmes on school workstations / portable devices.
- An agreed policy is in place (Acceptable Use Policy) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

- Teaching staff are provided with encrypted USB Keys to ensure safe transfer and storage of data.

3.6 Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum (please refer to E-Safety 'Click Safe' Posters for KS1 and KS2 in appendix 1.1 and 1.2).

- in lessons where internet use is pre-planned, children are guided to sites and pre checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches (Hector Image Alert on desk tops).
- Where children are allowed to freely search the internet, e.g. using search engines, staff must be vigilant in monitoring the content of the websites the young people visit.
- Children should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

3.7 Safer Teaching Practice

The computers are provided and maintained for the benefit of all staff, students and governors. Staff will be encouraged to use and enjoy these resources with E-safety and Child Protection in mind, ICT lessons and ICT resources should be planned in advance of lessons with URL's embedded within the planning. Children are to be directed to predetermined websites by URL with age appropriate content. In the event of open website searches, staff are requested to use safe methods of web searching such as 'Simple Sentence Search' exemplifying safe sentences to use in a search engine.

4. Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff and children need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals or the school in the short or longer term. The school will inform and educate users about these risks, provide training opportunities and employ a policy for acceptable use of social networking.

- When using digital images, staff should inform and educate children 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 e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims for internal use such as displays, classroom evidence folders etc., 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 (confirmation in Use of Images in School Policy).
- Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission.
- Teaching and support staff must make themselves aware of which pupils are not allowed (based on parent withdrawal of permission) to have their image used in school publications, school website and or external sources of media.
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Storage of photographs and videos are to be strictly stored upon the school server via the Public or personal profile.
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers is obtained before photographs of children are used or published on the school website (Use of images Policy contained with School Admissions Pack).
- By completing Appendix 1 and 2 of our Use of Images Policy, parents can protect the use of their child's image within

    - School display and portfolios
    - School Publications
    - School Website
    - External agency publications
    - The school does not use webcams with pupils at the present time
    - The school does not operate a CCTV system at the present time.

.

5. Data Protection

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances.

This includes:

Personal information about members of the school community-including children, members of staff and parents and carers e.g. names, address, contact details, legal guardianship/contact details, health records, disciplinary records.

- Curricular/academic data e.g. class lists, pupil/student records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisals
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members

The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed. Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay. All personal data will be fairly obtained in accordance with the 'fair processing code' and lawfully processed in accordance with the 'conditions for processing'.

All personal information curricular/academic data e.g. class lists, pupil/student records, reports, references, professional records e.g. employment history, taxation and national insurance records, appraisals and any other information that might be disclosed by parents/carers or by other agencies working with families or staff members will be kept secure by means of encrypting and/or pass wording data sticks and external hard drives.

All site Licences are stored within the central school safe. No passwords are stored centrally (no paper trail.) All software and Hardware discs are stored securely.

6. E-Safety Security:

The school operates a password security system to ensure that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- 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.
- Users can only access data to which they have right of access.
- No user should be able to access another's file, without permission.
- Access to personal data is securely controlled in line with the school's personal data policy.
- Members of staff are responsible for the security of their own passwords, no passwords are stored centrally (no paper trail.)

7. Our password system applies to all school ICT systems, including email, USB data travellers, external hard drives and Virtual Learning Environment:

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected.
- the device must be password protected .
- the device must offer approved virus and malware checking software.
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

8. Unsuitable / inappropriate activities

Some internet activity (e.g. accessing child abuse images or distributing racist material) is illegal and is obviously banned from our school and all other ICT systems. Other activities (e.g. Cyber-bullying) are also banned and could lead to criminal prosecution. There are however a range of activities (such as video hosting and photo chat) which may, generally, be legal but are inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities, referred to in Appendix 2.2 incidents, are inappropriate in our school context and that the staff should not engage in these activities in school or outside school when using school equipment or systems.

8.1 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 i.e.

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

Appendix 2.1 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.
All staff may report internally to the Computing Manager/ E-Safety Coordinator, further support may also be obtained from The Child Protection Company; www.childprotectioncompany.com

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 outlined in Pupil and Staff Action/Sanction checklists (**see Appendices 2.2, 2.3**).

8.2 Reporting Procedure

Children are provided with the skills and knowledge to use the internet and technologies safely as part of daily practice. In KS1 the children are provided with an e-safety passport (Appendix 3). In key stages 1 & 2 the children are able to report any concerns through their teacher, teaching assistant or the e-safety post box located in the school reception. The post box will be monitored regularly by the E-Safety coordinator, Computing coordinator and Computing Manager.

