Akaal Primary School

E-Safety Policy

January 2018

1. Background

The use of information and communication technologies (ICT), including the Internet, has developed rapidly and now involves every pupil and member of staff. The Internet has become an integral part of children's lives, enabling them to undertake research, talk to friends and access information from a wide range of sources. However, increasing use of the Internet, in and out of school, brings with it the need to ensure that learners are safe. Internet development is constantly evolving into ever more innovative areas, with many websites enabling amazing creativity and interaction between peers. Pupils interact with new technologies, such as mobile phones, tablets and the internet, on a daily basis and experience a wide range of opportunities, opinions and situations. The exchange of ideas, social interaction and learning opportunities involved is greatly beneficial but can occasionally place young people in danger.

2. E-Safety

At Akaal Primary we recognize the range of e-safety issues and plan accordingly to help ensure the appropriate, effective and safe use of electronic communications within our school.

E-Safety encompasses not only internet technologies but also electronic communications such as mobile phones, tablets, mobile devices and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using technology. It provides safeguards and raises awareness to enable users to control their online experiences. The internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day. Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism, access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their safety and that of others.

Why Use the Internet in School?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, enhance communication, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

3. Access

Some material available via the internet is inappropriate for primary pupils, but it is impossible to completely remove the risk that pupils might access these materials. At Akaal Primary School we take the following precautions to minimise this risk and ensure that users access only appropriate information: -

3.1 Internet access is a planned part of the curriculum. It is an entitlement for pupils but is based on responsible use. Pupils are given clear objectives for internet use;

3.2 Internet access is planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirements and age of pupils;

3.3 Pupils are educated in the effective use of Internet in research, including the skills of knowledge location, retrieval and evaluation;

3.4 The school's 'E-Safety Rules' poster is displayed prominently near computer systems with internet access and in all Key Stage 1 and 2 classrooms. Pupils are regularly reminded about the school's rules through discrete teaching sessions and also at the point of Internet use;

3.5 The school uses a recognised educational Internet Service Provider (ISP). This system incorporates a filter, which prevents access to the vast majority of undesirable materials;

3.6 Individual members of staff always preview websites to ensure that the materials in use are suitable for the age and maturity of pupils. Access is reviewed as pupils' internet use expands and their ability to retrieve information develops;

3.7 Wherever possible, children access teacher-prepared materials rather than the open internet. Such materials may be stored in a class 'Favourites' list or accessed via hyperlinks from another document;

3.8 Pupils are encouraged to inform a member of staff immediately if they encounter any material that upsets them, they feel is offensive or they feel may cause offence to others;

3.9 Any accessed material deemed inappropriate by staff is reported to the IT Coordinator and a record made of the URL. This information is then passed on to the Internet Service Provider.

3.10 The Head Teacher deals with any incidents involving misuse of the internet. The incident is recorded and parents are informed; sanctions for irresponsible internet use are linked to the school's behaviour policy;

3.11 The IT Coordinator checks all computer systems regularly to monitor all sites accessed;

3.12 Virus protection is installed and updated on every computer to increase system security;

3.13 Children are not allowed to use pen drives or disks brought from home unless they have been previously checked by the IT Coordinator;

3.14 All staff must accept the terms of the policy before using any Internet resource in school;

3.16 Staff are made aware that Internet traffic can be monitored and traced to the individual user. The school expects discretion and professional conduct from all staff;

3.17 When copying materials from the web, copyright laws are respected.

4. Using E-Mail Facilities

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects worldwide. However, the use of e-mail requires that the implications for pupils have been thought out and that appropriate safety measures have been put in place. At school we take the following precautions to ensure responsible and safe use: -

4.1 Specific E-mail use is taught using software which restricts sending and receiving mail to users on the school domain. Staff ensure that all safety precautions regarding email are fully understood before children are allowed to send e-mail via internet connections.

4.2 The forwarding of chain letters is forbidden in school;

4.3 All in-coming pupil e-mail is considered as a public document i.e. it can be viewed by all;

4.4 All E-mail prepared by pupils is approved by a teacher before sending;

4.5 Pupils may only use approved e-mail accounts on the school system;

4.6 Pupils must not reveal details of themselves or others in e-mail communication, unless they have checked with a member of staff first;

4.7 Only whole-class and not individual e-mail addresses are permitted for pupil use in school;

4.8 Wherever possible, teaching staff make every effort to check the credibility of e-mail recipients.

4.9 All e-mail contact from parents is made via the School Office e-mail addresses. Individual staff may give out their school e-mail address or a generic class-year group e-mail address but this is at the discretion of the individual.

5 School Web Site

The school has developed its own web site that contains information about the ethos and values of the school, the staff and other relevant information including recent newsletters. The website is updated on a regular basis and the content is reviewed regularly to ensure that it is well presented and that personal security is not compromised. The school takes the following precautions to ensure the security of its staff and pupils is maintained:

5.1 All materials published are monitored by the Head Teacher and/or IT Coordinator;

5.2 The web site and Facebook page contains names of individual members of staff, but individuals cannot be identified from photographs and no information relating to home addresses or individual e-mail identities are published;

5.3 Named photographs of pupils are not published on the web site. Any group photographs do not have a name list attached.

