

Queen Mary Avenue Infant and Nursery School



Online safety Policy

Autumn 2022

Review Frequency: Every Two Years

Approval Required by: Headteacher

Contents

Vision and values	3
Introduction	3
Linked Policies and Documentation	4
Our Aims	4
Scope of Policy	4
Review and Ownership	4
Communication of the Policy	4
Roles and Responsibilities	5
Online Risks	8
Managing digital content	8
Storage of Images	8
Learning and Teaching	9
Staff training	9
Resources	10
Managing ICT Systems and Access	11
Management of Assets	11
Data Protection and Information Security	12
Emerging Technologies	12
Filtering Internet Access	13
Internet Access Authorisations	13
Email	13
Mobile Phone Usage in School	14
Social Media	14
Reporting and Response to Incidents of Misuse	15
Guidelines to Inappropriate Internet Access by Pupils - Accidental	16
Guidelines to Inappropriate Internet Access by Pupils - Deliberate	17



Respect – Hard Work – Pride – Kindness – Honesty

Dream Big

We believe that everyone can succeed and achieve their dreams.

Shine Bright

We value and nurture each child's unique talents so that they can 'shine bright'.

Introduction

Queen Mary Avenue Infant School fully recognises the contribution it can make to protect children and support them in school. The aim of this policy is to safeguard and promote our pupils' safe use of the internet and electronic communication technology. The internet and other technologies have an important role in the learning and teaching processes however, we feel it is important to balance those benefits with an awareness of the potential risks. This policy will highlight the need to educate children and adults about the benefits and risks of using technologies both in and away from school. It will also provide safeguards and rules to guide staff, governors, pupils and visitors in their online experiences.

As a school we will take a whole school approach to safeguarding and any related policies and procedures. We will ensure that online safety is ongoing and interrelated which will include considering how online safety is reflected in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.

Keeping Children Safe in Education 2022 sets out specific responsibilities for governing bodies to ensure:

- children are taught about online safety
- appropriate filters and appropriate monitoring systems are in place
- online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach

When devising this policy we have carefully considered the 4Cs – content, contact, conduct and commerce – see p. 7 for more details.

The school acknowledges online safety and online security as important issues for our school community and strives to embed online safeguarding into our teaching and learning using technology. The school have considered the wider implications of e-safeguarding beyond classroom practice such as security and data.

Linked Policies and Documentation

The school online safety policy will operate in conjunction with other policies and documentation

- Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Data Protection Policy
- [Managing Allegations of Child on Child Abuse Policy](#)
- Acceptable Use Agreements with parents/carers and staff/governors

Aims

- To set out the key principles expected of all members of the school community at Queen Mary Avenue Infant School with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of Queen Mary Avenue Infant School.
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Scope of Policy

- This policy applies to the whole school community including governors, all staff employed directly or indirectly by the school, volunteers parents/carers and all pupils.
- The computing coordinator, safeguarding team and governors will ensure that any relevant or new legislation that may impact upon the provision for e-Safeguarding within school will be reflected within this policy.

Review and Ownership

- The computing co-ordinator, governors and Headteacher will be responsible for document ownership, review and updates.
- The online safety policy is reflected in many other school policies as outlined in section one.
- The school online safety policy has been agreed by the staff and approved by governors.
- The online safety policy will be reviewed every two years or when any significant changes occur with regard to the technologies in use within the school
- All amendments to the school online safety policy will be discussed in detail with all members of teaching staff.

Communication of the Policy

- The Senior Leadership team, Computing Co-ordinator and class teachers will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school online safety policy and the use of any new technology within school.
- The Online Safety Policy will be provided to and discussed with all members of staff, governors and teaching students and will be reviewed regularly.
- We endeavour to embed the online safety messages across the curriculum, whenever the internet or related technologies are used.
- The online safety policy will be introduced to the pupils at the start of each school year and revisited through ICT, PSHCE lessons and Safer Internet Day.

