**Cadoxton Primary School**

**Online Safety Safety Policy 2018**

**This policy applies to all members of the schoolcommunity (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.**

**Online Safety Policy**

Online Safety encompasses Internet technologies and electronic communications such as mobile devices, mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their Online Safety experience.

The Online Safety Policy has been written to raise awareness of the safety issues associated with electronic communications as a whole.

The school’s Online Safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Anti- Bullying, Curriculum, Data Protection, Security, Acceptable User, and Safeguarding/Child Protection.

This core Online Safety policy provides the essential minimal school Online Safety policy and has been developed and approved by the Cadoxton Primary School Online Safety Committee which includes:

* Headteacher
* Online Safety Officer / Coordinator
* Staff – including Teachers, Support Staff, Technical staff
* Governors
* Parents and Carers
* Community users

End to End Online Safety

Online 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 Online Safety policy in both administration and curriculum, including secure school network design and use.
* Safe and secure broadband from the Vale of Glamorgan, including the effective management of Websense filtering.
* National Education Network standards and specifications.

Further Information

* LEA 01446 709100.

**Schedule for Development/Monitoring/Review**

|  |  |
| --- | --- |
| This Online Safety policy was approved by the Governing Body *On:*The implementation of this Online Safety policy will be monitored by the:Monitoring will take place at regular intervals:*The Governing Body* will receive a report on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of Online Safety incidents) at regular intervals:The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:Should serious Online Safety incidents take place, the following external persons / agencies should be informed: | September 2017Online Safety Coordinator/Online Online Safety CommitteeAnnuallyAnnuallyJune 2017LA ICT Manager, LA Safeguarding Officer/Manager, Police. |

**Roles and Responsibilities**

7

**Governors:**

Governorsare responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governing body* receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Bodyshould take on the role of Online Safety Governor toinclude:

* regular meetings with the Online Safety Co-ordinator
* regular monitoring of Online Safety incident logs
* regular monitoring of filtering / change control logs (where possible)
* reporting to relevant Governors / sub-committee / meeting

**Headteacher and Senior Leaders:**

* The Headteacher has a duty of care for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety may be delegated to the *Online Safety* Co-ordinator.
* The Headteacher and designated Senior Leader should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.
* The Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
* The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
* The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

**Online Safety Coordinator and Safeguarding Officer:**

* leads the Online Safety Committee
* takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
* ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
* provides (or identifies sources of) training and advice for staff
* liaises with the Local Authority / relevant body
* liaises with (school) technical staff
* receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments.
* meets regularly with Online Safety Governor to discuss current issues, review incident logs and if possible, filtering / change control logs
* attends relevant meeting / sub-committee of *Governors*
* reports regularly to Senior Leadership Team

**Network Manager / Technical staff:**

The Network Manager / Technical Staff is responsible for ensuring:

* that the *school’s* technical infrastructure is secure and is not open to misuse or malicious attack
* that the schoolmeets (as a minimum) the required Online Safety technical requirements as identified by the Local Authority and also the Online Safety Policy that may apply.
* that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
* that they keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
* that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher, Senior Leader; Online Safety Coordinator for investigation / action / sanction
* that LA monitoring software / systems are implemented and updated as agreed in school policies

**Teaching and Support Staff:**

Are responsible for ensuring that:

* they have an up to date awareness of Online Safety matters and of the current schoolOnline Safety policy and practices
* they have read, understood and signed the Staff Acceptable Use Policy (AUP)
* they report any suspected misuse or problem to the *Headteacher / Senior Leader ; Online Safety Coordinator,* for investigation / action
* all digital communications with students / pupils / parents / carers should be on a professional level *and only carried out using official school systems*
* Online Safety issues are embedded in all aspects of the curriculum and other activities
* students / pupils understand and follow the Online Safety and acceptable use *agreements / policies*
* students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
* in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*

**Safeguarding Designated Person/Online Safety Coordinator:**

Is responsible for and trained in e-Safety issues and are aware of the potential for serious safeguarding issues to arise from:

* sharing of personal data
* access to illegal / inappropriate materials
* inappropriate on-line contact with adults / strangers
* potential or actual incidents of grooming
* cyber-bullying

**Online Safety Committee:**

The Online Safety Committee provides a consultative group that has wide representation from the schoolcommunity, with responsibility for issues regarding Online Safety and monitoring the Online Safety policy including the impact of initiatives.

