# Trinity CE Primary School

# Online Safety Policy

## Creating and reviewing the online safety policy

The online safety Policy is linked to the School Development Plan and has been developed in accordance with Child Protection, Safeguarding and ICT policies to ensure coverage.

The school will have a designated online safety officer. This may be the Child Safety Officer as there are similarities between roles.

This online safety policy has been created by the school based on Northampton County Council guidelines and wider government policies.

## Why is this policy necessary?

The internet and the services it can provide has risen considerably over the last decade. Whilst the internet and technology itself can be a helpful resource in a child's education, be that for research purposes or for communication, there are risks involved with a form of media that any person can access. This policy has been created with the aim of minimising those risks in the following ways:

Teaching and Learning: How we teach the children about safe use of technology.

Managing access: The filtering systems in place to ensure children are protected from inappropriate content and the schools capability to deliver secure access.

Email: The usage by both staff and in the future pupils and the safety precautions taken.

Publishing: Protecting both staff and children by limiting the details that we publish.

Social Media: Filtering and Educating.

Safeguarding: Individuals access to the internet within school, risk management of internet usage and reporting of incidents.

## Teaching and learning

**Why Internet use is important**

The Internet is an invaluable resource in the modern age, allowing collaboration, communication and providing educational content in both business and personal capacities. The school has a duty to ensure children have high quality internet access to further their education.

Internet usage is also part of the statutory curriculum requirements and is a necessary tool for both pupils and staff.

Children and Young People use the internet widely outside of school and need to learn how to evaluate internet information for themselves and take full responsibility for their safety and experience.

One of the main reasons schools use the internet is to raise educational standards, to promote achievements through pupils and support professional work of staff both within the school and further afield.

**Internet usage is a valuable resource**

The internet grants access to worldwide educational resources whenever and wherever children may need to use them. It can provide excellent interactive and engaging activities for pupils of all ages. The internet is also invaluable for staff as it allows them to access professional development content, contact one another both inside and outside of school and enables collaboration with other professionals. It also prepares children for the business world, as the majority of businesses communicate via email and it grants both pupils and staff access to experts in the field who may be too far away for face to face communication.

**Pupils will be taught to critically evaluate internet content**

Through ICT lessons on online safety children will be taught to evaluate websites and search results for their suitability and reliability, discussing how some websites may not be factual and others may be harmful to both computers and themselves.

Pupils will be given clear objectives whenever research and internet access is used in lessons, understanding what is acceptable and not acceptable whilst building on their information retrieval and comprehension skills.

Children will also be educated on copyright and the reasons behind it. Staff will ensure that pupils use of the internet complies with this law, as does their own.

## Managing access

**Safe usage by staff and school**

All staff must take responsibility for their own network use which includes:

- Content they access.
- Downloads of large files and the effect this could have on the service of others
- Work stations secured against unauthorised access (password locked when not in use).

Guarding against accidental error and deliberate actions which could affect security will be in place, with only the designated ICT consultant, the head teacher and the ICT coordinator having admin access to the network to make changes to accounts and programmes.

Access to the server is physically out of reach and restricted in a secure location. Software on the server such as virus protection and operating system will be kept up to date to ensure the security of the onsite network to both internal and external risks.

Regular reviews of school security, users with access and virus protection will take place and be updated accordingly. Any information leaving school containing personal data will be encrypted.

**Safe usage by pupils**

All children will have read and signed an Acceptable Use Policy letter which outlines responsibilities of using technology in school and the consequences for not doing so.

The school will work with the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved appropriately.

Pupils must tell an adult if they discover an inappropriate site and this will be logged by the online safety officer accordingly (for more details, see Safeguarding)

Filters will be regularly checked by senior staff to ensure they are appropriate, effective and reasonable.

**Safe usage by parents**

All parents will have been given and subsequently signed an Acceptable Use Policy form.

**Disclaimer**

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the internet and social media being so vast it is not possible to guarantee that access to undesirable material will never occur via a school computer or Wi-Fi. The school or organisation cannot accept liability for the material accessed, or any consequences resulting from the internet use.

## Email

Currently pupils do not have access to e-mail accounts in any form, however if/when these are established the following will apply:

- Pupils may only use their approved e-mail account on the school system.
- Pupils must immediately report any offensive e-mails to an adult immediately and this will be logged as an online safety incident.
- Pupils will be taught and must not give out personal details about themselves, other people or the school via e-mail without specific permission from a moderating member of staff.

School staff will ensure that they do not give out sensitive information to unknown parties. Any e-mails sent to external organisations will be written professionally mirroring their counterparts on school headed paper.

