***Newchurch Community Primary***

***Policy*** E-Safety

***Mission Statement***

Newchurch will give every child a flying start by working in partnership with parents, staff and the community to develop well-rounded citizens who will contribute in a positive way to society.

***Persons with Responsibility***

John Duckett

Sara Lawrenson

Jayne Narraway

***Linked Policies***

Computing

Child protection

***Next Review***: Sep 2020

E-safety encompasses the use of new technologies, internet and electronic communications, such as mobile phones, 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 experience. 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 Warrington, including the effective management of filtering;
- National Education Network standards and specifications.

Writing and reviewing the E-Safety policy

- The e-safety policy will relate to child protection documents and a variety of curriculum policies.
- The document will be reviewed regularly by the curriculum leader and other designated staff. This will also happen following any cause for concern or major incident.
- The governing body will be made aware of any changes to the policy.
- The policy will reflect the needs and access to communication technologies of the children of Newchurch Primary School.
- The document will take advice and guidance from Warrington Borough Council, the government, as well as other child and e-safety organisations (e.g. NSPCC)

Teaching and learning

Why Internet use is important

- 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;
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

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;
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

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;
- Approved search engines will be provided for the children to use in and out of school to ensure children are led to child friendly websites. These will be checked regularly and changed accordingly by the E-Safety Co-ordinator.

Managing Internet Access Information system security

- School ICT systems capacity and security will be reviewed regularly;
- Virus protection will be updated regularly;
- Security strategies will be discussed with Warrington.
- Newchurch will employ specialist technicians to monitor all onsite systems and to advice on best policy and practise.

E-mail

- Pupils may only use approved e-mail accounts on the school system after written permission from parents – this will only happen on specific teaching units;
- Pupils must immediately tell a teacher if they receive 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. This will be taught explicitly through E-Safety teaching in each year group;
- 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

- 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, by checking it regularly. The day to day editorial responsibility will lie with the E-Safety Coordinator and designated staff.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified unless parental permission has been given;
- Pupils' full names will not be used anywhere on the school website, particularly in association with photographs;
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website;
- Pupil's work and photographs may be published through the use of the VLE where group members only have access;
- Children will be taught to use websites outside of the school VLE responsibly through E-Safety teaching;
- 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;
- Staff will have access to their own class chat feed through e-schools VLE
- Pupils and parents will be advised that the use of certain social network spaces, such as Facebook, Instagram, Snapchat etc, outside school is inappropriate for primary aged pupils;
- Children will be taught how to use social network sites safely and encouraged only to use the school VLE for social networking.

- Parent workshops will be organised annually to help educate them on the risks inherent with social media and e-safety. This may be delivered by school, law enforcement or the NSPCC.

Managing filtering

- School use the Fortinet system for filtering online access. These systems and filters are agreed between Warrington schools and the LA.
- School uses the EDAC Sure system through EDAC computing support. This system gives four digit logins to all children and staff in school and allows for monitoring of internet access. See appendix 1
- The school will work with the LA, 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 E-Safety Coordinator;
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
- Children will be taught to use the same process at home, keeping communication links open with parents to encourage consistent behaviour at home.

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;
- Staff will use a school phone where contact with pupils is required.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Policy Decisions Internet access
- All staff must read and adhere to the 'Acceptable ICT Use Agreement' before using any school ICT resource;
- Access to the Internet will be by directly supervised access to specific, approved on-line materials;
- Images and data will not be collected on personal devices e.g. mobile phones.

Assessing risks

- The school will take 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 WBC can accept liability for the material accessed, or any consequences of Internet access;
- The school will audit ICT provision to establish if the E-Safety policy is adequate and that its implementation is effective.

Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff;
- Any complaint about staff misuse must be referred to the Headteacher;
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures;
- Pupils and parents will be informed of the complaints procedure;

- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Safeguarding against radicalisation, extremism and terrorism

- Staff trained through 'Prevent' initiative.
- Children's internet use monitored during sessions
- E-mail to be used only in structured sessions as a means to access approved programmes.
- Children educated about the risks of meeting people met online.
- Children made aware of the dangers of radicalisation at appropriate points without indoctrination to any belief offering balanced view – in line with government Prevent Guidance.
- Other safeguarding methods named in this document will be in place e.g. filtering and awareness.
- Staff made aware of places to seek advice on safe internet use e.g. https://www.saferinternet.org.uk/
- British values programme taught through PSHE to ensure children are aware of diversity within British culture without indoctrination.

Community use of the Internet

- External organisations using the school's ICT facilities must adhere to the E-Safety policy.

Communications Policy Introducing the E-Safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year;
- Pupils will be informed that network and Internet use will be monitored.

Staff and the E-Safety policy

- All staff will be given the School E-safety 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.

Enlisting parents'/carers' support

- Parents'/carers' attention will be drawn to the School E-Safety Policy through workshops, in newsletters and through documentation on the school Web site;
- Annual E-Safety parent workshops will be held to give parents up to date information about how to keep children safe at home.

Why might the internet or communications technology be used?

| Activities | Key e-safety issues | Relevant sites and programmes |
|---|---|---|
| Using search engines to access information from a range of websites. | Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access | Ask.com<br><br>Kidrex.org |

| | | |
|---|---|---|
| | material they are uncomfortable with. | |
| Exchanging information with other pupils and asking questions of experts via e-mail | Pupils should only use approved email accounts. Pupils should never give out personal information. | e-schools VLE<br>Designated blogging sites with parental permission only |
| Publishing pupils' work on school and other websites. | Pupil and parental consent should be sought prior to publication. Child names should be omitted if using websites outside of the VLE. | School VLE Blogs |
| Publishing images including photographs of pupils. | Parental consent for publication of photographs should be sought. File names should not refer to the pupil by name. | Kidblog<br>School website and VLE<br>Weebly.com (parent permission only) |
| Audio and video conferencing to gather information and share pupils' work. | Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used. | Skype |

Appendix

EDAC Solutions Ltd
Abacus House, 450 Warrington Road
Culcheth
Warrington
Cheshire WA3 5QX
01925 572573 / 596157
FAX 08717 146713

**EDACSure Internet Portal**

Following the installation of your Internet Portal, below is an outline of the functionality and requirements for use;

All Internet traffic on the school curriculum network is now routed through the portal.

Every pupil and staff member has a unique username and password which must be entered in order to access the Internet.

Each Internet session has its IP address, MAC Address, date and time and username recorded in a log which is exported to your main curriculum server in real time. This log is then backed up every night.

Users can be individually added, deleted or suspended which will affect that users Internet access rights.

The portal does not provide any filtering solutions, this is carried out by the WBC firewall. The firewall logs detail IP address which can be cross referenced to the portal logs to identify individual users. We recommend periodically requesting filter logs from WBC for auditing and filter checking purposes.

There is a 10 minute inactivity time out safe guard within the portal to avoid users inadvertently remaining logged on after a session along with a 90 minute hard timeout regardless of usage. These time limits can be adjusted for your individual needs.

If the portal is powered down or otherwise disconnected the Internet will not function and it is important to call us as soon as possible to rectify the problem.