Long Lawford Primary School

Love, Learn, Persevere and Succeed

Online Safety Policy

September 2019

Adopted by Governing Body:

Signed: _____ Headteacher

Signed: _____ Chair of Governors

Date of next review: _____

Introduction

In today's society, Information and Communication Technology (ICT) is an essential resource to teaching and learning, as well as playing an important part in our everyday lives. As a school, we embed ICT into all areas of the curriculum to provide children with the skills they will need throughout their lives and future employment.

The Computing curriculum covers a wide variety of resources, including web-based and mobile learning. The children at Long Lawford Primary School have the opportunity to use both computers and iPads to access websites and create their own content.

It is also important to recognise that many children have constant access to web or mobile devices in school (such as PCs, laptops, iPads, cameras etc.) and at home (such as PCs, laptops, tablets, cameras, game consoles, portable media devices etc.) and are using online resources frequently. Although this is both beneficial and enjoyable, all users need to be aware of the potential dangers of using internet technologies.

At Long Lawford Primary School, we understand the importance of educating our pupils in online safety issues, teaching them the appropriate behaviours and critical thinking to enable them to use these resources safely and responsibly, in and beyond the school environment.

End-to-End Online Safety

Online safety depends on effective practice at a number of levels:

- Responsible ICT use by schools including all staff and students, as well as parents, governors and advisers, 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 Launch including the effective management of Smoothwall filtering and Policy Central monitoring.

Further Information

Warwickshire ICT Development Service - 01926 414100
Jane Key, Warwickshire ICT Development Service Online Safety champion - key.j2@welearn365.com

1.0 School Online Safety policy

1.1 Roles and Responsibilities

As Online Safety is an important aspect of safeguarding children, the Head and school governors have ultimate responsibility to ensure that the policy and practices are in place and monitored. The named Online Safety co-ordinator for the school is Tim Sutcliffe and the nominated governor for computing and Online Safety is Tim Sutcliffe. The Designated Safeguarding Lead (DSL) is Nicola Hetherington and the Deputy Designated Safeguarding Leads are Claire Stringer, Caron Bird and Jeanette McSweeney. The nominated governor for safeguarding

is Rachael Boswell. All members of the school community should be made aware of who holds these posts. It is the role of the Online Safety co-ordinator to keep up to date with current issues and ensure that staff members and children are informed appropriately.

All staff, children and parents/carers are required to give consent to images of their child being taken/used within school and on the school website, twitter page or blog pages.

1.2 Writing and reviewing the Online Safety policy

The Online Safety Policy is part of the School Development Plan and relates to other policies including those for child protection, behaviour and curriculum.

- The school has an appointed Online Safety Coordinator, DSL and deputy DSL as well as governor involvement.
- Our Online Safety Policy has been written by the school, building on the Warwickshire ICT Development Service Online Safety Policy and government guidance. It has been agreed by the Senior Leadership Team (SLT) and approved by governors.
- The Online Safety Policy will be reviewed annually.

1.3 Teaching and learning

1.3.1 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 and Online Safety are part of the statutory curriculum and a necessary tool for staff and pupils.

1.3.2 Internet use will enhance learning

- The school Internet access will be designed specifically for pupil use and will include appropriate filtering.
- Pupils will be taught what Internet use is acceptable and what is not and given clear rules for Internet use.
- Internet access will be planned to enrich and extend learning throughout the curriculum where appropriate.
- 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.

1.3.3 Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported the school Online Safety co-ordinator who should then report to Warwickshire ICT Development Service.
- Our School should ensure that the use of Internet derived materials by staff and by 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.

1.4 Managing Internet Access

1.4.1 Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses Launch broadband with its firewall and filters.
- The school has regular visits from a technician Launch.

1.4.2 E-mail

- Pupils may only use approved e-mail accounts via the learning platform on the school system.
- 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.
- E-mail sent to an external organisation should be written as carefully as a letter written on school headed paper would be. It must be authorised by the class teacher before sending via the teachers e-mail.
- The forwarding of chain letters is not permitted.

1.4.3 Published content and the school website

- 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.

1.4.4 Publishing staff and pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be named.
- Pupils' full names will not be used anywhere on the school website, twitter page or blog, particularly in association with photographs.
- Written permission from parents/carers will be obtained before photographs of pupils are published on the school website, twitter page or blog.
- Pupil's work can only be published with the permission of the pupil and parents.
- Images of staff should not be published without consent.
- Wherever possible images of pupils will be accessed via the learning platform.

1.4.5 Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- 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 and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.

- The school has a social networking policy for staff and governors as well as one for parents.

