Tanfield Lea Community Primary School

E-Safety Policy

Introduction

Tanfield Lea Community Primary firmly believes that the effective use of information and communication technologies in school can bring great benefits. Recognising the e-safety issues and planning accordingly will help to ensure appropriate, effective and safer use of digital technologies.

Scope of the Policy

This policy has been written by the school, agreed by the Leadership Team and approved by Governors. It applies to all members of the school community (staff, pupils, volunteers, parents / carers, visitors and community users and other individuals who work for or provide services on behalf of Tanfield Lea Community Primary School) who have access to and are users of the school ICT systems both in and out of school.

Tanfield Lea Community Primary School will deal with such incidents within this policy (and associated behaviour and anti-bullying policies) and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that will take place inside and outside of the school.

Context

We live in a digital age where technology is playing an ever increasing part of our lives; it is changing the way that we do things both inside and outside of school and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, pupils and parents / carers associated with the school are to use technology in a safe and responsible manner.

Some of the potential dangers of using technology may include:

- Inappropriate use of social media
- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- Inappropriate communication / contact with others including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the online world but it is important that as a school we have a planned and coordinated approach to ensuring that all involved with the school use technology in a safe and responsible way. As with all risks it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

Why Internet use is important

The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through ICT and Internet use.

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- 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.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

How the Internet benefits 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.

Benefits of using the Internet in education include:

- 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
- exchange of curriculum and administration data with DCC and DFE;
- access to learning wherever and whenever convenient.

Enhancing learning using the Internet increased computer numbers and improved Internet access may be provided but its impact on pupils learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

- 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 given clear objectives for Internet use.
- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.

• 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 to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Learning how to evaluate Internet content

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

• Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

• The evaluation of online materials is a part of teaching/learning in every subject.

Managing Information Systems

The security of the school information systems and users will be reviewed regularly. Virus protection will be updated regularly. The school will comply with the terms of the data protection act and the General Data Protection Regulation , and is responsible for registering with the information commissioner's office advice is available from www.ico.gov.uk/for_organisations/sector_guides/education.aspx

● Personal data sent over the Internet or taken off site will be encrypted.

● Portable media may not be used without specific permission followed by an anti-virus / malware scan.

● Unapproved software will not be allowed in work areas or attached to email.

● Files held on the school's network will be regularly checked.

● The ICT coordinator/network manager will review system capacity regularly.

● The use of user logins and passwords to access the school network will be enforced.

• 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.

• 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. Wide Area Network (WAN) security issues include:

• Unapproved software will not be allowed in pupils' work areas or attached to email.

• Files held on the school's network will be regularly checked.

• The Technician will review system capacity regularly.

- Only the minimum amount of data required to operate a system will be uploaded

Social Media

Social media is now an everyday part of modern life. Communicating online with friends, colleagues is common place thanks to the rapid rise of platforms such as Twitter.

Tanfield Lea Community Primary School recognises the major benefits social media has brought in its communication with pupils, parents, and the local community.

The school has embraced social media, creating its own Twitter account and using blogs.

The school has much to celebrate and share with its audiences and will continue to adopt the latest technology to do this. But communication through social media has to be balanced with our duties as a school, our legal responsibilities and guarding our reputation.

School has set out guidelines in its Social Media Policy about what is and what is not acceptable behaviour. The School Social Media Policy aims to balance our continued support of innovative communication with good practice requirements.

Managing 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. In the school context (as in the business world), emails should not be considered private and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation. Spam, phishing and virus attachments can make email dangerous.

- Pupils may only use approved email accounts.
- 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.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.

Managing published content

Publication of information should be considered from a personal and school security viewpoint.

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images or work

Still and moving images and sounds add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount.

- Written permission from parents or carers will be obtained before images of pupils are electronically published.

• Images that include pupils will be considered carefully.

• Pupils' full names will not be used anywhere on the website and names will never be used in association with photographs.

Managing social networking, social media and personal publishing

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control. For responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. 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 should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. 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, instant messenger and many others.

• The school will control access to social media and social networking sites.

• Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

• Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.

• Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others by making profiles private.

• Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

How filtering will be managed

The school's broadband access will include filtering. The school will have a system in place to make changes to the filter and the HT is responsible for authorising changes. The school will work with DCC to review filtering. The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure. If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate. The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.

● Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.

● Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Durham Police or CEOP

● The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

Protecting personal data

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 2018 ("the Act") and the General Data Protection Regulation gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled

properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 2018 and General Data Protection Regulation applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (six data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The six principles are that personal data must be:

- Processed fairly and lawfully
- Purpose limitation
- Data Minimisation
- Accurate and up-to-date
- Not held no longer than is necessary
- Kept secure (integrity and confidentiality)

Managing video conferencing

All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

- Videoconferencing contact information will not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care. Users Pupils will ask permission from a teacher before making or answering a videoconference call. Videoconferencing will be supervised appropriately for the pupils' age and ability. Parents and carers consent should be obtained prior to children taking part in videoconferences.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Policy Decisions

Authorising Internet access

The school should allocate Internet access for staff and pupils. In school, where pupil usage should be fully supervised, all pupils in a class could be authorised as a group. Normally most pupils will be granted Internet access. Parental permission will be required for Internet access in all cases.

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read and sign the 'Staff Acceptable Use Policy' before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials.
- Parents will be asked to sign and return a consent form for pupil access.

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 DCC can accept liability for the material accessed, or any consequences resulting from Internet use. The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

● The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Durham Police.

● Methods to identify, assess and minimise risks will be reviewed regularly.

Responding to incidents of concern

● All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).

● The e-Safety Coordinator will record all reported incidents and actions taken in the School e-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 e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.

● The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.

● The school will inform parents/carers of any incidents of concerns as and when required.

● 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 e-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 e-Safety Officer.

● If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other schools in Durham.

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 e–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.

● All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

● Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.

● Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.

● All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How is the Internet used across the community

● The school will liaise with local organisations to establish a common approach to e– 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.

● The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

● The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

Managing Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. 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.

● 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, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

● Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

● Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

.

Managing the use of mobile phones in school

The use of mobile phones and other personal devices by staff in school will be decided by the school and covered in the school Acceptable Use or Mobile Phone Policies. Children are only allowed a mobile phone in school if parents have specifically requested this due to the arrangements for the child going home at the end of the day. If this is the case then the child would be required to bring their phone to the office first thing in the morning (with a letter from parents explaining why it is needed in school). It will then be locked away –switched off – until being returned to the child at the end of the day.

Staff Use of Personal Devices

● 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 unless authorised to do so by the Senior Leadership Team.

● Mobile Phone and devices will be switched off or switched to ‘silent’ mode.

● Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils during the normal school day when a school iPad is available but may be used (if no alternative) hen out on a school visit e.g. photo to tweet. Once the photos has been used it should be deleted (within the same school day)

● If a member of staff breaches the school policy then disciplinary action may be taken.

How will parents’ support be enlisted?

● Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.

● Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.

● Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.

● Interested parents will be referred to organisations listed in the “e–Safety Contact and references section”

E-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre):

www.ceop.police.uk Childline:

www.childline.org.uk Childnet:

www.childnet.com Children’s Safeguards Team:

www.kenttrustweb.org.uk?safeguards Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk Cybermentors:

www.cybermentors.org.uk Digizen: www.digizen.org.uk Internet Watch Foundation (IWF): www.iwf.org.uk Kent e–Safety in Schools Guidance: www.kenttrustweb.org.uk?esafety Kidsmart: www.kidsmart.org.uk Teach Today:

http://en.teachtoday.eu Think U Know website: www.thinkuknow.co.uk Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.co