MONKTON INFANTS SCHOOL

Aiming High!

E-Safety and Use of ICT Policy

E-SAFETY AND USE OF ICT POLICY

All adult users of the school network and internet must read and understand the scope of this policy and then sign an Acceptable use agreement before being allowed access to the school services.

Pupil users will agree to acceptable user rules and procedures appropriate to their age range and understanding, with support and monitoring by members of staff.

STATEMENT OF INTENT

At Monkton Infants School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff. The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

LEGAL FRAMEWORK

This policy has due regard to the following legislation, including, but not limited to:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997
- This policy also has regard to the following statutory guidance:
- DfE (2016) ‘Keeping children safe in education’

This policy will be used in conjunction with other safeguarding and computing school policies and procedures.

UNLAWFUL AND ILLEGAL USE

As a user, you agree to use the service for lawful purposes only and not to use the Service to send or receive materials or data, which is:

- In violation of any law or regulation
- Which is defamatory, offensive, abusive, indecent, obscene
- Which constitutes harassment
- Is in breach of confidence, privacy, trade secrets
- Is in breach of any third party Intellectual Property rights (including copyright)
- Is in breach of any other rights or has any fraudulent purpose of effect

You are prohibited from storing, distributing or transmitting or permitting the storage distribution or transmission (whether intentionally or otherwise) of, any unlawful material through the Service.

Examples of unlawful material include:

- Direct threats of physical harm
- Hardcore and child abuse images
- Copyrighted, trademarked and other proprietary material used without proper authorisation

You may not post, upload or otherwise distribute or permit the posting, uploading or distribution (whether intentionally or otherwise) of copyrighted material on our servers without the consent of the copyright holder. You must give acknowledgement to the source wherever such material is used.

In the event that the school, NGFL or BT become aware of any breach of this clause, action may be taken. The storage, distribution, or transmission of unlawful materials could also lead to UK authorities alleging criminal liability.

VIOLATIONS OF SYSTEM NETWORK SECURITY

Any violations of systems or network security are prohibited, and may result in the user facing criminal and civil liability. The school and Northern Grid will investigate incidents involving such violations and will inform and co-operate with the relevant law enforcement organisations if a criminal violation is suspected. The user may be refused access to the network as a result of any breach of security. Violations may include, but are not limited to, the following:

- Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network
- Unauthorised monitoring of data or traffic on any network or system without express authorisation of the owner of the system or network
- Interfering with any user, host or network including mail-bombing, flooding, and deliberate attempts to overload a system and broadcast attacks.

All machines connected to the Northern Grid network must have full up to date and appropriate virus protection. No user should try to remove or alter this software. Any violation will mean immediate removal of access.

No machine should be connected to the internet without protection. Any machine found to be infecting the Local Area Network (LAN) must be immediately disconnected, cleaned and not reconnected to the LAN until fully checked by an authorised school officer.

All users must log in to the school LAN and use the Northern Grid network to access the internet. No other method of access is permitted.

DISCIPLINARY AND RELATED ACTION

The school wishes to promote the highest standards in relation to good practice and security in the use of information technology. Consequently, it expects and supports the integrity of its users. The school system is monitored on a regular basis and any misuse is reported and followed through.

In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow. The school will also assist where necessary should an investigation be called for by the police.

In other instances the user may be restricted from using the service for a period determined by the Head. Disciplinary action may also be taken. All cases of inappropriate use are logged in the E-Safety Log, held in the Office. All cases of sites deemed inappropriate by the school and the action taken are also held on file.

USE OF THE INTERNET

The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.

When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual’s consent or knowledge

ROLES AND RESPONSIBILITIES

- It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.
- The governing body is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.
- The Headteacher, is responsible for ensuring the day-to-day e-safety in the school, and managing any issues that may arise.
- The Headteacher is responsible for chairing the e-safety committee.
- The Headteacher will organise all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.
- The Headteacher will ensure there is a system in place to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.
- The School Business Manager (SBM) will regularly monitor the provision of e-safety in the school and will provide feedback to the Headteacher.
- The Headteacher will maintain a log of submitted e-safety reports and incidents.
- The Headteacher will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.
- The Headteacher will ensure that all members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded.
- The Designated Governor will hold termly meetings with the Headteacher and SBM to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school’s duty of care.
- The SBM will evaluate and review this E-Safety Policy on an annual basis, taking into account the latest developments in ICT and the feedback from staff/pupils.
- The Headteacher will review and amend this policy with the SBM, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.
- All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-Safety Policy.
- All staff will ensure they understand and adhere to our Acceptable Use Agreement, which they must sign and return to the SBM.
- Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.
- The Headteacher is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.
- All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

E-SAFETY COMMITTEE

The E-safety Policy will be monitored and evaluated by the school’s e-safety committee on a termly basis. The committee will include a member of the Headteacher, the SBM and the designated safeguarding lead (DSL), as well as a designated member of the governing body.

