Sedbergh Primary School

E-Safety Policy – November 2016

This policy was written/updated in collaboration with school staff and should be read in conjunction with the following policy documents;

- Child Protection Policy
- Teaching and Learning Policy
- SEN (including most able) Policy
- Single Equalities Policy
- Home School Partnership Agreement
- Pupil acceptable use agreement
- Staff acceptable use agreement
- Incident log
- E-Safety scheme of work
- Behaviour Policy (including Anti-Bullying)

Approved by: *Sophie Lawson* **Date:** *28.11.16*

Review Date: *November 2018*

Our School Aims & Vision

- ✓ To embrace individuality, teach independent learning, nurture resilience and help pupils develop transferable skills.
- ✓ To provide a balanced and varied curriculum, that makes learning exciting, challenging and enjoyable for all.
- ✓ To further develop our school family feeling and positive community links, with an awareness and respect for diversity.
- ✓ To develop a more holistic approach to continuity and progression in learning across the school.
- ✓ To challenge every child to achieve their full potential.

Our highly committed and valued staff, working in partnership with parents, governors and all stakeholders, will ensure Sedbergh Primary is a place where:

- ✓ Effective teamwork forms the basis of a professional and motivated staff who always put children first
- ✓ A caring ethos that nurtures positive relationships, with everybody equally valued, celebrated and proud of their achievements
- ✓ An engaging, relevant and fun curriculum ensures children are well prepared for education, work and life
- ✓ A culture of challenge and high expectation is promoted to maximise individual potential and create an outstanding workforce
- ✓ An awareness of self, community and global issues that fosters responsible behaviour with a respect for British values
- ✓ Children are taught in a stimulating learning environment with high quality resources.

Policy for E-Safety

This document has been written and updated to meet the demands of safety within ICT in the 21st Century. The policy will be reviewed annually or in the event of a significant incident of concern. The ICT/Computing leader is responsible for the overview of E-Safety supported by the Head teacher and the governing body who are responsible for the approval of the policy.

Technical Staff - The school has a managed ICT service provided by Dales Computing Ltd who ensure that the school's infrastructure is secure and not open to misuse or malicious attack and that the school meets the e-safety technical requirement required for the school.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of this document
- They have read, understood and signed the School Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Head teacher
- They teach E-Safety issues (digital awareness) to the children following the scheme of work adopted by the school
- The children understand the internet 'rules' appropriate for their age
- Online video clips will be downloaded and checked by staff before the children see them
- They are aware that Internet use can be monitored and traced to the individual user. Discretion and professional conduct is essential on line

Safeguarding Lead - The Head teacher (DSL) and Deputy Head teacher (DDSL) are responsible for safeguarding/child protection in school. They are also aware of the potential for serious child protection issues that could 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

- Should use the ICT systems in school in accordance with the school rules and acceptable use agreement
- Understand how to report abuse, misuse or access to inappropriate materials
- Should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that this should extend to their actions out of school, if related to their membership of the school

Pupils with Additional Needs

- A fundamental part of teaching E-Safety is to check pupil's understanding and knowledge of general personal safety issues. Some pupils may need additional teaching that includes reminders and explicit prompts to link their existing knowledge of "how to keep safe" to the rules that will apply specifically to, for instance, internet use.

Parents/Carers

The school will take every opportunity to help parents understand the issues connected to E-Safety through newsletters, letters, parents' evenings and the school website. Parents and carers will be responsible for endorsing the Pupil Acceptable Use Contract and ensuring that they themselves do not use the internet/social network sites in an inappropriate or defamatory way. Parents' attention will be drawn to the school E-Safety policy in newsletters and on the school website.

Teaching and Learning at Sedbergh Primary School:

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Pupils will be educated in the effective use of the Internet
- Pupils will be taught how to evaluate Internet information and take care of their own safety and security
- Pupils will be taught how to report unpleasant Internet content e.g. using CEOP or Hector Protector

Information Systems

- School ICT systems security will be reviewed regularly
- Virus protection will be updated regularly
- Security strategies will be discussed with the IT provider

Email

- Pupils may only use approved e-mail accounts for school purposes
- Pupils must immediately tell a member of staff if they receive an offensive e-mail
- Pupils are taught not to reveal personal details of themselves or others in an e-mail communication or arrange to meet anyone without specific permission from an adult
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known

Use of Digital and Video Images

- 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 e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but should only use school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking images that pupils are appropriately dressed
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs on the website or elsewhere will be carefully selected and pupils' full names will not be used
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or in the newspaper. This letter is sent out at the beginning of each year.

Social Networking

- Pupils will not have access to social networking sites at school, but we will educate them in their safe use e.g. use of passwords and not giving out personal information.
- They will be advised never to give out personal details of any kind which may identify them, anybody else or their location
- Pupils will be advised to use nicknames and avatars when using social networking sites

Webcams and CCTV – the school currently does not use webcams and has no CCTV that is operational.

Data Protection – Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Disposal of Redundant ICT Equipment - All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

Policy Decisions – Internet Access

- All staff will read and sign the Staff Acceptable Use Policy before using any school ICT resources
- Parents will be asked to read the sign the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate
- At KS2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher directed where necessary

Assessing Risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use.

Responding to Incidents of Concern - If any apparent or actual misuse appears to involve illegal activity e.g.

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

The following process should take place

- Any concerns such as breaches of filtering, cyber-bullying, illegal content etc. should be reported to the Head teacher who will record the incident and action taken in the School Incident Log, should there be an incident involving Child Protection the Head teacher will take appropriate action
- Parents/Carers will be informed as and when required
- After an incident the school will evaluate and identify lessons learnt and areas for change or improvement
- Any racist incidents will be reported to Children's Services. Racist Incident Monitoring forms should be completed electronically through the School Portal

E-Safety Complaints

All complaints will be dealt with under the School's Complaints Procedure, staff misuse complaints will be referred to the Head teacher.

Cyberbullying

Cyberbullying (along with all forms of bullying) or any member of the school community will not be tolerated. Full details are set out in the Whole School Behaviour Policy. All incidents of Cyber bullying will be recorded.

Use of Personal Devices in school (mobile phones, tablets etc.)

- Staff should not use their own personal phones or devices to contact parents within or outside of the setting in a professional capacity except in an emergency.
- Mobile phones and devices should not be used for personal reasons during teaching periods. Staff are free to use administrative areas of school to make/receive phone calls or use their device at break times.
- Staff should not use their own devices to take photos or videos of pupils and will only use school equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- In addition, any visitors or volunteers in school should not use any personal devices in the presence of children and are not permitted to take photographs.
- Organised visits to school involving third parties who wish to capture images, audio and video for publication purposes will always seek the permission of the Head teacher of Deputy to do so. Third

parties will also comply with parental requests concerning digital marketing and publication in line with school policy

Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school begins to use them.

Communicating this Policy to Children

- Appropriate elements of the E-Safety policy will be shared with pupils
- E-Safety rules will be posted in all networked rooms
- Pupils will be informed that network and Internet use will be monitored
- Curriculum opportunities to gain awareness of E-Safety issues and how best to deal with them will be provided for pupils

Subject Leader: Neal Banner