1.4.6 Managing filtering

- The school will work in partnership with the Warwickshire ICT Development Service and WES ICT, as well as Launch to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school Online Safety coordinator.
- SLT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.4.7 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.
- The use of memory sticks and CD ROMs is not permitted, their functionality having been replaced by the OneDrive.
- Pupils are not allowed to bring mobile devices into school. If a child needs to bring a mobile phone into school for any reason, it should be left at the school office until the end of the day. Any mobile device found in school will be sent to the school office for the child or parent to collect at the end of the day.
- The sending of abusive or inappropriate messages outside of school is forbidden (anti bullying and behaviour policies)
- Staff will use a school phone where contact with pupils or parents is required.

1.4.8 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2016.
- School have a Privacy Notice in place. Which is available to staff, children and parents.
- School have a GDPR policy and an Information Security Policy in place.
- Staff are trained regularly with regards to protecting personal information, and reviews are regularly undertaken.

1.4.9 Online Safety Rules for Children, Visitors and Staff

All staff, visitors and children follow the below online rules when on school site:

- Use our own username and password
- Keep our personal information secure
- Communicate with others respectfully
- Only access suitable content
- Report any inappropriate content immediately
- Do not access social media

A breach of these rules will result in having access to the internet and school devices removed, or from being banned from school site.

1.5 Policy Decisions

1.5.1 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- Parents will be asked to register an objection if they do not wish their child to access the Internet within school.

1.5.1 Password Security

- All staff are provided with an individual network username and password.
- Staff are aware of their individual responsibilities to protect the security of the school network systems.
- All pupils are provided with an individual network username.
- Pupils are not allowed to deliberately access material or files on the school network of their peers, teachers or others.

1.5.3 Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 WCC can accept liability for the material accessed, or any consequences of Internet access.
- The headteacher and Online Safety co-ordinator will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.
- The school will audit ICT provision to establish the effectiveness and implementation of the Online Safety policy.

1.5.3 Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by the Online Safety co-ordinator or a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher who should use the agreed WCC procedures.
- 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.
- Sanctions within the school behaviour and discipline policy include:
  – interview/counselling by headteacher;
  – informing parents or carers;
  – Removal of Internet or computer access for a period of time.

1.5.4 Community use of the Internet

- The school will liaise with local organisations (e.g. the Police) to establish a common approach to Online Safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

1.6 Communications Policy

1.6.1 Introducing the Online Safety policy to pupils

- Pupils will be informed that Internet use will be monitored.
- An Online Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.

1.6.2 Staff and the Online Safety policy

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced via Policy Central to the individual user. Discretion and professional conduct is essential.
- A laptop issued to a member of staff by the school remains property of the school. Users of such equipment should therefore adhere to school policy both in and out of school.

1.6.3 Enlisting parents' support

- Parents' attention will be drawn to the School Online Safety Policy in newsletter and on the school website.

1.6.4 Monitoring and Review

- This policy is implemented on a day-to-day basis by all school staff and is monitored by the Online Safety co-ordinator.
- The effectiveness of this policy will be reviewed annually by the governors during reviews with the Online Safety co-ordinator, Computing co-ordinator, DSL, deputy DSL and the governors responsible for computing and child protection.

Online Safety Policy Update – COVID-19

During the COVID-19 outbreak during Spring 2020, school was closed to the majority of pupils for a number of weeks. To maintain contact between staff and students, Microsoft Teams was set up to facilitate this. Microsoft Teams is part of the welearn365 package and as such can be used to contact staff and pupils of Warwickshire schools. Members of the public are not able to access this.

Pupils have been given an individual login and have either had a unique password given to them or were required to change their password when first logging in.

To monitor the use of the chat feature, all adults associated with a class are able to see the conversation as well as members of SLT and Mr. Sutcliffe. Private chats are unable to be monitored. However, clear guidance has been issued to staff and parents that this feature is NOT to be used.

All user of Teams must do in line with the Acceptable Use Policy published by Warwickshire County Council in March 2020 and the Staff Behaviour (Code of Conduct) Policy 2019.

We have asked all staff and students to observe the following when using Teams:

- Children (and parents) should not contact staff through an audio or video call or through private messaging.
- Staff can only reply to messages from children in the main message thread.
- All users should be courteous and respectful in all interactions.
- All users should be thoughtful and critical before sharing any information using Teams.
- All staff should report any safeguarding concerns via an electronic green form to Nicola Hetherington and Claire Stringer.

Parents have been reminded about the importance of monitoring their children's internet usage in general, as well as ensuring they are respecting the guidance they have been given relating to Teams. Regular reminders will be sent to parents and children regarding appropriate use of Microsoft Teams.

All staff devices continue to be monitored by WCC ICT (regardless of these devices being used off school site). Any contravention of the Acceptable Use Policy (including offensive language or inappropriate websites) will be screenshot and sent to WCC ICT. This information will then be shared with the headteacher, and could result in disciplinary action.