USE OF ICT FACILITIES

The use of the IT facilities within the school is encouraged, as its appropriate use facilitates communication and can improve efficiency. Used correctly, it is a tool that is of assistance to employees. Its inappropriate use, however, can cause many problems, ranging from minor distractions to exposing the school to financial, technical, commercial and legal risks.

Staff should always be an example of good practice to the students, serving as a positive role model in every aspect.

Abuse of the IT facilities could result in the facilities being removed. Staff should always be aware of IT use, and misuse of the facilities, as defined in this policy, must be reported to the Headteacher. Since IT facilities are also used by pupils, it is the responsibility of staff to ensure they comply with that policy. This policy applies to any computer connected to the school's network and computers. Any breach of the rules in this policy may result in disciplinary action, which may lead to dismissal. A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved or the school.

AUTHORISED USE OF THE IT FACILITIES

The IT facilities should only be used as required by your work duties. This includes, but may not be limited to:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching for any school related task
- Any school encouraged tuition or educational use
- Collating or processing information for school business
- Personal e-mail accounts are only permitted to be used if they have built-in anti-virus protection approved by the IT technician. Access to your personal e-mail must never interfere with your work duties.

If unsure about your required use, please seek authorisation from the Headteacher.

UNAUTHORISED USE OF THE IT FACILITIES

- It is not permitted under any circumstance to:
    - Use the IT facilities for commercial or financial gain without the explicit written authorisation from the Headteacher.
    - Physically damage the IT facilities.
    - Re-locate, take off-site, or otherwise interfere with the IT facilities without the authorisation of the IT technician or Headteacher – *Certain items are asset registered and security marked; their location is recorded by the SBM for accountability. Once items are moved after authorisation, staff have a responsibility to notify the SBM of the new location.*
    - Use or attempt to use someone else's user account – *All users of the IT facilities will be issued with a unique user account and password. The password must be changed at regular intervals. User account passwords must never be disclosed to or by anyone. This is illegal under the Computer Misuse Act.*

- **Use the IT facilities at any time to access, download, send, receive, view or display any of the following:**
  - Any material that is illegal
  - Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
  - Remarks relating to a person's sexual orientation, gender assignment, religion, disability or age
  - Online gambling
  - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
  - Any sexually explicit content
- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
- Install hardware or software without the consent of the IT technician or the Headteacher.
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the IT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the school's computers. This is illegal under the Computer Misuse Act.
- Use or attempt to use the school's IT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.
- Purchase any IT facilities without the consent of the IT technician or Headteacher. This is in addition to any purchasing arrangements followed according to school policy.
- Use or attempt to use the school's phone lines for internet or email access unless given authorisation by the Headteacher. This includes using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.
- Use any chat-lines, bulletin boards or pay-to-view sites on the internet. In addition, you must not download or attempt to download any software.
- Use the internet for any auctioning activity or to purchase items unless given authority to do so by the Headteacher. This is in addition to any purchasing arrangement followed according to school policy.
- Knowingly distribute or introduce a virus or harmful code onto the school's network or computers. Doing so may result in disciplinary action, including summary dismissal.
- Use the IT facilities for personal use without the authorisation of the Headteacher. This authorisation must be requested on each occasion of personal use.
- Copy, download or distribute any material from the internet or e-mail that may be illegal to do so. This can include computer software, music, text, and video clips. If it is not clear that you have permission to do so, or if the permission cannot be obtained, do not do so.
- To obtain and post on the internet, or send via e-mail, any confidential information about other employees, the school, its customers or suppliers.
- Interfere with someone else's use of the IT facilities.
- Be wasteful of IT resources, particularly printer ink, toner and paper.
- Use the IT facilities when it will interfere with your responsibilities to supervise students.
- Any unauthorised use of e-mail or the internet is likely to result in disciplinary action including summary dismissal.
- If you are subjected to, or know about harassment or bullying, you are encouraged to report this immediately to your line senior or the Headteacher.

E-SAFETY CONTROL MEASURES

INTERNET ACCESS

- Pupils have restricted/limited access to the internet when using IT equipment for educational research and apps etc.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- The governing body will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the Headteacher.
- All school systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
- Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.
- Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only, and prohibited from using any personal devices.