Roles and Responsibilities

Responsibilities of the School Community

We believe that online safety is the responsibility of the whole school community and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Governing body

The senior leadership team including designated safeguarding lead

The computing coordinator

Teachers and support staff

Pupils

Parents and carers

Responsibilities of the Governing Body

To read, understand, contribute to and approve the school's Online Safety Policy and guidance

To develop an overview of the benefits and risks of the internet and how infrastructure provides safe access to the internet used by pupils

To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school

To support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school

To ensure appropriate funding and resources are available for the school to implement its online safety strategy

Responsibilities of the Headteacher and Senior Leadership Team

Ensure that all staff receive suitable training to carry out their online safety roles including online risks of extremism and radicalisation

Create a culture where staff and learners feel able to report incidents

Ensure that there is a progressive online safety curriculum in place

Ensure that there is a system in place for monitoring online safety

Follow correct procedure in the event of a serious online safety allegation being made against a member of staff or pupils

Inform the local authority about any serious online safety issues

Ensure that the school infrastructure/network is as safe and secure as possible

Ensure that policies and procedures approved within this policy are implemented

Work with the designated safeguarding lead, computing lead and data protection officer to ensure that the Online Safety Policy develop and implemented by the school meets safeguarding and online safety requirements

Log, manage and inform others of online safety incidents and how they have been resolved where this is appropriate.

Responsibilities of the Computing Lead

- To promote an awareness and commitment to online safety throughout the school
- To be a point of contact in school on all online safety matters along with the Head teacher
- To take day-to-day responsibility for online safety within school and to have a leading role in establishing and reviewing the school online safety policies and procedures
- To communicate regularly with school technical staff
- To create and maintain online safety policies and procedures
- To ensure that all members of staff receive an appropriate level of training in online safety issues
- To ensure that online safety education is embedded across the curriculum
- To ensure that online safety is promoted to parents and carers
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- To ensure that any online safety incidents are logged and followed up
- To ensure that the school Acceptable Use policies are current and pertinent

Responsibilities of Teachers and Support Staff

- To read, understand and help promote the school's online safety policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any suspected misuse or problem to the subject lead
- To develop and maintain an awareness of current online safety issues and guidance
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed online safety messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- To be aware of online safety issues related to the use of mobile phones, cameras and handheld devices
- To be aware of indicators of abuse and understand that children can be at risk of harm online
- To understand that children can abuse other children online and this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography to those who do not want to receive such content. See [Child on Child Abuse policy for more details.](#)
- To maintain a professional level of conduct in personal use of technology at all times

Responsibilities of ICT Technicians (TTS)

- To support the school in providing a safe technical infrastructure to support learning and teaching
- To ensure that access to the school network is only through an authorised, restricted mechanism
- To ensure that provision exists for misuse detection and malicious attack
- To take responsibility for the security of the school ICT system
- To liaise with the local authority and other appropriate people and organisations on technical issues
- To document all technical procedures and review them for accuracy at appropriate intervals
- To restrict all administrator level accounts appropriately
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- To ensure that controls and procedures exist so that access to school-owned software assets are restricted

Responsibilities of Pupils

- To understand and adhere to the school pupil Acceptable Use Policy
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to

Responsibilities of Parents and Carers

- To help and support the school in promoting online safety
- To read, understand and promote the school Acceptable Use Agreement for Pupils with their children
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home
- To discuss e-Safeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology
- To agree to and sign the school's parental permission form which clearly sets out the use of photographic and video images outside of school
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites. Photos that are used on social media must be cropped so that only their own child is shown.
- Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to school
- Parents and carers are required to give written instruction if they do NOT wish for any images of their child to be used.(parental permission form)

Online Risks

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing

Managing Digital Content - Using Images, Video and Sound

- Parents and carers will be asked if they give permission for using photographs for the school website or in any printed material when the child starts at the school.
- Parents and carers can withdraw permission, in writing, at any time.
- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound.
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites. Photos that are used on social media must be cropped so that only their own child is shown.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Storage of images

- Any images, videos or sound clips of pupils must be stored on the school server network and never transferred to personally-owned equipment.
- The school may store images of pupils that have left the school following their departure for use in school activities and promotional resources.
- Staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We will celebrate and promote online safety through whole school activities, including promoting Safer Internet Day
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way
- We will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil and parent will be asked to sign
- Children will be taught how to stay safe online
- Staff will model safe and responsible behaviour in their own use of technology during lessons
- All pupil internet use will be monitored and pupils will be reminded of what to do if they come across unsuitable content
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member
- Communications with parents and carers will be used to reinforce the importance of children being safe online and make them aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online

Staff and Governor Training

- Our staff will be kept up to date on any changes in online safety information and will receive training when necessary.
- As part of the induction process all new staff will receive information and guidance on the online safety policy and the school's Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

