

Humberston C of E Primary School E-Safety Policy

Agreed by Governors June 2014
Last Review: 2023
Next Review: Summer 2025

The Humberston C of E Primary School

E-safety Policy

Contents

Introduction	2
Development, Monitoring and Review	3-4
Roles and Responsibilities	5-7
Education and Curriculum	8-9
Infrastructure, Equipment, Filtering and Monitoring	10-11
Data Protection	12
Use of Digital Images	13
Communications	14-15
Unsuitable/Inappropriate Activities	16-21
Acknowledgements	22

Introduction

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 pupils 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 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.

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

The e-safety policy that follows explains how we intend to manage and reduce these risks, 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. It should be read in conjunction with the following documents and policies

- Computing policy.
- Acceptable Use Agreement.
- Anti-Bullying / Safeguarding Policy.

Development, Monitoring and Review

This E-Safety policy has been developed by the following:

- School Computing Subject Leader (E-Safety Coordinator)
- Headteacher

It will be made available to the whole school community through the following:

- Staff meetings
- Governors meeting
- School website

Schedule for Development, Monitoring and Review

This E-Safety policy was approved by the Governing Body/Governors Sub Committee on:	Summer term 2023
The implementation of this E-Safety policy will be monitored by the:	ICT Subject Leader & E-safety Committee
Monitoring will take place at regular intervals:	Annually by the Strategic Lead – ICT in Schools
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:	Autumn Term 2023
Should serious E-Safety incidents take place, the following external persons/agencies should be informed:	LA Safeguarding Officer Local Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Staff training

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school IT systems, both in and out of school.

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

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

Roles and Responsibilities

The following section outlines the roles and responsibilities for E-Safety of individuals and groups within the school.

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-Safety incidents and monitoring reports. The named E-Safety Governor is Mrs J Everitt.

The role of the E-Safety Governor will include:

- regular contact with the E-Safety Co-ordinator regarding E-Safety incidents
- reporting to relevant Governors committee

Headteacher:

- is responsible for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the E-Safety Co-ordinator.
- is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- will receive regular monitoring reports from the E-Safety Co-ordinator.
- should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff
- will regularly monitor the use of the network, internet, Virtual Learning Environment (VLE) and email in order that any misuse/attempted misuse can be investigated and possible sanctioned.
- will ensure that monitoring software/systems are implemented and updated as agreed in school policies.

E-Safety Coordinator:

- leads the E-Safety committee
- takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority
- receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments,
- communicates regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs

- attends relevant meeting/committee of Governors
- reports to Headteacher
- regularly monitor the use of the network, internet and emails in order that any misuse/attempted misuse can be reported to the Headteacher for investigation and possible sanction.

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices.
- they have read, understood and signed the school Staff Acceptable Use Agreement (AUP).
- they report any suspected misuse or problem to the E-Safety Co-ordinator and Headteacher for investigation and possible sanction.
- digital communications with pupils should be on a professional level and only carried out using official school systems.
- E-Safety issues are embedded in all aspects of the curriculum and other school activities.
- pupils understand and follow the school E-Safety and acceptable use policy.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor ICT activity in lessons, extra curricular and extended school activities.
- they are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Child Protection Co-ordinator –

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Agreement which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will therefore take every opportunity to help parents understand these e-safety issues through parents' evenings, newsletters, letters, website/VLE

and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Agreement

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.

- in lessons where internet use is pre-planned, it is best practice that 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.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should inform the Headteacher and e-safety co-ordinator.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Education

Pupils

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.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT, EPR and other lessons. It will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages will be reinforced as part of a planned programme of assemblies
- In all lessons, pupils will be taught to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Parents/Carers

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 and 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. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents evenings
- Reference to e-safety websites

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 programme of e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator will receive regular updates through attendance at LA training and e-safety co-ordinator sessions and by reviewing guidance documents released by BECTA, SWGfL, the LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings and will be available on the school network and in the school policy file.
- The E-Safety will provide advice, guidance and training as required to individuals as required.

Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members involved in ICT/e-safety, health and safety and child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority
- Participation in school training or information sessions for staff or parents

Infrastructure, Equipment, Filtering and Monitoring

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 ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Local Authority e-safety policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).
- The school maintains and supports the managed filtering service provided by the local authority
- Any filtering issues should be reported immediately to the local authority I.C.T. officer
- Requests from staff for sites to be removed from the filtered list will be considered by the, Head teacher and e-safety co-ordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.

An appropriate system is in place for users to report any actual/potential e-safety incident to the Network Manager, e-safety co-ordinator or headteacher (see flow chart appendix 1)

- 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 (This is covered by the school ICT SLA.
- An agreed policy is in place (to be described) for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place regarding the extent of personal use that users and their family members are allowed on laptops and other portable devices that may be used out of school. • An agreed policy is in place (to be described) that allows staff to install programmes on school workstations/portable devices.

-

Data Protection

Personal data will be recorded, processed, transferred and made available according to GDPR.

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

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 encryption and secure password protected devices.

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 (many memory sticks / cards and other mobile devices cannot 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

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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 KS2 pupils should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff and pupils are allowed to take digital/video images to support educational aims, but must ensure the following
 - Images should only be stored on school equipment.
 - Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
 - Written permission from parents or carers must be obtained before photographs of pupils or pupils work is published.
 - 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.
 - Pupils must not take, use, share, publish or distribute images of others without their permission.

Communications

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:

Communication Technologies	Staff & other adults				Pupils			
	Allowed	Allowed in social time	Allowed for professional/ educational purposes	Not allowed	Allowed	Allowed for educational purposes with staff permission	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						X	
Use of mobile phones in school		X						X
Use of mobile phones for personal use		X						X
Taking photos on other camera devices			X			X		
Use of hand held devices eg PDAs, PSPs			X			X		
Use of personal email addresses in school, or on school network	X						X	
Use of school email for personal emails				X			X	
Use of chat rooms/facilities			X			X		
Use of instant messaging			X			X		
Use of social networking sites			X			X		
Use of blogs			X			X		
Use of chat rooms, instant messaging, social networking sites or blogs for personal use		X						X

Unsuitable/Inappropriate Activities		Acceptable	Acceptable at certain times	Unacceptable	Unacceptable and illegal
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows: User Actions					
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images				X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse & fraud legislation				X
	adult material that potentially breaches the UK Obscene Publications Act				X
	criminally racist material in UK				X
	pornography			X	
	promotion of any kind of discrimination			X	
	promotion of racial or religious hatred			X	
	threatening behaviour, including promotion of physical violence or mental harm			X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute			X	
Using school systems to run a private business				X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Carrying out sustained or instantaneous high volume network traffic (downloading /uploading files) that causes network congestion & hinders others in their use of the internet				X	
On-line gaming (educational and non-educational)			X		
On-line gambling				X	
On-line shopping			X		
File sharing			X		
Use of social networking sites			X		
Use of video broadcasting e.g. Youtube			X		

When using communication technologies and/or school systems the school considers the following as good practice:

- Users need to be aware that email communications and use of school systems may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any electronic communication 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 pupils or parents/carers (email, 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 from systems other than the teachers to parents programme or public chat/social networking programmes must not be used for these communications.
- Pupils should 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 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.

