Fen Ditton C. P. School

I.C.T. ACCEPTABLE USE POLICY

Policy Review Schedule	
Last Updated	Next Planned Review and Update
18.4.13	18.4.15
22.2.2017	22.2.2019

Introduction

The internet is an essential element in 21st Century life for education and social interaction. The purpose of internet use in school is to promote pupil achievement, to support the professional work of staff and to enhance the school's management, information and business administration system. Benefits include:

- Access to worldwide resources and research materials
- Educational and cultural exchanges between pupils worldwide (Skype for instance)
- Access to experts in many fields
- Staff professional development such as access to online learning and forums
- Communication with support services, professional associations and colleagues
- Exchange of curricular and administration data (i.e. between colleagues, LA and DfE)

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. Consequently, in delivering the curriculum teachers need to plan to integrate the use of ICT and web based resources including e-mail to enrich learning activities. Effective internet use is an essential life skill.

Access to the Fen Ditton Primary School ICT network and use of ICT facilities owned by the school, including access to the Internet, are conditional on observance of Fen Ditton Primary School's Acceptable Use Policy. The Aims of this Acceptable Use Policy are to:-

- Allow all users access to school ICT resources and use of the Internet for educational purposes.
- Provide a mechanism by which staff and pupils are protected from Internet sites, information, and individuals that would undermine the principles and aims of the school.
- Provide rules which are consistent, and in agreement with the Data Protection Act 1984, Computer Misuse Act 1990 and other legislation relevant to the use of computers and electronic data in schools.
- Provide rules that are consistent with the acceptable procedures commonly used on the Internet, including those associated with netiquette.
- Provide rules relating to the use of computers and ICT facilities in school, which are consistent with the general policies of the school.

General Internet use and Consent

- Pupils who are to have access to the internet must understand the basic conventions and navigation techniques before going online and accessing material.
- Pupils must have returned a signed consent form before being allowed to use the ICT facilities that involve accessing the internet. (AUP KS1 or AUP KS2) The school will keep a record which will be regularly referred to by teachers and monitored by the Head teacher and admin staff. The use of the names of pupils or photographs of pupils for websites will require written permission from parent(s)/guardian(s) included on the consent form. If a picture is placed on the website the child's full name will not be displayed.
- **See appendix 1.1 Staff. Governor and Visitor code of conduct**
- **See appendix 1.2 KS1 Acceptable Use**
- **See appendix 1.3 KS2 Acceptable Use**
- Pupils must not use the school ICT facilities without the supervision of a member of staff. Although use of the ICT facilities and access to the Internet will be supervised, and all possible measures will be taken (including the use of E2BN Internet Service provider, filtering and firewall), Fen Ditton Primary School and Cambridgeshire County Council cannot accept liability for the accessing of inappropriate materials or any consequences of internet access.
- Fen Ditton Primary School is protected by E2BN filtering service, this is a live monitoring system which monitors and screen shots any inappropriate material viewed on a school computer. This material can be used as evidence in circumstances where a computer has been used to access such inappropriate material.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the ICT Co-ordinator immediately who will, in turn, record the address and report on to the Head teacher and Internet Service Provider.
- Pupils are aware that they must only access those services they have been given permission to use.
- Staff and pupils are made aware that the use of computer systems without permission or for inappropriate purposes is a criminal offence (Computer Misuse Act 1990)
- Staff and Governors must agree to and sign the Acceptable Use Agreement each year.
-

Log in and Passwords

- Pupils and staff must not disclose any password or login name given to anyone, or allow anyone else to use a personal account.
- Pupils and staff must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password.
- Staff and pupils must ensure terminals or lap tops are logged off (or hibernated) when left unattended.
- Adult users are expected to be in charge of their own areas on the network. Passwords are therefore set for each user. We recommend that passwords are changed frequently. Passwords should be over 4 characters and should contain letters, numbers and symbols. They should not contain spaces. Remember – passwords are case sensitive. "PASSWORD" is different to "password". To protect your work area do not tell anyone your password. The password is displayed on screen as a line of ******, however people watch fingers and it is quite easy over a period of time to work out what the password is, so be careful. Anyone who needs assistance in changing their password should contact the ICT Co-ordinator.

