

Purpose

This purpose of this policy is to guide practice in school to ensure the safety, security and confidentiality of pupils and staff when using computers, new technology and online services. The school recognises that computers, new technology and online work gives users access to vast amount of information and communication from many sources but this also increases the risks of information and communication being misused or users being exposed to inappropriate material for their age/context.

The school works within LA guidelines to ensure that it makes good use of appropriate systems to maintain and support the security and safety of its users. Internet use, email communication and published material and electronic communication security are covered by this policy.

Email

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits and interesting projects between schools in neighbouring villages and in different continents can be created.

Email should not be considered private and school reserves the right to monitor email. Email use is restricted in school and can only be accessed via a secure login to the broadband provider. In this way email use in school requires the authorisation of a member of staff which facilitates easier monitoring and limits this communication in the setting. Spam, phishing and virus attachments can make email dangerous. The LA approved broadband provider provides filtering and virus checking services that eliminates the majority of these risks. School IT equipment uses anti-virus/spy-ware software that also checks emails upon downloading.

- Pupils may only use the approved email accounts via the broadband provider and with the approval of their teacher
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Access in school to external personal email accounts may be blocked.
- The forwarding of chain messages is not permitted.
- Staff do not use school email accounts to communicate with pupils outside of the school setting.
- Staff should not use personal email accounts during school hours or for professional purposes

Published Content:

The school has a good website that provides information, communication and publishes children's work. Sensitive or personal information about the school and pupils is never published on the school's website, as it is widely available. Publication of information including children's work will be considered from a personal and school security viewpoint. Material specific to stakeholders of the school only will only be published in the school brochure or on a secure part of the learning platform which requires authentication.

Contact details on the website are the school address, email and telephone number. Staff or pupils' personal information must not be published. A named teacher is responsible for the regular management of the website and the Headteacher will take overall responsibility for ensure that content is accurate and appropriate.

Images that include pupils will be selected carefully and will not provide material that could be easily reused. Images will usually be of groups of pupils and will be small in size to limit re-use. Written permission from parents or carers will be obtained before images of pupils are electronically published. Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

Social networking, social media and personal publishing.

Emerging online spaces and social networks allow individuals to publish content can connect people in ways that are not easy to control. Mmaterial in such sites is much harder to mediate. For responsible adults, social networking sites provide easy to use, free facilities but 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. All staff are made aware of the potential risks of using social networking sites or personal publishing. They should be made 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, and instant messenger.

- The school does not allow access to social media and social networking sites on the

premises and the LA approved broadband provider filters out access to such sites.

- Pupils will be advised never to give out personal details of any kind which may identify them or their location when using online resources.
- School related blogs or wikis are password protected and run from the school learning platform with approval from the Senior Leadership Team.
- Staff will not establish links with pupils or past pupils under the age of 18 on social network or similar sites; where they are able to access a range of published materials not specifically targeted to an individual.

Filtering

Levels of Internet access and supervision will vary according to the user. Access profiles must be appropriate for all members of the school community. Staff might need to research areas subjects that pupil's filtering may block. Systems to adapt the access profile to user are available and can be changed by the system administrator. All pupils in our school are set to the highest level of filtering restricting their access to undesirable commercial and inappropriate sites including those with inappropriate advertising. Filtering includes

- Blocked of unsuitable sites. Maintenance of the blocking list is a major task and is undertaken by the LA broadband provider
- Dynamic filtering examines web page content or email for unsuitable words. Filtering of outgoing information such as web searches is also required.
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.
- The school will work with the LA and approved Broadband provider to ensure that systems used to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to LA IT support team and the broadband provider.
- The school's broadband access includes filtering appropriate to the age/maturity of pupils.
- Any material that the school believes is illegal must be reported to appropriate agencies.

Emerging Technology

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as risks.

Our school is committed to keeping up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies.

- As such technologies are developed the school will assess the risks and consider educational benefits before allowing them for school use.
- Pupil's mobile phones are not allowed to be used during school without the teacher's authorisation and as a rule are not permitted in school, this is to...
 - Reduce risk to or loss of potentially expensive personal property
 - Help prevent easy communication, image and video sharing that may (or may later) prove to be inappropriate, offensive, upsetting or misleading.

