E-Safety Policy

Background

New technologies have become integral to the lives of children and young people in today's society, both educationally and socially.

The internet and other digital technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps staff and pupils learn from each another. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

The requirements to ensure that young people are able to use the internet and related communications appropriately and safety is addressed as part of the wider duty of care to which we all work. This e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education plus the child themselves.

The use of these exciting and innovation tools in educational establishments and home has been shown to raise educational standards and promote pupil/student achievement. However, the use of these technologies can put young people at risk within and outside educational establishments. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of /sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication /contact with others, including strangers
- Cyber bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloads of music or videos
- 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 policies (eg behaviour, anti bullying and child protection).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build young peoples' 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.

Scope of the policy

This policy applies to all members of ## who have access to and are users of schools ICT systems, both in and out of the school.
The Education and Inspection Act 2006 empowers Headteachers, to such extent as reasonable, to regulate the behaviour of pupils when they are off the unit 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 the policy, which may take place out of the school but is linked to membership of the school.

The school will deal with such incidents within the policy and associated behaviour and anti bullying policies and will, where known, inform parents/carers of the incident.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current e-safety policy
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Headteacher
- Digital communication with pupils (email) 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 units 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 and extra curricular 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 lesson where internet use is pre-planned students/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

The Child Protection Co ordinator is trained in e-safety issues and is aware of the potential for serious child protection issues that arise from:

- Sharing of personal data
- Access to illegal/inappropriate material
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils should:

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance if reporting abuse, misuse or access to inappropriate material and how to do so
- Should understand the importance of adopting good e-safety practices when using digital technologies out of the unit and realise that the unit E-safety policy covers their actions out of school

Policy Statement

Education – pupils

Whist regulation and technical solution are very important their use must be balanced by educating pupils take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's provision. Children and young people need the help and support of the school to recognise and avoid e-safety risk and build their resilience.

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

- Key e-safety messages should be reinforced as part of a planned programme
- Pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Rules of use of ICT systems will be posted in all rooms
- Staff should act as good role models in their use ICT, the internet and mobile devices

Education – 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 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.

Curriculum

E-Safety should be a focus in all areas of the curriculum and staff should reinforce e-safety message in the use if ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the website the pupil visits

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they:

- At all times take care to ensure that safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged off' at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored
- Users need to be aware that email communication may be monitored
- User must immediately report to the nominated person – in accordance with the school policy, the receipt of any emails that makes them feel uncomfortable, offensive, threatening or bullying in nature and must not respond to any such emails
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content
- Pupils should be taught about email safety issues, such as the risk 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.