Settle and Malhamdale Partnership

E-SAFETY POLICY

Contents

Introduction:

Computing and the use of digital devices is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people, and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing and ICT covers a wide range of resources including, web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of computing within our society as a whole. Currently, the apps and software children and young people are using both inside and outside of the classroom include:

- Websites
- Coding
- Gaming
- Video & Multimedia
- Mobile devices
- Podcasting/Video Blogs

Whilst exciting and beneficial, all users need to be aware of the range of risks associated with the use of these technologies.

At Settle CE Primary School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviour and thinking skills to enable them to remain both safe and legal when using the internet and related technologies.

Both this policy and the Acceptable Use Agreements (for all staff, governors, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the school. Any visitors using their own devices within school adhere to the schools Acceptable Use Agreement and this e-safety policy.

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-safety co-ordinators who oversee safety at the school are Mrs Helen Wright (Computing Lead) and Miss Sarah Entwistle (STEM Lead) at Settle Primary and Mr Richard Wright and Mrs Amanda

Allen (Kirkby Malham Primary) – we also buy into County's ICT Services and receive additional support and guidance from our technician Mr Richard Freytag.

This policy, supported by the school's acceptable use agreement (we use an LA Approved Template provided by Veritau), in order to protect the interests and safety of the whole school community. It is linked to the following school policies: computing, child protection, behaviour, health and safety, anti-bullying and PHSE.

Managing the School E-Safety Messages

We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used. These messages will be appropriate to the age of the children being taught. The following areas facilitate the sharing of our e-safety messages in school:

- E-safety SMART rules will be prominently displayed around the school.
- The school provides opportunities within a range of curriculum areas to formally teach esafety.
- Educating pupils on the dangers of technologies that may be encountered, including outside school, is done informally when opportunities arise and as part of the computing e-safety curriculum.
- The teaching of e-safety focuses on helping children to recognise inappropriate content, conduct, contact and commercialism and helps them learn how to respond or react appropriately.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues.
- Pupils know how to seek advice or help if they experience problems when using the internet and related technologies i.e. parent/carer/ teacher/ trusted staff member, or an organisation such as Childline.

Security, Data and Confidentiality

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety policy.

When accessing, amending, and saving any data or information relating to the school or pupils, school staff follow the guidelines set out in the General Data Protection Regulations 2018.

Managing the Internet

All internet activity within school is monitored and filtered through the North Yorkshire Firewall system. Whenever any inappropriate use is detected, the ICT technician and DSL (designated leader for the school M r Wright) is notified, and the incident will be followed up in line with the school's Acceptable Use Policy.

The school maintains supervised access to internet resources (where reasonable) through the school's digital devices.

If internet research is set for homework, staff will remind students of their e-safety training. Parents are encouraged to support and supervise any further research.

Infrastructure

Our internet access is provided by North Yorkshire County Council.

North Yorkshire County Council manage the administrative devices throughout school and curriculum access is managed by the school's ICT Manager.

Staff and students are aware that should they encounter or access anything unsuitable or damaging they must report it immediately to teachers or e-safety co-ordinator.

Mobile Technologies

The school allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom. **These should not be used whilst children are present**.

The school is not responsible for the loss, damage, or theft of any personal mobile device.

Use of Emails

The use of email within school is an essential means of communication for staff. Staff must use the school's approved email system for any school business and should regularly monitor both their individual school email account and the class email account (where appropriate).

Staff must inform the e-safety co-ordinator/line manager if they receive an offensive or inappropriate e-mail.

Pupils currently do not access individual email accounts within school.

Social Networking

The school does not permit pupils to access their private accounts on social media or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of school.

Should the staff be made aware of incidents or activities on these social networks, which has a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the relevant organisations/companies.

Safe Use and Storage of Images

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

All staff are aware of specific children (they have responsibility for) in school which do or do not have photograph permissions. If they do have permission, staff are aware of which platforms they can be used on.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes field trips. School's own mobile devices must be used in this case.

Images/films of children are stored securely on the school server and/or on school staff's individual school laptops/login areas.

Publishing Pupil's Images and Work

All parents/guardians will be asked to give permission for the use their child's work/photos in publicity materials on the school website, social media accounts, or other public places.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. Parents/carers may withdraw or amend permission, in writing, at any time. Only pupils' first names will be published alongside their image and vice versa on the school website, social media accounts, or any other school-based publicity materials.

Misuse and Infringements: Complaints

Complaints or concerns relating to e-safety should be made to the e-safety coordinator or DSL/headteacher.

Misuse and Infringements: Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the teacher, e-safety leads or head teacher.

Deliberate access to inappropriate materials by any user will lead to the incident being logged, in the first instance, by North Yorkshire County Council and then forwarded to the e-safety co-ordinator. Depending on the seriousness of the offence, investigation may be carried out by the head teacher or Local Authority. Staff are aware that negligent use or deliberate misconduct could lead to disciplinary action.

Equal Opportunities: Pupils with Additional Needs

- The school partnership endeavours to deliver a consistent message to parents and pupils regarding the school's e-safety rules.
- Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.
- Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety.
- Internet activities are planned and well-managed for these children and young people.

Reviewed Autumn 2025
Next Review Autumn 2025