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

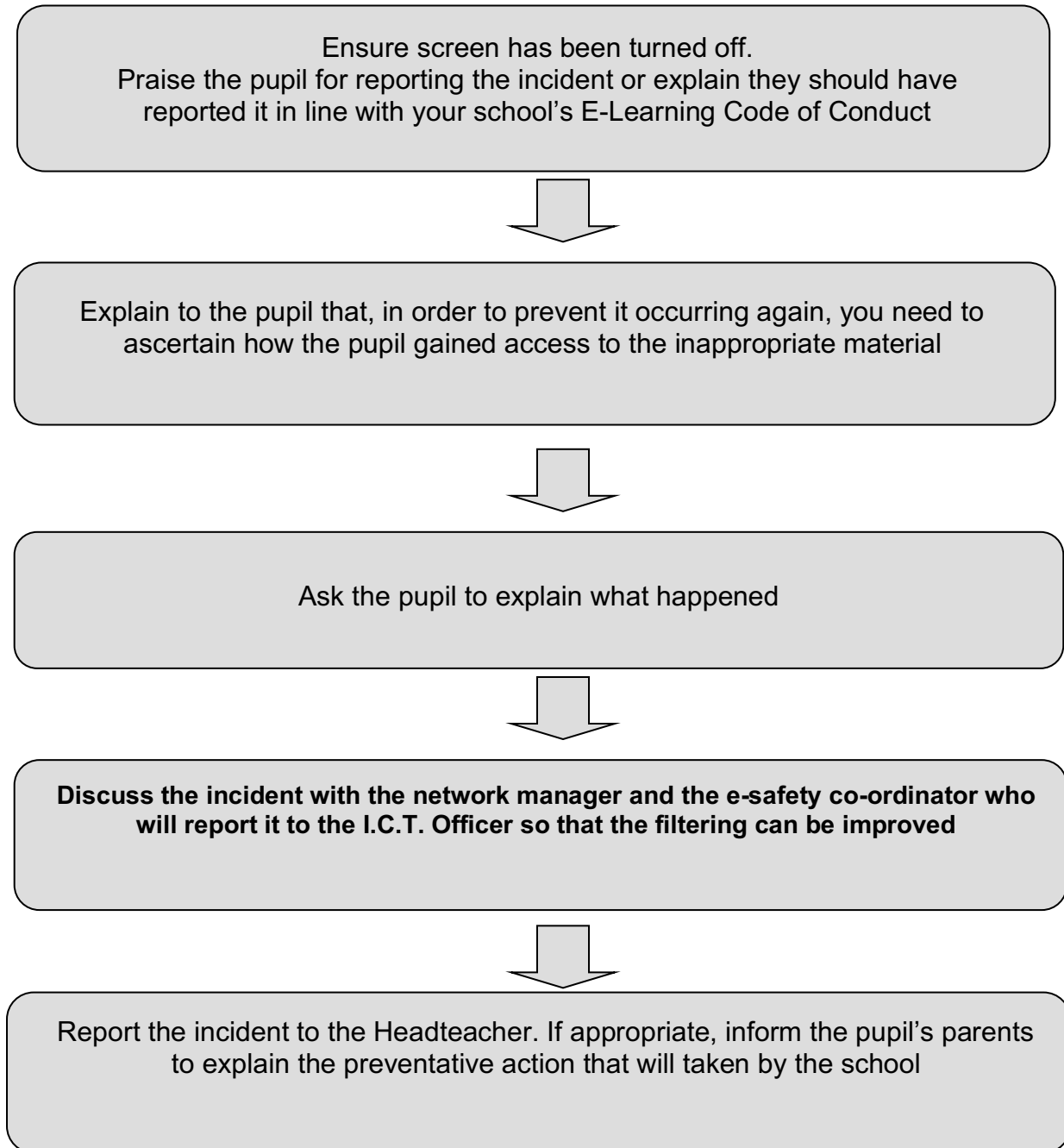
staff must follow school safeguarding procedures.

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. More than one member of staff will be involved in the investigation which should be carried out on a “clean” designated computer.

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:

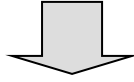
Primary School Guidelines to Inappropriate Internet Access

Whilst using the Internet during school hours, a pupil **accidentally** types in a website address that will display inappropriate material. What should you do?

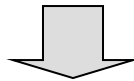


Whilst using the Internet during school hours, a pupil **deliberately** types in a website address that will display inappropriate material. What should you do?

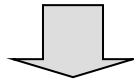
Explain to the pupil that they have broken the rules of your school's E-Learning Code of Conduct and that their behaviour is unacceptable



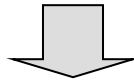
Take the pupil off the computer for the duration of the lesson. At a convenient time, ask the pupil to explain what happened and tell them that by doing so they may lessen the seriousness of the incident.



Draw the pupil's attention to the E-Learning Code of Conduct that they agreed with their parents on starting at the school, which is summarized on the poster displayed in your ICT area



Discuss the incident with the network manager and the e-safety co-ordinator who will report it to the I.C.T. Officer so that the filtering can be improved



Report the incident to the Headteacher. Decide the sanctions as per the school behaviour policy for breaking rule. If appropriate, inform the pupil's parents and explain the action taken by the school