Staff are provided guidance via staff training and information upon the school safeguarding board in the staffroom. Staff are able to report all concerns upon an E-safety welfare form located on the school safeguarding board in the staffroom and these forms are to be taken to the E-safety Coordinator. Further support may also be obtained from The Child Protection Company www.childprotectioncompany.com

9. Communications

When using communication technologies the school considers the following as good practice:

- The official school email service is safe and secure and is monitored. Staff and children should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the e-Safety Coordinator – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and children or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class, group or individual (to be used in school only) email addresses will be used at upper KS2 only. These accounts will be set and monitored by the ICT Manager with the support of the e-safety coordinator.
- Children will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails (THINK U KNOW activities-CEOP and support from the child protection company www.childpotection.com) and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

10. Monitoring/Review

This e-safety policy was approved by the *Governing Body*	04th February 2014
The implementation of this e-safety policy will be monitored by the:	*E-Safety Coordinator, Computing Coordinator Senior Leadership Team*
Monitoring will take place at regular intervals:	*Termly by E-Safety Coordinator/ Computing Coordinator and Computing Manager*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	Initiated March 2015 Review March 2016
Should serious e-safety incidents take place, one or more of the following external persons / agencies should be informed:	LSCB/ CC Safeguarding officer/ LADO/ MARU

The school will monitor the impact of the policy using:

- Logs of reported incidents using proxy server information.
- Internal monitoring data for network activity
- Feedback from staff consultation
- Feedback from parental consultation meetings
- Feedback from pupils

Appendix 1.1 KS1 'Click Safe' Poster

Appendix 1.2 KS2 'Click Safe' Poster

e-Safety Links for Parents

These links will give you information on safe Internet use.

