E-Safety Policy

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 outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. 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.

However, the use of these new technologies can put young people at risk within and outside the school. 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 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.

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 E Safety Committee

Ben Heritage – E-Safety Leader /Named Person/ Computing strand team lead
Rav Kaur – PHSE Strand team lead /Named Person
Jemma Gordon, Tracy Harp, Beth Horrocks– Computing Strand team

Monitoring the impact of the policy

The school will monitor the impact of the policy using

- Logs of reported incidents in the e safeguarding incident log/ CPOMS
- Internal monitoring data for network activity
- Should any issue occur the filtering logs from EXA Networks can be checked
- Student e-safety data will be gathered through the use of the E-safety Logbook.

Roles and Responsibilities

Governors:

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 School Improvement Committee receiving regular information about e-safety incidents and monitoring reports.

The role of the governors will include meeting with the E-safety Committee where:

- e- safety issues will be discussed
- e-safety incident logs will be monitored at Welfare committee
- EXA Networks filtering logs will be monitored

Head teacher and Senior Leaders:

- The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community.
- The Head teacher is responsible for ensuring that relevant staff receives suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head teacher is aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. This is detailed in the Child Protection and Safeguarding Policy.

Safeguarding Leader

- takes day to day responsibility for e-safeguarding issues and has a leading role in establishing and reviewing the school e-safeguarding policy.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- attends all Governors Committee meetings (which discusses e safeguarding issues).

Network Manager / Technical staff:

Calderdale Council - the school technician ensures:

- that the school's IT infrastructure is secure and is not open to misuse or malicious attack
- that they keep up to date with e-safety technical information and updates the E Safety leader or Computing coordinator as relevant.
- that monitoring software and anti- virus software is implemented and updated

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
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety leader
- digital communications with pupils should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities. E Safety lessons are taught through the 'Rising Stars 'Switched On' scheme. E safety assemblies are delivered at the beginning of each year (to Key Stage 1 and Key Stage 2) and the SMART rules are used throughout school. E safety poster competitions are also held. Our PSHE (SCARF) curriculum encompasses all e safety messages.
- pupils understand and follow the school e-safety and acceptable use policy
- 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

Named person for child protection

- Dan Burns, Emma Dixon and Jane holden are the named people for child protection. (DSL's)

They are trained in e-safety issues and to 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

Children

- are responsible for using the school Computing systems in accordance with the Pupil Acceptable Use Policy.

Parents / Carers

The school will take every opportunity to help carers / parents to understand issues related to e safety. We will assist parents to understand key issues in the following ways:

A parent's E safety presentation takes place periodically.

Our school web site http://www.oldearth.co.uk has links to e-safety guidance and also the 'Green Button' for children to report any concerns they may have.

Parents are asked to discuss the pupil Acceptable use policy with their children.

Regular twitter updates and articles in the newsletter keep parents abreast of e-safety issues.

Education – Pupils

The education of pupils in e-safety is 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:

- The Rising Stars 'Switched On' Scheme of work highlights e Safeguarding issues that arise in the context of Computing lessons.
- Key e-safety messages are reinforced as part of a planned programme of assemblies
- Pupils are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information. Validation of information is covered in the research strand of the Rising Stars 'Switched On' scheme of work.
- Rules for use of Computing systems will be posted in all classrooms alongside the 'SMART' rules
- 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. Evaluation and cross referencing of sources is covered in the research strand of the Switched On scheme of work which the school follows.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Copyright free audio and image sources are detailed in the Multimedia and Sound strands of the Rising Stars 'Switched On' scheme of work which the school follows.

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:

- An audit of the e-safety training needs of all staff will be carried out regularly.
- 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.

Internet Provision

The school Internet is provided by the EXA Networks. All sites are filtered using strict filtering systems which generates reports on user activity.

Use of digital and video images - Photographic, Video

- 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 online.
- Staff are allowed to take digital / video images to support educational aims. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Photographs of children published on the website or blog must not contain names.
- Parents are asked to inform the head teacher if they do not want their children to be photographed for inclusion on any school publication (paper or online)

Personal Data Protection

Staff must ensure that they:

- At all times take care to ensure the 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 such as memory sticks.

Passwords

- All users (adults and young people) will have responsibility 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.

- Passwords for new users and replacement passwords for existing users can be allocated by Calderdale Council.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in Computing and / or e-safety lessons
- through the Acceptable Use Agreement

All users (at KS2 and above) will be provided with a username and password by Calderdale Council/Ben Heritage who will keep an up to date record of users and their usernames. Tracey Sharp will keep an up to date record of passwords for the school's Purple Mash and Education City accounts.

Updated: September 2022