Denton Community Primary School

E-safety and Acceptable Use policy

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying, social media and child protection.

- The school will appoint an e-Safety Leader. This person is Guy Walsh, Head Teacher.
- Our e-Safety Policy has been written by the school, building on government guidance. It has been agreed by senior management and approved by governors.

- The e-Safety Policy was revised by: …Guy Walsh and SLT members, September 2017

- It was approved by the Governors on: … …22.5.18

- The next review date is (at least annually): May 2019

Section 1

1.1 Teaching and learning

1.1.1 Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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.

1.1.2 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 shown how to publish and present information to a wider audience.
- Pupils will be given access to an online learning platform where they will learn to use different forms of communication such as forums, wikis and email and to use the internet to store and retrieve their own work

1.1.3 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 will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content by contacting the e-safety leader.
- Pupils will take part in discrete safety lessons in each year group following the East Sussex County Councils e-safety lesson plans
- Parents will be given a copy of the Pupil Acceptable Use Agreement (section 3) and asked to sign it after talking the content through at home.

1.2 Managing Internet Access

1.2.1 Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

1.2.2 E-mail

- Email use must follow the guidance of the staff and pupil Acceptable use agreements (sections 2 and 3).

1.2.3 Publishing pupil's images and work on the school website

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Photographs of pupils will not be published on the school Web site if this goes against the wishes of parents/guardians
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

1.2.4 Social networking and personal publishing The school will control access to social networking sites, and consider how to educate pupils in their safe use.

- Pupils in upper juniors will be taught specifically about social networking sites
- All access to social networking sites will follow the acceptable use agreements in sections 2 and 3
- A separate Social Media policy for Denton CP School should be referred to when creating and managing social media on behalf of Denton CP School

1.2.5 Managing filtering

- The school will work with East Sussex County Council to ensure systems to protect pupils are reviewed and improved.
- Content on the school Learning Platform will be screened and filtered by e-schools
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety leader following the attached flow
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.2.6 Managing videoconferencing & webcam use

- See Acceptable use agreements in sections 2 and 3

1.2.7 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 senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

1.2.8 Protecting personal data

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

1.3 Policy Decisions

1.3.1 Authorising Internet access

- All staff must read and sign the Acceptable Use Policy before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Parents will be asked to sign and return a consent form.

1.3.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor ESCC can accept liability for any material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

1.3.3 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. (See flowchart of responses to an incident of concern in section 4.)
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy) where appropriate.
- Pupils and parents will be informed of consequences for pupils misusing the Internet

1.4 Communications Policy

1.4.1 Introducing the e-safety policy to pupils

- E-Safety rules will be regularly referred to in all year groups appropriate to the task in hand.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed and taught in each year group.
- E-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.
- All children will be required to sign the Pupil Acceptable Use Agreement (differentiated for Key Stage 1 and 2)

1.4.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety and acceptable use Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff who manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- No access to ICT resources will be granted until the Staff Acceptable Use Agreement has been read and signed
-

1.4.3 Enlisting parents' and carers' support

- Parents and carers attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers. Regular resources and e-safety information will be sent home.
- The school will ask all new parents to sign the Pupil Acceptable Use Agreement when they register their child with the school.

Section 2

Denton CP School Staff ICT Acceptable Use Agreement

Denton CP School provides a range of ICT resources which are available to all staff. In order to ensure the safety of both staff and pupils, it is important that all staff follow the guidelines detailed below.

Terms of Acceptable Use:

1. **Application of Agreement**

   This policy applies to all staff of the school, regardless of their use of ICT systems

2. **School Email**

   Every member of staff is provided with a school email address. The email system can be accessed from both the school computers, and via the internet from any pc.

   The sending of emails is subject to the following rules:

   - Language must not include swear words, or be offensive or abusive.
   - Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
   - Sending of attachments which contain copyright material to which the school does not have distribution rights is not permitted.

   Limited personal use of the email system is permitted, provided that it complies with the guidelines set out in section 4 of this policy, and that any content complies with the rules above. Staff should keep levels of personal email to a minimum.

   All email within the school is monitored, and email accounts can be checked in order to ensure compliance with the above rules.

   All staff should be aware that email is not a secure communications medium, and therefore should not be used for the transmission of confidential files or staff / student data.

   Staff are not permitted to send via email any information which is covered by the Data Protection Act, without prior written authorisation from the schools data protection officer.

   Other than the examples listed above, use of email should comply with the ESCC E-mail use policy.

3. Internet Access

The school provides internet access for all staff and pupils in order to allow access to the wide range of content available.

The schools internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasion it may be possible to view a website which is inappropriate for use in a school; in this case the website must be reported in writing (e-mail) to the ICT Support Manager.

It is not permitted to attempt to access, on any device, pornographic, illegal, sexist, violent, racist or inappropriate material in school.

Members of the ICT Support Team have access to an unfiltered internet connection. Access is still only permitted to appropriate websites, unless directly instructed by the Head Teacher.