5.4 Wherever possible, photographs with smaller images of children are used to minimize identification of individual children;

5.5 Checks are made that all pupils in photographs are appropriately clothed;

5.6 Parental permission is obtained for all pupils whose photographs appear on the website. Additional permission is obtained regarding use of the child's photograph in local media;

5.7 The point of contact on the web site and Facebook is the school address, telephone number and e-mail address;

5.8 Pupils are encouraged to share their ideas and views using only closed and controlled forums and discussion groups. Any inappropriate content will be removed immediately and an appropriate sanction taken.

6 Social Networking and Personal Publishing

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control. For use by responsible individuals, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published. Examples include: blogs, wikis, MSN, Facebook, Twitter, Whatsapp, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

The school recognises the increasing value of social networking and personal publishing but takes the following precautions to ensure safety: -

6.1 Conferencing will only be permitted to a known group of users, that has been selected and approved by the class teacher;

6.2 Social networking sites will not be made available to pupils unless an educational requirement for their use has been demonstrated;

6.3 Wherever possible, forums, blogs etc are encouraged via a recognised educational provider which has a restricted audience and can be managed by the school. Entries will be monitored closely by the creator of the forum and any mis-use will be reported to the IT Coordinator;

6.4 Pupils will not be allowed access to public or unregulated chat rooms;

6.5 Children are only permitted to use regulated, educational chat rooms. This use is supervised and the importance of chat room safety emphasised;

6.6 Pupils are advised not to place personal photos on any social network space.

6.7 Pupils are reminded never to reveal personal details of themselves, friends or family without checking first with a responsible adult;

6.8 Pupils are reminded that users may try to assume a different identity and that all communication should be done with caution. Similarly, pupils should never pretend to be someone else or steal their identity;

6.9 All pupils are advised to talk to a responsible adult if they suspect that a site is being used inappropriately;

6.10 Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

6.11 Pupil mobile phones are only permitted in school with specific permission for a specific purpose. Pupils who bring mobile phones into school must adhere to the following:

- Phones must be kept in the child's school bag
- Phones must not be taken out at playtime
- The pupil should always ask permission before making or receiving a call or message.
- The school accepts no responsibility for the phone.

7 Video Conferencing

Video conferencing enables users to see and hear each other between different locations. It is a real time, interactive technology and has many uses in education. Equipment ranges from small PC systems (web cameras), tablets, mobile devices (including Skype and Facetime, to large room based systems that can be used for whole classes or lectures. The video conferencing equipment uses a network to communicate with the other site. The school takes the following precautions to ensure the safety of staff and pupils:

7.1 All video conferencing uses the broadband network to ensure quality of service and security rather than the Internet;
7.2 All video conferencing equipment in the classroom is switched off when not in use and not set to auto answer;

7.3 External IP addresses are not made available to other sites;
7.4 Video conferencing contact information is not put on the school website;
7.5 Equipment is secured and locked away when not in use;
7.6 School video conferencing equipment is not taken off school premises without permission as use over the non-educational network cannot be monitored or controlled;
7.7 Pupils should ask permission from the supervising teacher before making or answering a video conference call;
7.8 Video conferencing is always supervised appropriately;

7.9 Dialogue is established with other conference participants before taking part in a video conference. Measures are taken to check that materials to be delivered are appropriate for the age group of participants;
7.10 Unique log on and password details for the educational videoconferencing service are only issued to members of staff and kept secure.

8 Emerging Internet Applications

Many emerging communications technologies offer the potential to develop new teaching and learning tools. Mobile communications, wide Internet access and multimedia present opportunities which need to be evaluated to assess risks, to establish benefits and to develop good practice. When considering the use of any new technology, the school applies the following principles:

8.1 Emerging technologies are examined for educational benefit;
8.2 A risk assessment is carried out before use in school is permitted;
8.3 Pupils are reminded about safe practices and responsibilities;
8.4 Use of the technology is monitored and regulated.

9 IT System Security

The school IT system is central to the smooth running of the establishment and it is vital that security of the system is not compromised. The school takes the following measures to minimize risks: -

9.1 Only software approved by the Trust or a reputable supplier may be loaded onto the system;
9.2 Software must be approved by the IT Coordinator before loading onto any network, laptop, tablet or hard drive;
9.3 Appropriate security restrictions are in place on the network to prevent accidental or deliberate changes to network settings;
9.4 The main network server and cabinet is housed in a Network Equipment Room. Where possible, access to this room is restricted to maintain security of the system;
9.5 Virus protection is managed and updated by the school's IT providers;
9.6 Firewalls and routers are configured to prevent unauthorised access
9.7 A full backup of curriculum and administrative data is carried out daily.

10 Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act applies to anyone who handles or has access to information concerning individuals.

10.1 Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual).

10.2 The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individuals rights
- Kept secure
- Transferred only to other countries with suitable security measures.

10.3 All Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.

11 IT Coordinator

At Akaal Primary School, we recognize the importance of promoting e-safety and have a designated IT Coordinator whose responsibilities include those of an e-safety manager.

11.1 Key e-safety responsibilities include:

- Developing an e-safe culture and acting as a named point of contact on all e-safety issues.
- Promoting the school's e-safety vision to all stakeholders
- Ensuring that e-safety is embedded within CPD and co-ordinating training as appropriate
- Ensuring that e-safety is embedded across the curriculum
- Maintaining an e-safety log
- Monitoring and reporting on e-safety issues to the SLT and other agencies
- Reviewing and updating e-safety policies.

Date of policy – Jan 2018