WELFORD ON AVON PRIMARY SCHOOL POLICY

ONLINE SAFETY POLICY

Reviewed: **June 2017**

Review: **June 2018**

Our Online Policy has been written by the school following government guidance. It has been agreed by the senior management and approved by staff and governors. It will be reviewed annually.

Created by: Mr Mills

Vision

Welford on Avon Primary School provides a diverse, balanced and relevant approach to the use of technology. Children are encouraged to maximize the benefits and opportunities that technology has to offer. The school ensures that children learn in an environment where security measures are balanced appropriately with the need to learn effectively. The children are equipped with the skills and knowledge to use technology appropriately and responsibly and will be supported in this role by their teachers and parents or guardians. All staff are able to recognise the risks associated with technology and how to deal with them, both within and outside the school environment and all users in the school community understand why there is a need for an OnlineSafety Policy. Parents and guardians of pupils are encouraged to be involved with their children's use of technologies to ensure they can manage and unforeseen problems they may encounter.

The Importance of Internet Use:

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The Internet is an essential element 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.

The Benefits of Using the Internet in School includes:

- access to world-wide educational resources including museums and art galleries;
- inclusion in government initiatives such as the DfES ICT in Schools and the Virtual Teacher Centre (VTC) **http://vtc.ngfl.gov.uk**;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LEA and DfES.
- mentoring of pupils and provide peer support for them and teachers

The Internet will enhance pupils' learning:

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will learn to evaluate Internet content:

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Training will be available to staff in the evaluation of Web materials and methods of developing students' critical attitudes.

E-Mail:

- Pupils may only use approved e-mail accounts on the school system.
- Individual email addresses are issued with portal access.
- The forwarding of chain letters is not permitted.

School Website:

- The points of contact on the Web site are the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils are selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names are not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers is obtained before photographs of pupils are published on the school Web site.
- The headteacher and ICT subject leader take overall editorial responsibility and ensures that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

(see website policy for further details)

New Technology:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

The Authorisation of Internet Access:

- The school keeps a record of all staff and pupils who are granted Internet access.

  The record will be kept up-to-date, for instance a member of staff may leave or a

  pupil's access be withdrawn.
- At Key Stage 1, access to the Internet is by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents are informed that pupils will be provided with supervised Internet access (an example letter for primary schools is included as an appendix).

Risk Assessment:

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school takes all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor LA can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

Filtering:

- The school will work in partnership with parents, the LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT subject leader.

Accessing the Internet:

- Rules for Internet access will be clearly posted in the ICT suite.
- Instruction in responsible and safe use should precede Internet access.
- All children will have participated in a series of e-safety lessons (created by the ICT subject leader) prior to accessing the learning platform.

Staff Use of the Internet:

- All staff including teachers, supply staff, classroom assistants and support staff, are provided with the School Internet 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.
- Staff development in safe and responsible Internet use, and on the school Internet policy will be provided as required.

Maintaining Security:

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly by the LEA.
- Files held on the school's network will be regularly checked.
- The ICT subject leader will ensure that the system has the capacity to take increased traffic caused by Internet use.

Complaints regarding Internet use:

- Responsibility for handling incidents will be delegated to the e-safety teacher.
- Any complaint about staff misuse must be referred to the headteacher.
- Children and parents are able to collect an e-safety reporting form from the school office and ICT suite to report any issues related to e-safety – this will be looked into by the e-safety teacher and, if necessary, the designated child protection teacher / governor

Use of technologies outside of school.

The school regards e-safety as a wider community issue and confirms that it will deal rigorously with out of school e-safety incidents that relate to members of the school community. If the school is unable to facilitate a resolution concerning an out of school incident then we can suggest an agency to approach to help and support people's needs

Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Please referee to the sanction guidelines for further information.

Personal Technologies and Mobile Devices

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Regular audits and monitoring of usage will take place to ensure compliance

Social Networking

Welford on Avon Primary School has a duty of care to provide a safe learning environment for pupils and staff. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the e-safety committee to ensure compliance with the Social Networking, Data Protection, Digital Image Policies.

See also the Policy on Use of Social Media

Cyber Bullying

The school recognises that technology plays an important and positive role in children's lives, both educationally and socially. It is committed to helping all members of the school community to understand both the benefits and the risks, and to equip children with the knowledge and skills to be able to use technology safely and responsibly.

Please see the Cyber Bullying Policy for more information.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive

- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained.
- It has a Data Protection Policy.
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

Cloud Storage

- Staff should not use personal cloud storage for any data relating to the school.
- Any Data stored on cloud storage devices should be verified by senior members of staff (Head Teacher).
- Any use of cloud storage must be verified by senior staff members.

See Cloud Storage policy for more information.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Passwords

Passwords are to be created in line with the password policy. Passwords can be requested to allow visitors the use of the school network. Please see the password policy for details.

Filtering

The schools computer systems are filtered to allow children and staff to use computer devices effectively.

Digital and Video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

- When using digital images, staff should inform and educate students / 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 eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / pupils* in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website.

Staff

Staff Use of the Intenet:

- All staff including teachers, supply staff, classroom assistants and support staff, are provided with the School Internet 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.
- Staff development in safe and responsible Internet use, and on the school Internet policy will be provided as required.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Social Networking

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Related Policies:

PSHE, Anti-Bullying, Behaviour, Data protection, Safegaurding, Computing, Password, Mobile Devices and Social Network, Cloud Storage.