The use of online real-time chat rooms is banned, unless specific permission is sought from the Head Teacher.

The use of personal online email accounts, such as Hotmail, is permitted, provided that the usage complies with Section 4 of this policy, and that no attachments are downloaded onto the school network. Any emails sent using this system must comply with Section 2 of this policy.

No member of staff may download any software from the internet for installation onto a school computer system without prior written authorisation from the ICT Support Services Manager.

In addition to the examples listed above, use of the internet should comply with the ESCC Internet access and use policy.

4. Personal use of Equipment

The ICT provisions provided by the school are for work relating to the School. However the school acknowledges that, on occasion it may be necessary to use the ICT equipment for personal use. This is permitted provided that:

- Any activities carried out on them comply with the other terms of this policy.
- No personal applications are loaded onto any computers.
- Any activity completed on school equipment does not result in personal gain for the member of staff involved.
- The removal of ICT equipment from the school site for personal use is only permitted with the consent of the ICT Support Services Manager. The exception to this is any equipment assigned to, and signed for by individual members of staff.
- Any personal calls made using the School's phone system must be declared to the School Finance Secretary and paid for. All calls are logged and may be recorded.

All staff members are responsible for reporting their own personal use of a school computer, and any associated tax costs this has.

No technical support is provided by the school for problems arising as a result of personal work on the equipment.

5. Digital cameras

The school encourages the use of digital cameras and video equipment. However, staff should be aware of the following guidelines:

- Photos should only be named with the pupil's name if they are to be accessible in school only – photos for the website or press must only include the child's first name.
- The use of personal digital cameras in school is permitted, except those which are integrated into mobile phones. However, images of children must be downloaded to the school network and removed from the camera before it leaves the school site.
- All photos should be downloaded to the school network
- The use of mobile phones for taking photos of pupils is not permitted.

6. Security

All staff using any of the School's information systems will comply with the School's information access and security policy.

Each member of staff is allocated a username and password. Staff are responsible for ensuring their password remains a secret and their account is secure. Staff are not permitted to write their password down.

Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner. When any pc is left unattended, it must either be logged off or locked. No member of staff may use a computer which is found logged on as someone else; it must be immediately logged off.

Passwords must be regularly changed in accordance with the information access and security policy.

Staff will only access areas of the school's computer systems to which they have been authorised access.

7. File Storage

Each member of staff has their own personal area on the network, as well as access to shared network drives. Any school related work should be stored on one of these network drives. Personal files are not permitted on the network areas, but may be stored on individual's laptops, provided this does not affect the performance of the laptop.

All staff should be aware that any files stored on a laptop computer are not backed up, and no attempt will be made to recover them in the event of a fault developing with the laptop.

Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files.

Any files stored on removable media must be stored in accordance with the information access and security policy, summarised as follows:

- No school data is to be stored on a home computer, or un-encrypted storage device.
- No confidential, or School data which is subject to the Data Protection Act should be transferred off site using unsecure email.

8. Video Conferencing

The school makes use of video conferencing facilities. All conferences should be checked with the ICT dept, before organising with the third party.

9. Mobile Phones

Mobile phones permitted, with the following restrictions:

- They are not to be used when you are directly supervising or working with children.
- Mobile phone cameras are not to be used on the school site, or any school outings. The school provides digital cameras for this purpose.
- All phone contact with parents regarding school issues will be through the school's phones.

10. Social networking

Denton CP School has a separate Social Media Policy. The key requirements for staff are as follows:

For the purposes of this section the term 'friends' is used to define any link created between the online profiles of 2 or more people.

Under no circumstances are staff permitted to be 'friends' with any pupil of the School who is not a direct relative.

The School recommends that staff are not 'friends' with any ex pupil of the school who is under the age of 18.

No details or opinions relating to any pupil are to be published on any website.

No opinions regarding another member of staff which could cause offence are to be posted

No communication should take place between pupils and staff members using any online service apart from the school's email or Learning Platform service.

No communication should take place between parents of pupils or pupils and staff members regarding any issues relating to the school or pupils using social networking sites.

No photos or videos which show pupils of the school who are not directly related to the person posting them should be uploaded to any site other than the school's Website or Learning Platform.

No comment, images or other material may be posted anywhere, by any method that may bring the school or, the profession into disrepute.

The school disciplinary policy is available to the Head Teacher to address any breach of this policy.

Staff Agreement

As a school user of the network resources, I agree to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the ICT Support Team.

I agree to report any misuse of the network to the ICT Support Services Manager.

I also agree to report any websites that are available on the school Internet that contain inappropriate material to The ICT Support Services Manager

Lastly I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to The ICT Support Services Manager or Head Teacher.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Signed …….. Date ……..

Print name ……

Section 3

Denton CP School Pupil ICT Acceptable Use Agreement

Denton CP School provides a range of ICT resources which are available to you to help you learn and access the best online information to help you find out about your world. We want you to use the ICT facilities safely, and with respect for yourself and other users. We want you to tell us if you have a problem and we will help to put it right.