EMAILS

- The school email system and internet connection are available for communication and use on matters directly concerned with school business.
- Staff will be given approved email accounts and are only able to use these accounts.
- The use of personal email accounts to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other staff or third parties via email.
- Staff members are aware that their email messages are not monitored.
- If any email contains confidential information, the user must ensure that the necessary steps are taken to protect confidentiality. The school will be liable for any defamatory information circulated either within the school or to external contacts.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.
- The school email system and accounts must never be registered or subscribed to SPAM or other non-work related updates, advertisements or other personal communications. School email addresses should not be shared without confirming that they will not be subjected to SPAM or sold on to marketing companies.
- Non-text e-mails (containing graphics or colour) and e-mail attachments may contain harmful materials and computer viruses, which can seriously affect the IT facilities. If unsure, seek assistance or approval from the IT technician.
- All e-mails that are sent or received must be retained within the school for a period of six months.
- Offers or contracts sent via e-mail or the internet are as legally binding as those sent on paper. An exchange of e-mails can lead to a contract being formed between the sender, or the school, and the recipient. Never commit the school to any obligations by e-mail or the

internet without ensuring that you have the authority to do so. If you have any concerns, contact the Headteacher.

- Online purchases are only permitted by the SBM, in order to comply with monitoring and accountability. Hard copies of the purchase must be made. This is in addition to any purchasing arrangement followed according to school policy.
- Any failure to follow these procedures satisfactorily may result in disciplinary action, including summary dismissal.

PASSWORDS

- All users must log in to the school LAN and the internet using user name and password provided. These must be kept secure, and no-one should give their user details to another to use. Any limitations in log in should be notified to the network administrator immediately. Breach may mean access is denied. Even the youngest pupils should be encouraged to have individual user names and passwords appropriate to their age.
- Access to the LAN will be granted at various levels deemed appropriate to the level of need of the user, i.e. pupils, and most staff will have a lower access level granted than the SBM and technician.
- Any work conducted on the network must be supervised by technician, SBM or agent of the NGFL or Local Authority. All software must be installed by an authorised person or their agent.
- **Users should not share logins or passwords. Passwords should be changed regularly.** All passwords should be complex in nature including capitals, lowercase, symbols and numerals. The more complex the password the more protection you are providing. Passwords should be between 8-10 characters using single letters. A phrase password, which includes spaces, may be easier to remember.
- All machines should be locked or logged out when unattended. Staff should also follow the policy of the school for security of the premises and equipment on it.

STAFF LEAVING THE SCHOOL NETWORK

- Logins will be cancelled within 1 month. Files should be transferred to the new staff member if appropriate. Files will be stored for a short while, 3 months, then deleted if not useful.
- Learning platform account and e-mail will be disabled the official staff leaving date. Any useful documents will be transferred to an appropriate staff member.
- Portable devices need to be thoroughly checked for inappropriate content, malware, illegal copies etc. prior to being made available to other users.
- Files, programs, data - ensure none are taken away from the school if the copyright is only for the institution.
- Images – no teacher can take images of pupils away from the school when they cease to be employed by the school.
- ‘Shared Accounts –change any shared service passwords such as administrator accounts on servers, printers and network devices if necessary.
- Service contracts and web sites where the employee is a named contact will need to be updated.

STORAGE OF INFORMATION

- Digital images may only be stored on the LAN in recognised files. These will be detailed with date and title of school event. Should users need to store images in local document folders these will be kept to a minimum and kept public. No images will be stored in private or password protected areas of the network.
- School images stored on teacher laptops will also be in an identifiable folder clearly visible on the desktop. Images will be kept for teaching purposes only. Any publication of images will conform to the school policy. Individuals will not be identifiable by name or year group unless parental permission is obtained. Work may be identified by Christian name and year group only, however it should preferably remain anonymous.
- Data files, resources and planning files will be stored in clearly labelled folders and handed over if the member of staff leaves. Storage of pupil information follows guidance in the data protection act. Files may be transferred on USB sticks only if the USB stick has been encrypted. Files should be uploaded to named folders and not remain on USB sticks for more than 1 month.

WORLD WIDE WEB USAGE

- All access to the Internet is filtered via a Cachepilot or a similar proxy server.
- The school monitors internet sites visited and may prohibit access to some sites deemed unacceptable or inappropriate; this includes pornography sites or any sites that promote radicalisation.
- All Internet usage from the Northern Grid network is monitored and logged and a log is kept of all sites visited. When specific circumstances of abuse warrant it, individual web sessions will be investigated and traced to the relevant site and user account. Such an investigation may result in action and possibly criminal investigation.
- Copyrights and licensing conditions must be observed when downloading software and fixes from the web sites of authorised software suppliers. Such files must never be transmitted or redistributed to third parties without the express permission of the copyright owner.
- The laws of all nation states, regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax, apply equally to on-line activities.
- Documents or material must not be published or accessed on the web which are defamatory or which may constitute intimidating, hostile or offensive material on the basis of sex, race, colour, religion, national origin, sexual orientation or disability under the sovereign law of the country in which the web server hosting the published material is sited.

