



The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to E-Safety. E-Safety relates to accessing the Internet using a range of electronic devices such as laptop computers, iPad and mobile phones etc. It highlights the need to educate pupils about the benefits and risks of using technology and the Internet and provides safeguards and awareness for users to enable them to control their online experience.

The school's E-Safety policy operates in conjunction with other policies including: Acceptable Use Policy, Behaviour, Data Protection, Child Protection and Anti-Bullying.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of E-Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from KCON – FinchITSolutions who provide the network, services and facilities for our learning community.

## Writing and reviewing the E-Safety policy

This E-Safety policy was approved by the Governing Body on: 28 <sup>th</sup> January 2016
The implementation of this E-Safety policy will be monitored by the: Headteacher and Deputy Head
The E-Safety will be reviewed annually
Serious E-Safety concerns and incidents must be reported to; Lou Harrison (DSP), Maxine Michalowski (DSP) or Sharon Norris (DSP)

## Scope of Policy

This policy applies to:

- All teaching and support staff (including peripatetic staff)
- School governors and volunteers
- Children within the school
- Visitors and community organisations and users.

## Teaching and learning

### Why Internet use is important

- The Internet is an essential resource in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Pupils use the Internet widely inside and outside of school and need to learn how to evaluate Internet information and to take care of their own personal safety and security whilst online.

### Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.

- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Allows for access to worldwide educational resources and contacts.

### **Pupils will be taught how to evaluate Internet content**

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to DSP and KCON

### **Published content and the school website**

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

### **Publishing pupils' images and work**

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

### **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.
- Although primary age pupils should not use Facebook, Instagram, Snapchat or similar sites, pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.
- No member of staff should use social networking sites or personal publishing sites to communicate with students, past or present.
- Staff need to be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.
- If teachers decide to create official blogs or wikis, they should be password protected and run from the school website. Teachers should be advised not to run social network spaces for students on a personal basis.
- Teachers should not under any circumstances mention any references to their working lives on any social media.
- The school will control access to social media and social networking sites at school and social networking sites and newsgroups will be blocked unless a specific use is approved.
- Staff are advised not to run social network spaces for pupil use on a personal basis.
- School staff and parents should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.
- Parents will be advised that during class assemblies and school performances, that Parents and families may photograph their own children, but images must be edited prior to posting onto social media sites to ensure that the photograph shows no other children's faces
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.

- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

### **Managing filtering**

- The school will work with KCON to ensure that age appropriate filters and systems are in place to protect pupils and that these are reviewed and improvements implemented.
- If staff or pupils discover unsuitable sites, the URL must be reported to DSP and KCON
- Any material that members of staff believe is illegal must be reported to the Headteacher who will inform the appropriate agencies.
- The school keep up to date with new technologies, including those relating to mobile phones and handheld devices, and develop appropriate strategies.
- Emerging technologies will be examined for educational benefit and the Head teacher in consultation with staff will give permission for appropriate use.
- There are dangers for staff, however, if personal phones are used to contact pupils or families and therefore this will only be done when authorized by a senior member of staff.
- Abusive messages should be dealt with under the school's behaviour and anti-bullying policy.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- Pupils are not allowed to bring mobile phones into school. Under certain circumstances exceptions can be discussed with the Head teacher, so that pupil mobile phones can be kept in the school office. Parents must complete the permission slip to acknowledge that the school takes no responsibility for phones which are left in the office.

### **How will Internet access be authorised?**

- The school allocates Internet access for staff and pupils on the basis of educational need.
- Authorisation is as individuals and usage is fully supervised. Normally all pupils will be granted Internet access.
- Parental permission is required for Internet access in all cases as new pupils join the school.
- All staff must read and sign the Code of Conduct before using any school ICT resource.
- Parents will be asked to sign and return a consent form for pupil access. Parents will be informed that pupils will be provided with supervised Internet access.

### **How will e–Safety complaints be handled?**

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the Headteacher. If the complaint is about the Headteacher this should be reported to the Chair of Governors.
- All e–Safety complaints and incidents will be recorded by the school — including any actions taken.
- Pupils and parents will be informed of the complaints procedure. Parents and pupils will work in partnership with staff to resolve issues.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguards Unit to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's Disciplinary and Child Protection procedures.

### **How is the Internet used across the community?**

- We recognise that children can access the internet outside of school and offer support and advice to parents on internet safety through regular information sent home with children and through advice on our website.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will hold E-Safety assemblies for all children.

- E-Safety information will be shared with parents regularly throughout the year at parents' evenings, parent meetings and workshops and through newsletters and school website links.

### How will Cyberbullying be managed?

- Cyberbullying is defined as "The use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone" DfE 2007.
- It is essential that pupils, staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond.
- The school will make use of expert advice on such issues. The DfE and Childnet have produced resources and guidance that will be used to give practical advice and guidance on cyberbullying:  
<http://www.digizen.org/cyberbullying>
- Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents of cyberbullying reported to the school will be recorded.
- There are clear procedures in place to investigate incidents or allegations of cyberbullying:
  - Pupils, staff and parents/carers will be advised to keep a record of the cyberbullying as evidence.
  - The school will take steps to identify cyberbullying behaviour, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
  - Sanctions for those involved in cyberbullying may include: asking the perpetrator to remove any material deemed to be inappropriate or offensive.
  - A service provider may be contacted to remove content.
  - Internet access may be suspended at school for the user for a period of time.
  - Parent/carers will be informed and the Police will be contacted if a criminal offence is suspected.

### Sexting and Pornography

- Sexting – Children in Year 5 and 6 will be informed about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the World Wide Web.
- Pornography – many children will come across some type of pornographic content when searching the Internet. Children will be taught about what to do if they access this type of material and who to speak to.

### How will the policy be introduced to pupils?

- E-Safety is taught as an ICT lesson activity (*see Somerset IT Scheme*).
- All users are informed that network and Internet use will be monitored.
- Pupil instruction in responsible and safe use should precede Internet access every time they go online.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum.
- Particular attention will be given where pupils are considered to be vulnerable.

### How will the policy be discussed with staff?

- The e-Safety Policy will be formally provided to and discussed with all members of staff and published on the school website.
- To protect all staff and pupils, the school will implement Acceptable Use Policy. Staff should be aware that Internet traffic can be monitored and traced to the individual user; discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.

### How will parents' support be enlisted?

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach with parents will be encouraged. This will include parent meetings with demonstrations and suggestions for safe home Internet use.
- Parents will be requested to sign an E-Safety/internet agreement as part of the school's on entry procedures.
- Leisure activities that include responsible use of the Internet will be made available to parents.