

# Low Ash Primary School



## School Policy for Online Safety

**Phil Ebbage**

**Online Safety Leader**

**November 2017**

### **Rationale**

In implementing this policy due consideration to equal opportunities, with regard to race, gender, religion and ability, should be ensured with reference to the Race Relations Amendment Act 2000 (as amended) and all other relevant legislation.

ICT plays an important role in the everyday lives of children, young people and adults. As a result, schools need to use these technologies in order to equip children with the skills to access life-long learning and employment.

Information and Communications Technology 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 ICT within society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- websites
- learning platforms and virtual learning environments (VLE)
- email and instant messaging
- chat rooms and social networking
- blogs and wikis
- podcasting
- video broadcasting
- music downloading
- gaming
- mobile/ smart phones with text, video and/or web functionality
- other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Low Ash Primary School we understand the responsibility to educate our pupils on eSafety issues. eSafety is not about blocking or banning children from accessing inappropriate content, but rather, about giving them the skills and the responsibility to make good choices and to know how and when to seek help.

Both this policy, the Acceptable Use Policy and ICT rules for pupils are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by staff, but brought onto school premises (such as laptops, mobile phones and camera phones).

## **Roles and Responsibilities**

As eSafety is an important aspect of strategic leadership within the school, the headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety leader in our school **Phil Ebbage** supported by the eSafety team, which includes teachers, children and a governor.

The Named Governor Safeguarding is responsible for feeding information back to the governors. All members of the school community have been made aware of who holds the eSafety leader post. It is the role of the eSafety team to keep abreast of current issues and guidance through organisations such as Bradford Metropolitan District Council (BMDC), Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

The Senior Leadership Team and Governors are updated by the eSafety team and governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's Acceptable Use Policy for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following school policies: Child Protection and Safeguarding, Health and Safety, PSHCE Policy, Behaviour and Anti-Bullying Policy and Home–School Agreements.

### **eSafety skills development for staff, student teachers and work experience pupils**

- Our staff, including the eSafety named Governor, receive information and training on eSafety issues in the form of staff meetings, INSET and written correspondence.
- New staff, student teachers and work experience pupils receive information on the school's Acceptable Use Policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know to report the misuse of technology by any member of the school community to the Headteacher or eSafety Leader.
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

### **Managing the school eSafety messages**

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- The eSafety policy will be introduced to the pupils at the start of each school year by their class teacher linked to the age appropriate scheme of work. Children are also reminded throughout the year.
- eSafety rules are displayed in the ICT Suite and classrooms.
- A pupil eSafety group will be established each year to evaluate current eSafety education and provision and to suggest improvements.

## **eSafety in the Curriculum**

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. Each ICT topic will include an eSafety teaching element (see long term plan). eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- A scheme of work has been developed for staff to integrate into the curriculum and provides guidance and ideas for the teaching of eSafety.
- Educating Key Stage 2 pupils on the dangers of technologies that may be encountered outside school is done during PSHCE lessons, informally when opportunities arise and as part of the eSafety curriculum.
- Pupils are aware of where 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/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models and discussions.

## **Managing the Internet**

## **Use of the Internet to Enhance Learning**

- The school internet access is designed for pupil use and includes filtering.
- Pupils are taught what internet use is acceptable and what is not.
- Internet access will be planned to enrich and extend learning activities.
- Where possible, staff will preview any recommended sites before use.
- Staff will guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation.

## **Authorised Internet Access**

- All staff must read the Acceptable Use Policy before using any school ICT resource.
- Parents/carers are asked to read and sign the home-school agreement which includes consent for pupils to use ICT and access the internet at school.
- Pupils are asked to sign the home-school agreement which includes following the rules for ICT safety.

## **Internet**

- Our internet is provided by a registered educational internet support provider.
- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the class teacher who will report to the support technician.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up to date on all school machines.

## **Use of blogs, wikis, podcasts and social networking**

The use of public blogs, non-educational wikis, non-educational podcasts and social networking sites (e.g. Bebo, Myspace, Facebook) is not allowed in school.

- School will block/filter access to these sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils are taught not to place personal photos anywhere.
- Staff should not communicate with pupils via any of the above.
- Staff using social networking sites are advised to be aware of the potential audience of their own social networking use and that material posted should be consistent with their professional status and employment at the school. The posting of any material that might be deemed as harmful to the reputation and interests of the school, its staff and pupils could be regarded as a disciplinary matter.

## Mobile technologies

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.
- When pupils bring personal mobile devices/phones to school the devices are kept in the office until the end of the school day.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.

## Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for school business only.
- Under no circumstances should staff contact pupils or parents/carers using personal email addresses.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal their personal details or those of others in e-mail communication, or arrange to meet anyone without specific permission.
- Access by pupils, in school, to external personal e-mail accounts is not permitted.