www.swgfl.org.uk/safety

www.childnet-int.org/kia/parents/

www.thinkuknow.co.uk

SW GRID for LEARNING

THINK U KNOW

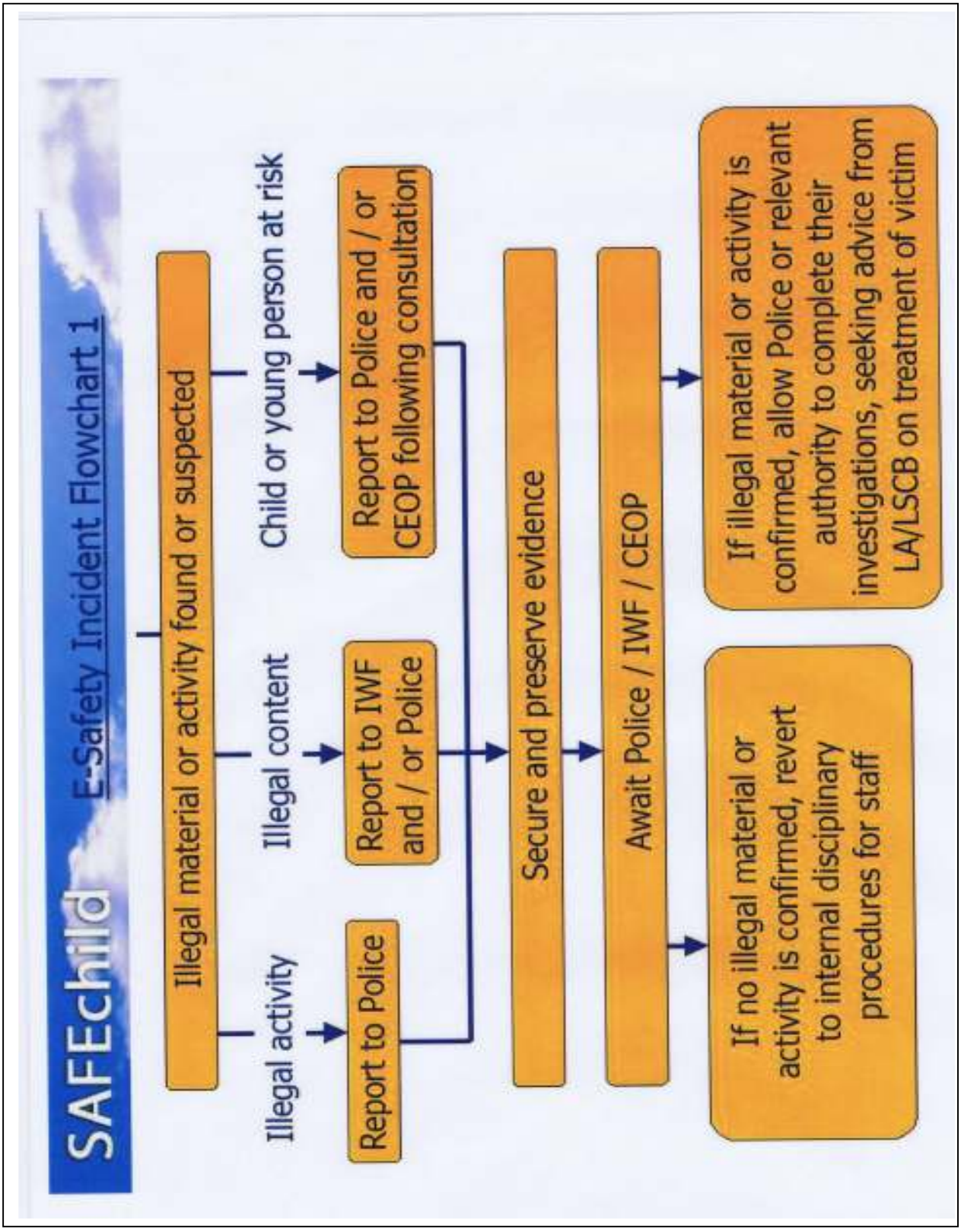
Childnet International

SOMERSET County Council

Developed by South West Grid for Learning Trust and Somerset County Council

Heamoor

Appendix 2.1


SAFEchild
E-Safety Incident Flowchart 1
Illegal material or activity found or suspected
Illegal activity
Report to Police
Illegal content
Report to IWF and / or Police
Child or young person at risk
Report to Police and / or CEOP following consultation
Secure and preserve evidence
Await Police / IWF / CEOP
If no illegal material or activity is confirmed, revert to internal disciplinary procedures for staff
If illegal material or activity is confirmed, allow Police or relevant authority to complete their investigations, seeking advice from LA/LSCB on treatment of victim

Appendix 2.2

Staff — Actions / Sanctions

Incidents: Any Incident where it is deemed necessary to investigate further could result in suspension and disciplinary action		Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to IT Manager 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).		✓	✓	✓			✓	✓
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 e.g. 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 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		✓	✓			✓		✓
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 in school		✓	✓	✓	✓		✓	✓
Breaching copyright or licensing regulations						✓		
Continued infringements of the above, following previous warnings or sanctions		✓	✓	✓	✓		✓	✓

Appendix 2.3

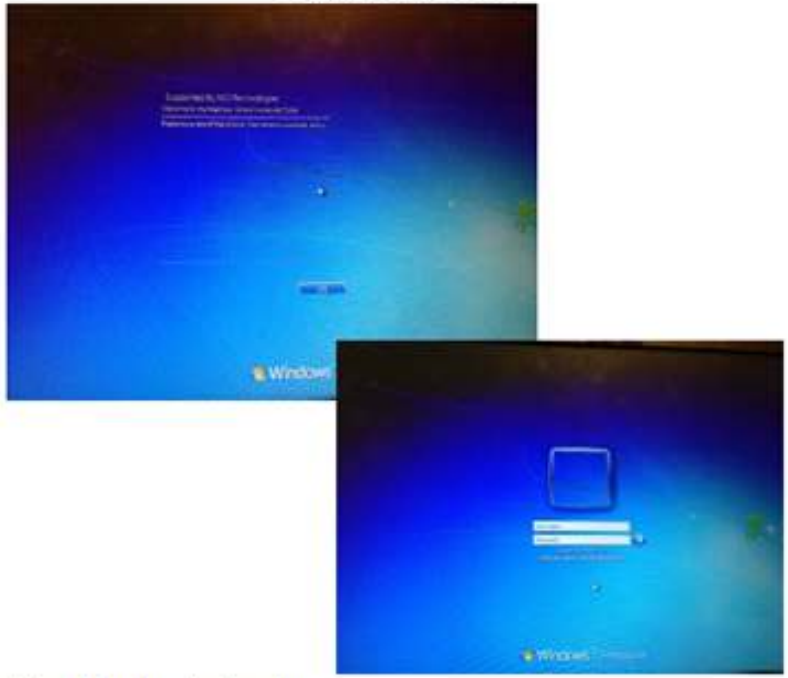
Pupils — Actions / Sanctions

Incidents: Any incident where it is deemed necessary to investigate further could result in temporary or permanent exclusion.		Refer to class teacher	Refer to Headteacher	Inform parents / carers	Refer to Police	Refer to IT Manager for action re filtering etc	Removal of network / internet access rights	Warning	Further sanction e.g. PSP / 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 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		✓	✓	✓	✓	✓	✓		✓

Appendix 3

E-Safety
My E-Safety Passport to ICT at Heamoor School
EYFS & KS1
Be smart on the internet
Name: .....
Class: .....
My Passport Stamps
Have I used the ICT suite safely?

Logging on at School



How I log in at school -

My username

.....

When I log onto a school computer I understand that I use the rules for E-Safety.

I know how to stay safe on the computers at school.

All about Hector

A picture of Hector