IMAGES

- Any images that involve children must not identify children by name and permission must have been agreed by the subject and/or relevant parent / carer before posting. The photos should then be stored in a safe area within the school LAN and only used for legitimate educational purposes as directed by the Headteacher
- Download images from camera/memory card/mobile device to a LAN secure shared area and store in a clearly labelled folder. This must be done within seven days.
- Delete original images on camera or other device prior to it being taken off site.

- Before using images in other media (e.g. email, online, paper based and other collateral) ensure permission given covers intended use.
- Equipment must not be available for further use until images have been transferred/deleted.
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- 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.

MOBILE DEVICES AND HANDHELD COMPUTERS

- Mobile devices are not permitted to be used during school hours by pupils or members of staff.
- Staff are permitted to use Laptops which have been provided by the school.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Mobile devices will not be used to take images or videos of pupils or staff.
- The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

SCHOOL WEBSITE

- The Headteacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take pictures, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

TECHNICAL - INFRASTRUCTURE/EQUIPMENT, FILTERING AND MONITORING

Technical security features, virus software, filters and downloads are kept up-to-date and managed by the technician and the Local Authority through the school's Service Level Agreement. It is the responsibility of the school to ensure that the service provider carries out all the e-safety measures that would otherwise be the responsibility of the school, as suggested below.

- 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 are implemented.
- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the NGfL Security Policy and Acceptable Usage Policy and any relevant 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 must be securely located and physical access restricted.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe).
- Remote management tools are used by technical staff to control workstations and view users activity.
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager (or other relevant person).
- 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.

ACCESS TO INAPPROPRIATE MATERIAL AND REPORTING

Should a user access a site that they deem to be inappropriate by accident they should inform the Headteacher who will then inform the LA. Pupils should activate screening software immediately (Hector Protector). The site will be recorded in the e-safety log and filtering adjusted if necessary. Do not show anyone the content or make public the URL. If reporting a URL do not copy and paste, type the address.

Users must report and a log made of all e-safety concerns such as access to inappropriate sites, unacceptable e-mail and any instances of cyber-bullying. The report will be made to the Headteacher who will then decide whether the incident should be progressed further in accordance with guidance issued by the LA.

MISUSE BY PUPILS

- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the Headteacher, using a Complaints Form.
- Any pupil who does not adhere to the school's e-safety rules and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the Headteacher and will be issued once the pupil is on the school premises.
- Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection and Safeguarding Policy.

MISUSE BY STAFF

- Any misuse of the internet by a member of staff should be immediately reported to the Headteacher, using a Complaints Form.
- The Headteacher will deal with such incidents in accordance with the Allegations of Abuse against Staff Policy, and may decide to take disciplinary action against the member of staff.
- The Headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

USE OF ILLEGAL MATERIAL

- In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.
- Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.
- If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL and Headteacher will be informed and the police contacted.

SOCIAL NETWORKING

- Use of social media on behalf of the school will be conducted following the processes outlined in our Social Media Policy.
- Access to social networking sites will be filtered as appropriate.
- Pupils are regularly educated on the implications of posting personal data online outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school which may affect its reputability.
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the Headteacher prior to accessing the social media site.

CYBER BULLYING

For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

- The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

- The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.
- Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.
- The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.
- Reporting misuse
- Monkton Infants School will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement / Behaviour Policy, ensuring all pupils and staff members are aware of what behaviour is expected of them.
- Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

E-SAFETY EDUCATION

PUPILS

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / 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 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.

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

- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.
- A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- PSHE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Pupils 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.
- Pupils should be helped to understand the need for the student / 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.
- Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens

- Staff should act as good role models in their use of ICT, the internet and mobile devices.
- Clear guidance on the rules of internet use will be presented in all classrooms.
- Children to take part in Kidsafe programme in which a session covers E-Safety aspects.
- The school will hold e-safety events, such as Safer Internet Day and Anti Bullying Week, to promote online safety.

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 / 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 will therefore seek to provide information and awareness to parents and carers through:

- Information on E-Safety sessions held at the Openzone Learning Centre
- Letters, newsletters, web site, VLE
- Parents evenings
- E-safety parents meetings in school

STAFF

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

- A planned programme of formal 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. It is expected that some staff will identify e-safety as a training need within the performance management process.
- 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 Policy
- The SBM (or other nominated person) will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.

GOVERNORS

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

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