E-SAFETY POLICY

Introductory Statement

The internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available. Use of email, mobile phones, internet messaging and blogs all enable improved communication and facilitate the sharing of data and resources.

There are some dangers associated with the internet and emerging new technologies that are highly publicised in the media.

- Children and/or young adults might inadvertently access content of an unsavoury, distressing or offensive nature on the internet or receive inappropriate or distasteful emails.
- Children and/or young adults might receive unwanted or inappropriate emails from unknown senders, or be exposed to abuse, harassment or ‘cyber-bullying’ via email, text or instant messaging, in chat rooms or on social-networking websites, such as MySpace, Bebo, Facebook, etc.
- Chat rooms provide cover for unscrupulous individuals to groom children.

However there are social and educational benefits to be derived from using the internet and other technologies in school.

- Children and/or young adults are equipped with skills for the future.
- The internet provides Instant access to a wealth of up-to-date information and resources from across the world, which would not be otherwise available.
- The internet helps to improve children’s and/or young adults’ reading and research skills.
- Email, instant messaging and social networking helps to foster and develop good social and communication skills.

We believe that these far outweigh the risks involved so long as all users in school are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours.

This policy focuses on each individual technology available within the school and outlines the procedures in place to protect users and the sanctions to be imposed if these are not adhered to.

Procedures for Use of a Shared Network

- Users must access the network using their own logons and passwords. These must not be disclosed or shared. Adult users will be made familiar with this policy and pupils will be made familiar with the ‘Pupil and Parent Acceptable Use Policy’ (see appendix I). Frequent guest users will be made aware of this E-Safety policy. Occasional guests will not be given access to the shared network.

- Users must respect confidentiality and attempts should not be made to access another individual’s personal folder on the network without permission.

- Removable media are automatically scanned for viruses when used on a machine connected to the network.

- Machines must never be left ‘logged on’ and unattended. If a machine is to be left for a short while, it must be ‘locked.’ (Ctrl+alt+del followed by ‘lock computer’).

- Machines must be ‘logged off’ correctly after use.

- The wireless network is secure and password protected. The ICT technician and ICT coordinator have the password. Laptops and other mobile devices connect automatically to the wireless network.

Procedures for Use of the Internet and Email

- All regular staff users must read and understood this E-Safety policy before access to the internet and email is permitted in school. They must adhere to the guidance provided.

- Parental or carer consent is requested in order for children to be allowed to use the internet or email (see ‘Pupil and Parent Acceptable Use Policy’, Appendix I).

- Users must access the internet and email using their own logon / password and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user’s email account.

- The internet and email must only be used for professional or educational purposes during the school day. Staff may use the internet and email within reason for personal use when the school is not in session. This is at the headteacher’s discretion with some activities not permitted at all e.g. online gambling, shopping on EBay, downloading videos for personal use. If uncertain, please ask the headteacher.

- Children must be supervised at all times when using the internet and email.

- Procedures for safe internet use and the sanctions applicable if rules are broken will be clearly displayed in every room with access to the internet. Children will be taught regularly and at an age appropriate level to ensure they understand how to keep themselves safe online.

- Accidental access to inappropriate, abusive or racist material is to be reported without delay to the teacher and subsequently the ICT technician, under the supervision of the headteacher, and a note of the offending website address (URL) taken so that it can be blocked.

- Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is reviewed and updated regularly.

- Internet and email use will be monitored regularly by the ICT technician and reviewed by the headteacher in accordance with the Data Protection Act.

- Email addresses assigned to individual pupils will not be in a form which makes them easily identifiable to others.

- Users must not disclose any information of a personal nature in an email or on the internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.

- All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.

- All emails sent from a school email account will carry a standard disclaimer disassociating the establishment/service and the Local Authority with the views expressed therein.

- Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.

- If users are bullied, or offensive emails are received, this must be reported immediately to a trusted adult or member of staff within the school. Emails received should not be deleted, but kept for investigation purposes.

- Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.

- All email attachments are scanned before they are opened. This is carried out automatically by the email provider and also by the anti-virus software.

- Pupils must seek permission before downloading any files from the internet.

- All users will be made aware of copyright law and will acknowledge the source of any text, information or images copied from the internet.

Procedures for Use of Instant Messaging (IM), Chat and Weblogs

- The use of instant messaging (e.g. MSN messenger) is not permitted.

- Use of social-networking websites (e.g. Bebo, MySpace, Facebook, Habbo, Piczo, etc.) is not permitted within school time. The use of Shaka Tameside is permitted.

- Children and staff must not access public or unregulated chat rooms.

- Use of the school educational weblogs is permitted. This will be supervised and children will be reminded of the safe practices and behaviours to adopt when posting material, as well as the need to adopt a formal and polite tone at all times.

Social Networking Sites

Mottram Primary School recognises that most social networking sites have age restrictions of 13 or above, however, we are also aware that some parents do allow their children to use and access these sites outside of school.

- Children are not allowed to access social networking sites on the school premises.