We hope that all out ICT users will develop safe practices that show respect for all other users. The School Behaviour and Disciplinary Policy also applies to ICT use.

Terms of Acceptable Use:

11. Application of policy

This policy applies to all school-provided ICT equipment, and to pupils' uses of ICT whether in school or not, and whether they occur inside or out of normal school hours.

12. School Email

Every pupil from year 3 onwards is provided with an email address, which they can use to send email to other pupils and teachers' school email addresses. No external email facilities are provided for pupils, and staff will not respond to emails sent to them at any address other than their school email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the school does not have distribution rights is not permitted.
- The forwarding of "blank" emails is prohibited, as is the sending of emails with malicious software attached.

All email within the school is monitored, and email accounts can be checked in order to ensure compliance with the above rules.

13. Internet Access

The school provides internet access for all pupils in order to allow access to the wide range of content available.

The school's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasion it may be possible to view a website which is inappropriate for use in a school; in this case the website should be immediately reported to the class teacher.

The use of online real-time chat rooms is banned, unless specific permission is given by the class teacher.

No attempt must be made to access personal email accounts, such as Hotmail. Pupils must only use the school-provided email system when working in school.

Photos, videos and written information must not be uploaded to any website other than the school Learning Platform.

No pupil is permitted to share any personal information with anyone on the internet unless specific permission if given by the class teacher.

14. Personal use of Equipment

The ICT provisions provided by the school are provided for school work only. Only activities which have been assigned by the class teacher are permitted.

The only exception to the above rule is the use of E-learning laptops at home. These may be used for any purpose, subject to the following conditions:

- The usage does not cause any physical damage to the laptop.
- No attempt is made to enter the BIOS of the laptop.
- They are not used for any illegal activities.
- Non school work is not saved to the thaw drive.

15. Digital cameras

The school encourages the use of digital cameras by pupils, and provides specific cameras for this purpose. Cameras are only to be used under direction from a member of staff. Photos and videos captured using the cameras should be appropriate, and not cause offence to anyone. Under no circumstances should acts of violence, invasion of privacy or any other infringement of the schools rules be recorded by a pupil.

16. Security

All pupils in year 3 onwards are issued with a username and password. No attempt should be made to access another pupil's user account. No pupils are permitted to share their username and password with anyone other than their parents /guardians.

All pupils have an account for access to the school's VLE. No pupil is permitted to access the VLE from an account other than their own.

Pupils are not permitted to use a computer that is logged on as a member of staff, unless under direct supervision from that member of staff.

Pupils must not leave any computer logged on when they are not using it.

If a pupil believes their password has been found out they must report it immediately to their class teacher.

17. File Storage

Each pupil has their own area on the network which should be used to store all of their work. In addition to this pupils in year 3 onwards have access to a memory stick, allowing children to save work done at home. All work stored should be appropriate for viewing in a school. The storage of music files, other than those created in school is not permitted.

No files which breach copyright law may be brought into the school.

18. Video Conferencing

The school makes use of video conferencing facilities. All video conferences are arranged by the class teacher, and are with third party education providers, who provide content appropriate to the age range of the pupils. The video conferencing facilities should never be used by a pupil unsupervised.

19. Mobile Phones

The School recognises that many parents wish their children to carry a mobile phone for a variety of reasons; however use of mobile phones by pupils is not permitted during school hours.

Mobile phones must be handed in to the School Office at the start of the day, to be securely stored until the end of the School day.

10. Social Networking

Denton CP School recognises the rise in popularity of Social Networking sites, and the rapid development of sites specifically targeted at primary aged children.

Pupils must not attempt to contact any members of staff or request to be 'friends' with them through any social networking site or personal email service.

Parents should not contact staff regarding any school issue via a social networking site. An email facility is provided for this purpose.

KS 2 Pupil's Agreement

I agree that:

- I will ask permission from a member of staff before using the Internet
- The messages I send will be polite and responsible
- I will not give my full name, home address, telephone number, any other personal information or arrange to meet anyone under any circumstances
- I will report any unpleasant material or messages sent to me to my teacher immediately
- I understand that the school will check computer files and will monitor the Internet sites that I visit
- I will not access other people's files
- I will only use my own username and password

Signed …….. Class ……..

Parent's Agreement

I have read and accept the Schools ICT Acceptable use policy. I have discussed the policy with my child.

Pupils Name …….. Date…….

Signed ……

KS 1 / Reception Pupil's Agreement

I agree that:

- I will ask an adult before using the computers
- I will follow the instructions of the teacher when on the computer
- I will not give my full name, home address, telephone number, any other personal information or arrange to meet anyone under any circumstances
- I will tell my teacher if I see anything on the computer which I think I shouldn't have done
- I understand that the teacher can check everything that is done on the computer.
- I will only open my own files
- I will only use my own class's username and password

Signed …….. Class ……..

Parent's Agreement

I have read and accept the Schools ICT Acceptable use policy. I have discussed the policy with my child.

Pupils Name …….. Date…….

Signed ……

Section 4

Denton CP School E-Safety incident flow chart