E Safety Policy

Governor responsibility	Academic
Owner/Author	Headteacher
Date & version	September 2023
Next review date	September 2024

Scope

This guidance is applicable to all those involved in the provision of e-based education/resources at the school and those with access to / are users of the school ICT systems.

Objectives

- To ensure that pupils are appropriately supervised during school activities.
- To promote responsible behaviour with regard to e-based activities.
- To take account of legislative guidance, in particular the UK General Data Protection Regulations and the Data Protection Act 2018.

Guidance

The Bursar / Head Teacher will be responsible for the implementation of this policy.

The Bursar will act as E- Safety Co-ordinator and will:

- compile logs of e-safety incidents;
- report to the Head Teacher on recorded incidents;
- ensure that staff are aware of this guidance;
- provide / arrange for staff training;
- liaise with school technical staff;
- liaise with the Head Teacher on any investigation and action in relation to e-incidents; and
- advise on e-safety policy review and development.

The School ICT Co-ordinator/Network Manager will:

- be responsible for the IT infrastructure and that it is not open to misuse or malicious attack;
- ensure that users may only access the networks and devices through an enforced password protection policy;
- keep up to date with e-safety technical information in order to carry out their role;
- ensure that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse; and
- implement any agreed monitoring software / systems.

Teaching and Support Staff will:

- maintain awareness of school e-safety policies and practices;
- report any suspected misuse or problem to the Head Teacher or E-Safety Co-ordinator;
- ensure that all digital communications with pupils / parents / carers/ fellow staff are on a professional level and conducted on school systems;
- where relevant e-safety is recognised in teaching activities and curriculum delivery;
- ensure pupils understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
- monitor the use of digital technologies (including mobile devices, cameras etc during school activities; and

- ensure that where the use of the internet is pre-planned, pupils are 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.

Child Protection/Safeguarding

- Those responsible should be trained in e-safety issues and aware of the implications that may arise from:
- sharing of personal data;
- access to illegal / inappropriate materials;
- inappropriate contact on-line with adults / strangers;
- potential or actual incidents of grooming; and
- cyber-bullying.

Pupils

- are responsible for using school digital technology systems in accordance with the school acceptable use policy;
- will understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
- will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- are expected to understand policies on the use of mobile devices and digital cameras, the taking / using of images and cyber-bullying; and
- will understand that the e-safety policy will include actions outside of school where related to school activities.

Parents / Carers

- will be encouraged to support the school in the promotion of good e-safety practice; and
- should follow school guidelines on:
    - digital and video images taken at school events;
    - access to parents' sections of the school website / pupil records; and
    - their children's / pupils' personal devices in the school (where this is permitted).

Community Users / Contractors

- Where such groups have access to school networks / devices, they will be expected to provide signed acceptance to abide by school e-safety policies and procedures.

Associated policies

- Safeguarding Policy
- Behaviour Policy
- Anti-bullying Policy
- AI Policy
- SEND Policy

School Policies | Moon Hall School (moonhallschoolreigate.co.uk)

Advisory Guidance

Teaching online safety in schools - GOV.UK (www.gov.uk)
E-safety for schools | NSPCC Learning
Love Life: resources for young people with learning disabilities | NSPCC Learning

Appendix

Online Safety for Learners with SEND (kelsi.org.uk)

Ashley Assiter, Online Safety Development Officer
Rebecca Avery, Education Safeguarding Advisor (Online Protection)
Education Safeguarding Service, The Education People, November 2018

Online Safety for Learners with Special Educational Needs and Disabilities (SEND)

What is different for learners with SEND?

The internet and technology are an integral part of everyday life for children. It is important that we acknowledge the positive opportunities the internet provides for young people with Special Educational Needs and Disabilities (SEND); the accessibility of images and video online make it an excellent learning tool, whilst global connectivity enables children with SEND to socialise and access support.

However, children with SEND are more likely than their peers to experience online issues such as cyberbullying, online grooming and exploitation. Similarly, children with SEND are more likely to have their internet use restricted and therefore have limited opportunities to learn through experience, develop resilience or seek support, which would empower them to use technology safely.

Online safety is a fundamental part of our safeguarding responsibilities and education settings should implement a range of targeted and differentiated strategies to enable learners with SEND to access the internet safely and appropriately.

Online safety messages

For some learners, the use of abstract language and concepts can lead to confusion, frustration and misunderstandings. It is important that settings work together with their learners to build and develop a collaborative understanding of the terminology being used.

Consider:

- *What does the term 'online predator' mean to a child with SEND? Is it a dangerous person or a wild animal?*
- *Isan online contact still a stranger if you know their name or they send a 'friend request'?*
- *If you must never share personal information online, how do you tell online shops where to deliver your orders?*

Be mindful that there are usually exceptions to rules which can sometimes be difficult for children with SEND to accept; ensure the 'rules' you provide are clear, consistent and not left open to interpretation.

Examples:

- *A learner who finds it difficult to understand abstract meaning may not be able to interpret hidden messages or metaphors in many popular video resources.*
- *Instead of saying: "Don't share personal information online", consider a more realistic statement: "Always ask your trusted adult, before sharing personal information online".*

Education and training

Online safety education should be delivered in an age and context appropriate way, based on learner needs and experiences. Staff should establish what learners already know about online safety and how much experience or exposure they have to the online environment.