Members of the Online Safety Committee will assist the *Online Safety Coordinator* with:

* the production / review / monitoring of the school Online Safety policy / documents.
* mapping andreviewing the Online Safety curricular provision – ensuring relevance, breadth and progression
* monitoring network / internet / incident logs where possible
* consulting stakeholders – including parents / carers and the students / pupils about the Online Safety provision
* monitoring improvement actions identified through use of the 360 degree safe Cymru self review tool

Students / pupils:

* are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement and Online Safety Code of Conduct
* have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
* will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
* should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school’sOnline Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, website / VLE and information about national / local Online Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good Online Safety practice and to follow guidelines on the appropriate use of:

* digital and video images taken at school events
* access to parents’ sections of the website / VLE and on-line student / pupil records
* their children’s personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems / website / VLE as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

**Online Safety Audit**

This quick self-audit will help the senior leadership team (SLT) assess whether the Online Safety basics are in place to support a range of activities that might include those detailed within Appendix 1.

|  |  |
| --- | --- |
| Has the school an Online Safety Policy that complies with CFE guidance? | **Y** |
| Date of latest update: June 2016  |
| The Policy was agreed by governors on: September 2017 |
| The Policy is available for staff at: Hwb – staff documents policies 2017 |
| And for parents at: www.cadoxtonprimary.com |
| The Designated Child Protection Coordinator is: Mrs J Hayward Head Teacher. The Deputy Child Protection Officer is Mrs V Tattersall |
| The Online Safety Coordinator and Safeguarding Officer is: Mrs V Tattersall |
| Has Online Safety training been provided for both students and staff? | **Y** |
| Do all staff sign an ICT Code of Conduct on appointment?  | **Y** |
| Do parents sign and return an agreement that their child will comply with the School Online Safety Rules?  | **Y** |
| Have school Online Safety Rules been set for students?  | **Y** |
| Are these Rules displayed in all rooms with computers? | **Y** |
| Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access  | **Y** |
| Has an ICT security audit has been initiated by SLT, possibly using external expertise?  | **Y** |
| Is personal data collected, stored and used according to the principles of the Data Protection Act?  | **Y** |

**Teaching and learning**

**Why Internet use is important**

The Internet is a part of everyday 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.

**How does internet use benefit education**

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

* access to learning wherever and whenever convenient.
* access to worldwide educational resources including museums and art galleries;
* educational and cultural exchanges between pupils worldwide;
* vocational, social and leisure use in libraries, clubs and at home;
* access to experts in many fields for pupils and staff;
* professional development for staff through access to national developments,  educational materials and effective curriculum practice;
* collaboration across networks of schools, support services and professional associations;
* improved access to technical support including remote management of networks and  automatic system updates;

**How can internet use enhance education**

* The school’s Internet access will be designed to enhance and extend education.
* Pupils will be taught what Internet use is acceptable and what is not and how to act responsibly on the internet with clear objectives for Internet use.
* The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
* All members of staff and pupils will be taught copyright and plagiarism law.

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

* The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
	+ Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

**Managing Information Systems**

**How will Information system security be maintained**

# Local Area Network (LAN) security issues include:

* Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
* Users must take responsibility for their network use.
* Workstations should be secured against user mistakes and deliberate actions.
* Servers must be located securely and physical access restricted.
* The server operating system must be secured and kept up to date.
* Virus protection for the whole network must be installed and current.
* Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

The security of the school information systems and users will be reviewed regularly.