Resources

The following resources may also help schools and colleges understand and teach about safeguarding:

- DfE advice for schools: teaching online safety in schools
<https://www.gov.uk/government/publications/teaching-online-safety-in-schools>
- UK Council for Internet Safety (UKCIS) Education for a connected world guidance:
<https://www.gov.uk/government/publications/education-for-a-connected-world>
- The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk. The helpline provides expert advice and support for school and college staff with regard to online safety issues
- Internet Watch Foundation: If the incident/report involves sexual images or videos that have been made and circulated online, the victim can be supported to get the images removed by the Internet Watch Foundation (IWF) <https://www.iwf.org.uk/>
- • Childline/IWF Report Remove is a free tool that allows children to report nude or sexual images and/or videos of themselves that they think might have been shared online
<https://www.iwf.org.uk/our-technology/report-remove/>
- UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people
<https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people>
- The UKCIS external visitors guidance will help schools and colleges to ensure the maximum impact of any online safety sessions delivered by external visitors
<https://www.gov.uk/government/publications/using-external-visitors-to-support-online-safety-education-guidance-for-educational-settings>
- National Crime Agency's CEOP education programme: Thinkuknow
<https://www.thinkuknow.co.uk/>
- Public Health England Every Mind Matters
<https://campaignresources.phe.gov.uk/schools/topics/mental-wellbeing/overview>
- Harmful online challenges and online hoaxes - this includes advice on preparing for any online challenges and hoaxes, sharing information with parents and carers and where to get help and support.
<https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes>
- LGFL 'Undressed' <https://undressed.lgfl.net/> provided schools advice about how to teach young children about being tricked into getting undressed online in a fun way without scaring them or explaining the motives of sex offenders.

Managing ICT Systems and Access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructures will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- All users will sign an end-user Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.

Management of Assets

All schools will have both software and hardware assets for both educational and administrative purposes. All equipment and software comes at a cost to the school and is therefore controlled and documented appropriately. By maintaining valid inventories, we are in a position to extract full value from our purchases as educational activities can be based and planned around the assets held. Recording information on all equipment also assists in hardware replacement programmes and software upgrades, as spending can be planned against asset age and specification. Old hardware such as laptops, PCs, servers and removable media will be formatted prior to disposal (or through a third party) to ensure no sensitive or personal data remains on old hardware.

- Details of all school owned hardware will be recorded in an electronic hardware inventory.
- All redundant ICT equipment will be disposed of through an authorised agency (recommended by TSS). This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen

Data Protection and Information Security

The school's Data Protection Policy provides full details of the requirements that are met in relation to Data Protection regulations.

The school will:

- at all times take care to ensure the safe keeping of personal and sensitive data, minimising the risk of its loss or misuse which must include regular back-ups and anti-virus protection updates
- use personal data only on secure password protected computers and other devices
- ensure that users are properly 'logged-off' at the end of any session in which they are accessing personal data
- provide staff with secure equipment/services to store or transfer data e.g. remote access, One Drive, SharePoint school portal, encryption and secure password protected devices
- remove data in line with the school's Data Retention Policy
- ensure that all staff are aware of the need to immediately report any loss of personal or sensitive data to the Data Protection Lead and that relevant staff understand the full requirements of Data Protection Act 2018
- complete a privacy impact assessment and check the terms and conditions of sites/apps used for learning purposes to ensure that any pupil personal data is being held securely

Emerging Technologies

New and emerging technologies are being developed constantly in today's fast-moving digital world. These technologies can be anything from handheld devices to new faster communication mechanisms. Schools should try to always be aware of new and appealing technologies as these can, in many cases, offer the potential to develop new teaching and learning tools. As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an online safety point of view. We will amend the online safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an online safety risk.

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

Emerging technologies can incorporate software and/or hardware products.

The acceptable use of any new or emerging technologies in use within school will be reflected within the school online safety and Acceptable Use policies.

Prior to deploying any new technologies within school, staff and pupils will have appropriate awareness training regarding safe usage and any associated risks.

The school will audit ICT equipment usage to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.

Methods to identify, assess and minimise risks will be reviewed regularly.

Filtering Internet Access

The internet is a valuable tool for teaching and learning. Unfortunately, not all content that is available on the internet is suitable for schools, so provision has to be made to ensure that a suitable, fit-for-purpose internet filtering solution is deployed.