If a phone is required for emergency contact purposes this must be authorised by the parent and then kept by the teacher during school hours for safety.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. This gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

Internet access

Internet access for staff and pupils is allocated on the basis of educational need and controlled by individual log-ins that access the correct profile for the user's status. As such all pupils have Internet access for curriculum use and with the permission of the teacher which is limited by predetermined security settings. Parental permission is required for Internet access.

- 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 This

is done through the Home / School Planner.

- 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 DCC can accept liability for the material accessed, or any consequences resulting from Internet use.

E-safety Complaints

Any complaints regarding e-safety will be dealt with using the usual school's complaints procedure. The facts will need to be established and appropriate action taken.

A minor transgression of the rules may be dealt with by a member of staff. Other situations could potentially be more serious and a range of sanctions may be required where appropriate these may be linked to or superseded by the school's disciplinary policy, anti-bullying policy, confidential reporting policy or child protection policy.

- Any safeguarding of children or illegal issues must be referred to the school Designated Child Protection Coordinator (Headteacher).
- Any complaint about staff misuse must be referred to the Headteacher; or if the complaint involves the Headteacher should be referred 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.
- Parents and pupils will work in partnership with staff to resolve issues.
- Advice will be sought from the LA legal team, Safeguarding Board or Police where appropriate

How will Cyberbullying be managed?

Cyberbullying is defined as “The use of ICT, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 2007. DCSF and Childnet produced resources and guidance that can be used to give practical advice and guidance on cyberbullying can be found at: <http://www.digizen.org/cyberbullying>

Possible Statements:

- Cyberbullying will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.
- All incidents of cyberbullying reported to the school will be recorded.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully
- Sanctions for those involved in Cyberbullying will be in line with school's anti-bullying policy but may also include:
 - Removal of 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.
 - The Police will be contacted if a criminal offence is suspected.

Learning Platform

The school's Learning Platform can enable pupils and teachers to collaborate in and across schools, can share resources and tools for a range of topics, create and manage digital content and pupils can develop online and secure e-portfolios. The school's platform is Managed by Kaleidos/RM listed on Becta's Learning Platform Services Framework to ensure that standards and functions are met.

- The Learning Platform is subject to careful monitoring by teaching staff and the SMT.
- Pupils/staff are advised on acceptable conduct and use when using the learning platform.
- Only members of current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns with content may be recorded and dealt with in the following ways:
 - a) The user will be asked to remove any material deemed to be inappropriate or offensive.
 - b) The material will be removed by the site administrator if the user does not comply.

- c) Access to the LP for the user may be suspended.
- d) The user will need to discuss the issues with a member of SMT before reinstatement.
- e) A pupil's parent/carers will be informed.
- A visitor may be invited onto the LP by a member of the SMT. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

How will the policy be introduced to pupils?

- All users will be informed that network and Internet use will be monitored.
- Pupil instruction in responsible and safe use should precede Internet access.
- An e-Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. As new software and resources are taught e-safety will be reinforced.
- Particular attention will be given where pupils are considered to be vulnerable.

Useful e-Safety programmes to refer to include

Think U Know: www.thinkuknow.co.uk, Childnet: www.childnet.com, Kidsmart: www.kidsmart.org.uk and Safe Social Networking: www.safesocialnetworking.com

How will the policy be discussed with staff?

Teaching staff have discussed and contributed to this policy and understand that the rules and expectations regarding e-safety and appropriate use of new technology. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with a SMT member or the Headteacher.

- Staff are made aware of their responsibility to maintain confidentiality of school information when using systems or technology outside of the school setting
- Induction of new staff should include a discussion of the school e-Safety Policy.

Parents support.

The school will continue to work in partnership with parents to secure safe use of new technology for education at home and at school. As the school introduces new technology or programmes into use it will advise parents about e-safety in connection with it. This may include parent workshops where appropriate.

- Parents' attention will be drawn to the School e-Safety Policy and placed on the Learning Platform
- A partnership approach with parents will be encouraged. This may include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e-Safety at parent evenings/
- Parents will be requested to sign internet use agreement
- Interested parents will be referred to organisations and websites listed in this policy

Review

This policy will be reviewed every 2 years or as emerging new technology / guidance dictates a change in practice to better secure e-safety of users.