School staff will only use their school e-mail accounts for professional use to reduce the risk of spam and other high risk incoming e-mails from entering the system.

## Social Media

Staff must not under any circumstances accept networking requests from pupils. Pupils will be made aware of this.

All access to social media sites via the school internet will be blocked.

Children will be made aware of both the benefits and risks of social media. They will be taught not to reveal information about themselves which could identify them or their location, or the identity and location or another person.

Parents will be advised that social media use for primary age pupils is inappropriate and contradicts terms and conditions from social media sites themselves.

## Safeguarding

All staff, pupils and parents must have signed the acceptable use policy before accessing the internet within school.

Filters will be put in place to block any inappropriate content from reaching children. Again due to the vast nature of the internet the school nor NCC can accept any liability for an inappropriate website appearing. Steps will be taken however to log this as detailed in the reporting section and the filter will be updated to exclude that website from appearing again. Filters will be regular checked and updated to ensure no new sites are able to pass through unless appropriate.

The school shall regularly review the ICT provision and online safety policy to ensure that it is both adequate and continues to be effective.

## Monitoring and Reporting

The school has a very robust internet filtering system monitoring usage online. This system has been set up to block certain words or phrases from appearing on screen. This is adapted and added to when necessary, normally after any incidents have been occurred.

The online safety lead receives a monitoring report produced by the system every week regarding any ‘suspicious searches’. If this report identifies ay unsuitable searches, these are fully investigated by the online safety lead and the head teacher is notified. As the system identifies the user of the machine when the search was carried out, if necessary, action is taken against any individual (please refer to Acceptable Use Policy and Staff Code of Conduct for further information) acting inappropriately.

## Filter Change Requests

All staff, pupils and parents are able to request a filter change after discovering information that may concern them. There is a clear reporting structure in place for any online safety complaint or concern. Pupils have been taught to inform an adult of any inappropriate pages or activities and have been told about using CEOP to report serious incidents. Within school, forms are available for staff to complete which give details about any online safety incident, including the URL of the offending site and a detailed description of the incident. A log shall be maintained providing an overview of online safety incidents. This log shall be reviewed regularly by the online safety lead to ensure safety of the pupils.

An online form is also available to parents to log any such incidents, especially that of cyberbullying. These will be discussed with a member of staff and details verified before entering the online safety log.

## Use of Personal Mobile Technologies

Pupils are not permitted to bring personal mobile technology into school and therefore no use of these are permitted on school site. However, should a parent or pupil have a particular need for a child to bring a personal device to school on one particular occasion, then this will need to be discussed and agreed with the Executive Head Teacher. If agreed, the child will need to hand in the mobile device to the school office at the beginning of the day for it to be stored securely until the end of the day when the pupil can collect the device. This is only agreed in very exceptional circumstances. No use is permitted on school transport.

Staff are permitted to bring mobile devices to school but these should be stored securely during the day and out of reach and site of pupils. The mobile devices should not be used in the presence of children. Staff are not permitted to use the schools wi-fi unless special agreement has been granted or they access the wi-fi designated for visitor use. This is to enable better and more accurate monitoring of the system by pupils and other users.

Parents are permitted to bring mobile devices on site for the purpose of taking photos of their own children in events. It is made clear to the parents, through the acceptable use policy as well as verbal reminders at each event, that photos that are taken are to be used for their own personal use and not to be uploaded to any social media platform as other children may be visible in their photographs. The school reserves the right to remove this permission at any time or during any event in order to safeguard all children.

For further details, please refer to the acceptable use polices for parent, children and staff, staff code of conduct, safeguarding children policy and our visitor information booklet.

## 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.

## Protecting personal data and information

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2016.

## Managing the policy

**Communication to pupils**

All pupils will be made aware of the rules of using technology within school and will have signed the AUP. The rules for using technology, drawn from these, shall be displayed in classrooms.

**Communication to parents**

Parents will have also been made aware of the rules the pupils agree to when using technology within school through the AUP. The online safety policy will also be made available on the school website for parents to access should they require more details.

**Communication to staff**

Staff will have been consulted and the important of the online safety policy explained to each individual member. Any causes for concern will have been addressed before the publication of this policy.

Staff should know that all internet traffic can be and will be monitored for protection purposes.

Professional conduct and discretion when using technology is essential.

**Communication to governors**

Governors will have been made aware of and consulted on the online safety policy. The importance of online safety will have been discussed with governors and this policy ratified before being officially published by the school.

## Review

This policy will be reviewed annually by the online safety lead and a member of the leadership team to ensure it remains current.

**Signed ICT coordinator**……

**Signed Head Teacher**……

**Signed Chair of Governors** ……