* Virus protection will be updated regularly.
* Personal data sent over the Internet or taken off site will be encrypted.

**Managing email**

* Pupils may only use approved e-mail accounts on the school system.
* Pupils must immediately inform an adult if they receive an offensive e-mail.
* Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
* E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
* The forwarding of chain letters is not permitted.

**Published content and the school web site, blog and Twitter account**

* The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils’ personal information will not be published.
	+ The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

**Publishing pupil’s 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 or Blog, 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.
* Pupil’s work can only be published with the permission of the pupil and parents.

**Social networking and personal publishing**

* The school will block/filter access to social networking sites.
* Newsgroups will be blocked 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 and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
* Staff personal use of social networking, social media and personal publishing sites  will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

**Managing filtering**

* The school will work with the LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
* If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator.
* Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

 **Managing videoconferencing**

* IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
* Pupils should ask permission from the supervising teacher/adult before making or answering a videoconference call.
* Videoconferencing will be appropriately supervised for the pupils’ age.

**Managing emerging technologies**

* 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.
* Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.

 **Protecting personal data**

* Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

**Policy Decisions**

**Authorising Internet access**

* All staff must read and sign the LEA ‘Acceptable ICT Use Agreement’ before using any school ICT resource.
* The school will keep 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 will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
* Parents will be asked to sign and return a consent form.

 **Assessing risks**

* 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 LEA can accept liability for the material accessed, or any consequences resulting from Internet use.
* The school will audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

 **Responding to incidents of concern**

* All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
* The Online Safety Coordinator will record all reported incidents and actions taken in the School Online Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
* The Designated Child Protection Coordinator will be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
* Pupils and parents will be informed of the complaints procedure.
* After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
* Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children’s Safeguard Team or Online Safety officer and escalate the concern to the Police.
* If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children’s Officer or the County Online Safety Officer.

**Handling E safety complaints**

* Complaints about Internet misuse will be dealt with under the School’s complaints procedure.
* Any complaint about staff misuse will be referred to the head teacher.
* All Online 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 need to work in partnership with the school to resolve issues.

**Community use of the Internet**

The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

**Handling cyberbullying**

Cyberbullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 2007

* Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school’s policy on anti-bullying and behaviour.
* There are clear procedures in place to support anyone in the school community affected by cyberbullying.
* All incidents of cyberbullying reported to the school will be recorded.
* There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

**Managing Learning Platforms**

* SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
* Pupils/staff will be advised about acceptable conduct and use when using the LP.
* Only members of the 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 onto the LP.
* 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 about content on the LP 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 SLT before reinstatement.

e) A pupil’s parent/carer may be informed.

**Managing Personal Devices**

The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school Acceptable Use or Mobile Phone Policies.

* The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
* School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Management team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
* Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.
* If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff use of Mobile Phones

* Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
* Staff will be issued with a school phone where contact with pupils or parents/carers is required.
* Mobile Phone and devices will be switched off or switched to ‘silent’ mode, Bluetooth communication should be “hidden” or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior ManagementTeam in emergency circumstances.
* If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Management Team.
* Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
* If a member of staff breaches the school policy then disciplinary action may be taken.

**Communications Policy**

 **Introducing the Online Safety policy to pupils**

* An Online Safety training programme, supported by the school’s eCadets, is established and consistently delivered across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
* Online Safety rules/code of conduct are posted in all networked rooms and discussed with the pupils regularly throughout the academic year.
* Pupils are informed that network and Internet use will be monitored.

**Staff and the Online Safety policy**

* The Online Safety Policy will be formally provided to and discussed with all members of staff.
* To protect all staff and pupils, the school will implement Acceptable Use Policies.
* Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
* Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

**Enlisting parents’ support**

* Parents’ attention will be drawn to the school Online Safety Policy in newsletters, the school prospectus and on the school website.
* A partnership approach to Online Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings, assemblies and sports days.
* Parents will be requested to sign an Online Safety/Internet agreement as part of the Home School Agreement.
* Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.