- Staff are permitted to access social networking sites using school computers outside of school hours.

- If staff choose to have a social networking profile this must be set to the highest privacy setting available so children and parents cannot access information about them.

- Staff must not accept or make online friendship requests from or to pupils who are still in the education system (primary or secondary).

- Staff must not use social networking sites to air their personal or professional opinions about school or staff.

- Parents or staff must not upload images or videos taken during school activities onto their own social networking profile.

Procedures for the School Twitter Account

- Children are not allowed to access the School Twitter account in school.
- Parental permission must be sought before uploading a pupil’s work or picture to the site. No pupil names should be used.
- Staff are permitted to access the School Twitter site using school computers and/or school iPads.
- Staff must not accept or make online follow requests from or to pupils who are still in the education system (primary or secondary).
- All followers on the School Twitter page are individuals known to school e.g. parents, carers, grandparents etc.
- Staff must not use the social networking sites to air their personal or professional opinions about school or staff.
- Users must respect confidentiality and attempts should not be made to access another individual’s personal Twitter account.

Procedures for Use of Cameras, Video Equipment and Webcams

- Permission will be obtained from a child's parent or carer before photographs or video footage can be taken. Permission is obtained on admission to the school and a record of this is kept in the school office (see 'Parent Consent Form for use of Pupil Images', Appendix II).

- Photographs or video footage will be downloaded immediately from the camera used and saved into a designated folder. This will be password protected and accessible only to authorised members of staff.

- Any photographs or video footage stored must be deleted immediately when no longer needed.

- Any adult using their own camera, video recorder or camera phone during a trip or visit must transfer and save images and video footage into a password protected folder on the school network immediately upon their return. The images must then be immediately deleted from the device used to take them.

- Children should not accept files sent via Bluetooth to their mobile phones by an unknown individual. If they do, and the content received is upsetting or makes them feel uncomfortable, they should pass this on to a trusted adult straightaway.

- Video conferencing equipment and webcams must be switched off (disconnected) when not in use and the camera turned to face the wall.

- Webcams must not be used for personal communication and should only be used with an adult present.

- Children and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

- Parents may take still or video footage of their own child/children during school events provided this is for personal use only and will not be uploaded and shared on a public place.

Procedures to ensure safety of the school website

- The school has a designated member of staff who is responsible for approving all content and images to be uploaded onto its website prior to it being published.

- The school website is subject to checks to ensure that no material has been inadvertently posted, which might put children or staff at risk.

- Copyright and intellectual property rights must be respected.

- Permission will be obtained from parents or carers before any images of children can be uploaded onto the school website. Permission is obtained on admission to the school and a record of this is kept in the school office (see 'Parent Consent Form for use of Pupil Images', Appendix II);.

- Names will not be used to identify individuals portrayed in images uploaded onto the school website. Similarly, if a child or member of staff is mentioned on the website, photographs which might enable this individual to be identified must not appear.

- When photographs to be used on the website are saved, names of individuals should not be used as file names.

Procedures for using mobile phones and Personal Digital Assistants (PDAs)

- Staff are permitted to have mobile phones on school premises. These must be put away during lesson times, switched onto silent mode and only be used for emergencies whilst in lessons. Staff are permitted to use their mobile phone (with discretion) in school during breaks.

- Children are not encouraged to bring mobile phones into school; however, if these are needed for safety reasons (walking home from school, afterschool clubs etc) then they must be either stored in the teacher's desk (locked) or taken to the school office for safekeeping.

- Parents may take still or video footage of their own child/children during school events provided this is for personal use only and will not be uploaded and shared on a public place.

- Children are not permitted to use mobile phones during the school day. Any misuse of a phone during the school day will be dealt with in accordance with appropriately.

Procedures for using wireless games consoles

- Wireless games consoles are not permitted within school.

Procedures for using mobile devices (e.g. iPods)

- Children are not encouraged to bring mobile devices into school; however, if they do then they must be either stored in the teacher's desk (locked) or taken to the school office for safekeeping.
- Staff may use personal mobile devices during lesson time for educational purposes and outside lesson time for personal use (with discretion).
- Use of school mobile devices including iPods is covered by separate policies as appropriate.

Sanctions to be imposed if procedures are not followed

- Letters may be sent home to parents or carers (if applicable). Children may receive a warning with their name recorded in the headteacher's office.
- Users may be suspended from using the school computers, internet or email, etc. for a given period of time / indefinitely.
- Details may be passed on to the police in more serious cases.
- Legal action may be taken in extreme circumstances.

Concluding Statement

The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into school. This policy will not remain static. It may be that staff and children might wish to use an emerging technology for which there are currently no procedures in place. The use of any emerging technology will be permitted upon completion and approval of a risk assessment commissioned by the Headteacher, which will be used to inform future policy updates.

Appendix

I. Pupil and Parent Acceptable Use Guidelines
II. Parent consent form for use of pupil images
III. Staff Acceptable Use Guidelines
IV. Guest Acceptable Use Guidelines