## Safe Use of Images/Filming

### **Publishing and storing pupils' images, videos and work**

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- *Sporting events, school productions (which could involve parent/carers taking photos/videos). School visits, class photographs, individual photographs, school prospectus, school website. Generally, images taken by staff will not be used alongside pupils names. Photography used by local newspapers tend to include the children's name. Staff will never use their own photographic equipment or record images for their own personal use.*

This consent form is considered valid for the entire period that the child attends this school. Parents/carers may withdraw permission, in writing, at any time.

Images of children should be stored securely on the school's network or a valid encrypted device provided by school (memory stick, laptop) and deleted when no longer required.

Pupils and staff are not permitted to use their own personal digital equipment, including mobile phones and cameras during the normal school hours or during a trip unless it is for school contact purposes.

Parents who attend weekly Achievement Assemblies are reminded (via a slip given by the Office) that images taken should not be posted on social media sites.

### **Published content and the school website and learning platform.**

- Photographs that include pupils will be selected carefully and are only used if parents/carers have given permission through our photographs/filming agreement.
- Pupils' full names will not be used anywhere on the Web site or school Blog, especially in association with photographs.

### **Consent of adults who work at the school**

- Permission to use images of all staff who work at the school will be sought before these are taken.

### **Webcams**

- Some webcam sites may contain, or have links to, inappropriate or adult material. Teachers view any webcam sites or listings before allowing pupils to do so.
- Pupils are alerted to the danger of using web cams as an extension of a chat room. Although this will be highly unlikely at school, pupils need to know the risks involved when using web cams at home.

## **Managing ICT systems and access**

### **Filtering**

The school will work in partnership with the technical support provider (who work closely with Bradford Council) and the internet service provider to ensure filtering systems are as effective as possible. We currently have filtering 'Surf protect'. For example, if you type in certain key words then this is not allowed. There is also a facility to block certain websites eg adult/gaming/gambling websites.

### **Managing Emerging Technologies**

Emerging technologies will be examined by the Computing Leader for educational benefit and a risk assessment will be carried out before use in school is allowed.

### **Information System Security**

- School ICT systems capacity and security will be reviewed regularly. Staff are asked to respect system security and will not disclose any password or security information. They will all use a 'strong' password that contains numbers, letters and symbols, with 8 or more characters.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the technical support provider and internet service provider.

## **Protecting Personal Data**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 (as amended)

## **Assessing Risks**

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate.

## **Equal Opportunities**

### **Pupils with additional needs**

- The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the school's eSafety rules.
- However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.
- Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

## **Parental Involvement**

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school. This will be carried out in the following ways:

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy via eSafety training, governor meetings, parents' questionnaire
- Parents/carers are asked to read and sign the home-school agreement which includes consent for pupils to use ICT and access the internet at school.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain through the Photographs/Filming agreement.
- We will seek to disseminate information and guidance to parents/carers on eSafety through leaflets and information sessions.

These sessions have now developed to include Low Ash children working alongside Titus Salt Secondary students at Parent Consultation Evening, where guidance and support is offered through leaflets and face to face conversations.

# Handling eSafety Complaints

- Complaints of Internet misuse will be dealt with by the eSafety Officers or Headteacher and recorded in the Incident Log (Appendices).
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be reported to the Named Persons for Child Protection (Terry Woollin, Beth Medhurst, Dan Hurst, **Fiona Meer** and Jane Gibson).
- Pupils and parents/carers will be informed of the complaints procedure through the website and distributed eSafety leaflets. Pupils are encouraged to inform their teacher or other adults in school regarding anything which makes them feel uncomfortable while using ICT.

## Communication of Policy

### Pupils

- Rules for Internet access will be posted in all classrooms and the ICT suite.
- Pupils will be informed that Internet use will be monitored.

### Staff

- All staff will be made aware of the school eSafety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

### Parents/carers

- Parents/carers' attention will be drawn to eSafety in newsletters, leaflets, the school prospectus and on the school website.

## Links to Other Policies

- Health and Safety Policy
- Child Protection and Safeguarding Policy
- ICT Policy
- Acceptable Use Policy
- Staff Computer Access Policy
- Behaviour and Anti-Bullying Policy
- PSHCE Policy

## Reviewing this Policy

### Review Procedure

- There will be an on-going opportunity for staff to discuss with the eSafety Team or Named Person for Child Protection any issue of eSafety that concerns them.
- This policy will be reviewed annually and consideration given to the implications for future whole school development planning.
- The policy will be amended if new technologies are adopted or central government change the orders or guidance in any way.

**Reviewed: November 2017 by**

**Signed: .....**

**Next Review Date: November 2018**