



E – Safety Policy

March 2021

Mersea Island School

Barfield Road, West Mersea, Colchester, Essex, C05 8QX
Tel: 01206 382736

Email: office@merseaschool.org

Website: www.merseaschool.org



Background

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives within the wider community. 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 requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This E-Safety policy should help to ensure safe and appropriate use. The development and implementation of this policy should involve all the stakeholders in a child's education from the Head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of the internet, with its 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 environment.

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 with others, including strangers*
- *Cyber-bullying / Mobile Phone bullying*
- *Access to unsuitable video and internet games*
- *An inability to evaluate the quality, accuracy and relevance of information on the internet*
- *Plagiarism and copyright infringement*
- *Illegal downloading of music or video files*
- *The potential for excessive use which may impact on the social and emotional development and learning of the young person*

Many of these risks reflect situations in the off-line world and it is essential that this E-Safety policy is used in conjunction with other school policies (e.g. Behaviour, Anti-Bullying, and Acceptable Use and Safeguarding policies).

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 school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The E-Safety policy that follows explains how we intend to do this, 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.

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 ICT systems/Wi-Fi connection, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of 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:

Governing Body:

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 at a termly Safeguarding meeting.

Head teacher and SLT:

- The Head teacher 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 all of the safeguarding leads.
- The Head teacher is responsible for ensuring that all relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues.
- The Head teacher and another member of the Senior Leadership Team 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.

ICT Technician and Computing Coordinator:

As well as an ICT Coordinator, the school has a managed ICT service provided by PEP. The ICT Technician and Computing Coordinator are both responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the E-Safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- That they keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant

Teaching and Support Staff:

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.
- They report any suspected misuse or problem to a safeguarding Officer for investigation.
- Digital communications with pupils should be on a professional level
- 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

Safeguarding Leads:

The Safeguarding Leads 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 Policy.
- 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
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking of images and on cyber-bullying.
- Should understand the importance of adopting good E-Safety practice when using digital technologies out of school.

Parents and Carers:

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and/or mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and website.

Parents and carers will be responsible for:

- Endorsing the Pupil Acceptable Use Policy

Community Users:

Community Users who access school ICT systems and/or websites part of the Extended School provision will be expected to sign a Staff User Acceptable Use Policy before being provided with access to school systems. They will have access to a guest Wi-Fi code.

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 should be provided as part of Computing, PHSE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key E-Safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities including Internet Safety Day
- 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 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

Education - Parents and 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 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:

- Letters, newsletters, social media and the school website, Parents evenings

Education - Staff Training

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:

- 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

All Teaching and Support staff will complete a yearly Online Safety course.

- The E-Safety Coordinator will receive regular updates through attendance at training sessions
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings and INSET days

Training - Governors

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

- Attendance at training provided by the Local Authority and National Governors Association
- Participation in school training sessions for staff or parents

Technical - Equipment Filtering and Monitoring

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School ICT systems will be managed in ways that ensure that the school meets the E-Safety technical requirements outlined in the Acceptable Use Policy
- 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
- All users will have clearly defined access rights to school ICT systems
- All users will be provided with a username and password
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school maintains and supports the managed filtering service
- Any filtering issues should be reported immediately to the ICT Technician/Computing Coordinator
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy
- Actual and/or potential E-Safety incident to be reported to the Safeguarding leads
- 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
- The school infrastructure and individual workstations are protected by up to date virus software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secure

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.
- Pupils should be taught in all lessons to be critically aware of the 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

Use of digital and video images

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. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. 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 they should recognise the risks attached to publishing their own images on the internet
- Staff are allowed to take digital and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital and video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupils' full names will not be used anywhere on a website or social media, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers

Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR 2018), which states that personal data must be:

- Processed Fairly, Lawfully and Transparently
- Processed for a Specified and Legitimate Purpose
- Adequate, Relevant and limited to what is relevant
- Accurate and up to date
- Kept no longer than necessary
- Stored securely using technical and organisational measures

Staff must ensure that:

- All electronic devices are password-protected to protect the information on the device in case of theft
- Where possible, the school will enable electronic devices to allow the remote blocking or deletion of data in case of theft
- All staff will be provided with their own secure login and password and every computer regularly prompts users to change their password
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipients
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients
- Before sharing data, staff will ensure they are allowed to share it, that adequate security is in place to share it and that who will receive the data has been outlined in a privacy notice

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

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- Memory sticks will not be used to hold personal information, unless they are Password-protected and fully encrypted
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- The official school email service is regarded as safe and secure and is monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and parents or carers (email) must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or public chat and social networking programmes must not be used for these communications. Teaching staff should only communicate with parents through the class email account and not from their personal accounts.
- 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.

Through our home/school links and communication channels, parents are kept up to date with relevant online safety matters, policies and agreements. They know who to contact at school if they have concerns.

Monitoring of Use

All internet activity is logged by the school internet provider.

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.

If any apparent or actual misuse appears to involve illegal activity. For example:

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

The police will be contacted immediately and staff member removed from post.

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.

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 and disciplinary procedures.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary actions in accordance with the schools Disciplinary Procedure or, where appropriate, the Essex County Council Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.