- The school uses a filtered internet service appropriate to the age and maturity of pupils.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school has a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the online safety Coordinator or the Head Teacher. All incidents should be documented.
- The school will regularly review the filtering product for its effectiveness.
- Pupils will use age-appropriate tools to research internet content.
- We recognise that "over blocking" can lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

Internet Access Authorisations

- Parents will be asked to read the school Acceptable Use Policy for pupil access and discuss it with their children, when and where it is deemed appropriate.
- All pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy prior to being granted internet access within school.
- All staff will have the appropriate awareness training and sign the staff Acceptable Use Policy prior to being granted internet access within school.
- The school will maintain a current record of all staff and pupils who have signed the Acceptable Use Policy.
- Any visitor who requires internet access will be asked to read and sign the Acceptable Use Policy.

Email

Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.

- Staff should not use personal email accounts for professional purposes, especially to exchange any school-related information or documents.
- It is the responsibility of each account holder to keep the password secure.
- School email accounts should be the only account that is used for school-related business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Pupils and staff will be reminded about the dangers of revealing personal information within email conversations.
- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal account.
- Pupils and staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- Irrespective of how staff access their school email (from home or within school), school policies still apply.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.

Mobile Phone Usage in School

In today's digital world, communications and content are available almost anywhere at any time. Modern-day smart phones are effectively mobile computers, which are far more powerful and feature-rich devices than the original home computers.

Mobile Phones and personally owned devices will be switched off or switched to 'silent' mode during teaching periods unless permission has been granted by a member of the senior leadership team.

Mobile phones and personally owned mobile devices brought in to school by staff are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.

Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school equipment for this purpose.

Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during visits, or for contacting pupils or parents, then they may use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes.

Personal devices should be pin code or fingerprint protected and not discoverable by third parties.

If a member of staff breaches the school policy then disciplinary action may be taken.

Social Media

- School will control access to social media and social networking sites in school.
- When using the school Facebook or Instagram page staff should ensure that any digital communication between staff and pupils or parents and carers is open, transparent and professional in tone and content
- Staff will ensure that in private use:
 - No reference is made in social media to students / pupils' parents/ carers or school staff
 - Data about pupil/ staff or parents is not shared on social media
 - 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 /academy or local authority
 - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Reporting and Response to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of computing, 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.

Incidents of misuse should be reported to a senior leader or the chair of governors if the incident relates to the Headteacher. They will be recorded.

When responding to incidents of misuse, more than one member of staff (at least one should be a senior leader) will be involved. All sites and content checked will be recorded and screen shots, signed and dated, will be kept where this is appropriate. Where content being reviewed is suspected or known to include images of child abuse, the investigation will be referred to the Police immediately and no further access will be made by the school to the material.

- Staff will record incidents in the appropriate concerns log. All reported incidents will be dealt with and actions recorded
- The Designated Safeguarding Lead (DSL) will be informed of any online safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures
- The school will manage Online safety incidents in accordance with the School Behaviour Policy
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact N. E Lincolnshire Safeguarding Team and escalate the concern to the police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Local Authority Designated Officer (LADO).

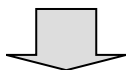
The police will be informed where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist or terrorist material, verbally abusive or threatening material information which is false and known or believed by the sender to be false

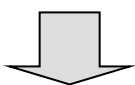
Guidelines to Inappropriate Internet Access by Pupils

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

Ensure screen has been turned off.
Praise the pupil for reporting the incident or explain they should have reported it in line with your school's E-Learning Code of Conduct



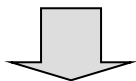
Explain to the pupil that, in order to prevent it occurring again, you need to ascertain how the pupil gained access to the inappropriate material



Ask the pupil to explain what happened



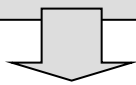
Discuss the incident with the network manager and the e-safety co-ordinator who will report it to the Computing Officer so that the filtering can be improved



Report the incident to the Headteacher. If appropriate, inform the pupil's parents to explain the preventative action that will be taken by the school

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

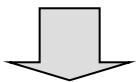
Explain to the pupil that they have broken the rules of your school's E-Learning Code of Conduct and that their behaviour is unacceptable



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.



Discuss the incident with the network manager and the e-safety co-ordinator who will report it to the Computing 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