Learning Platform (VLE – Virtual Learning Environment) - Edmodo

- The school has a Virtual Learning Environment (VLE) provided by Edmodo. All pupils can have access to an area of the VLE to store and update their learning. These areas are password protected. Passwords are issued to children and shared with their parents for safe access at home.

General Safety and Risk Assessment

- The consumption of food or drink is forbidden whilst using a computer. It is hazardous to the equipment and to individuals.
- Users must treat with respect equipment and services in school and at other sites accessed through school facilities, and are subject to regulations imposed by the respective service providers. Malicious action will result in immediate suspension from use of the school facilities.
- Staff are responsible for sharing the safety issues with their pupils.

Cyber Bullying (see Anti-Bullying Policy)

The experience of being cyber bullied can be very painful for those who are the targets. Adults need to help children and young people prepare for the hazards of using technology while promoting learning and social opportunities. Some forms of cyber bullying are different from other forms:

- Through various media children can be cyber bullied 24 hours a day.
- People who cyber bully may attempt to remain anonymous.
- Anyone of any age can cyber bully.
- Some instances of cyber bullying may be unintentional – such as a text sent as a joke or an email to the wrong recipient.

Prevention

- We recognize that the best way to deal with cyber bullying is to prevent it from happening in the first place. By embedding good, safe ICT practice into all our teaching and learning, incidents can be avoided. Our community's principals of e-safety are contained in our e-safety policy.
- We recognize we have a shared responsibility to prevent incidents of cyber bullying but the Head teacher has the responsibility for coordinating and monitoring the implementation of anti-cyber bullying strategies.

Understanding Cyber bullying

- The school community is aware of the definition of cyber bullying and the impact cyber bullying has.
- Staff receive guidance and review the Anti-Bullying and Acceptable Use Policies regularly. Children are taught how to recognize cyber bullying and their responsibilities to use ICT safely. ICT safety is integral to teaching and learning practice in the school.
- Record Keeping and Monitoring Safe Practice
- As with other forms of bullying, the Head teacher keeps records of cyber bullying. Incidents of cyber bullying will be followed up using the same procedures as other forms of bullying. However, we recognize to monitor internet use on a regular basis as a disincentive for bullies misusing school equipment and systems. The ICT Co-ordinator will conduct regular use checks, log any concerns and inform the Head teacher.

E-Safety

- Children and staff are reminded of E-Safety Codes of Conduct at the start of each academic year.
- Any work or activity on the Internet must be directly related to schoolwork. Private use of the Internet (including social networking sites) in school is strictly forbidden.
- Staff are discouraged from being members of social networking sites. However, if staff are members they are reminded of the necessity to keep their profiles secure and to avoid contact with persons (particularly parents/pupils or ex-pupils) related to the school. Staff are reminded that any action or comment that brings the school or colleagues into disrepute or compromises pupil or staff confidentiality will be classed as a disciplinary matter.
- Do not give personal email or postal addresses, telephone / fax numbers of any person.
- Under no circumstances give email or postal addresses / telephone numbers / fax numbers of any teachers or pupils at school.
- Distribution of computer viruses, electronic chain mail, computer games, use of Internet Relay Chat and similar services are strictly forbidden by pupils and staff as they can result in degradation of service for other users and increase the workload of the IT staff.
- Do not download, use or upload any material that is copyright. Always seek permission from the owner before using any material from the Internet. If in doubt, or you cannot obtain permission, do not use the material.
- Users should assume that ALL software is subject to copyright restrictions, including shareware. Pupils must not, under any circumstances download or attempt to install any software on the school computers. Staff should seek the advice of the ICT Co-ordinator before attempting to download or upload software.
- Under no circumstances should users view, upload or download any material that is likely to be unsuitable for children or schools. This applies to any material of violent, dangerous, racist, or inappropriate sexual content. If users are unsure about this, or any materials, users must ask teachers or ICT co-ordinator. If in doubt, DO NOT USE. The transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden as they breach the laws of the UK under the Computer Misuse Act. Possession of certain types of unsuitable material can lead to prosecution by the police.
- Search engines (such as Google) should be used with care and generally only when the learning objective specifically demands it.

School Network and Pupil Files

- Always respect the privacy of files of other users. Do not enter the file areas of other users without obtaining their permission first. Files to be shared should be saved to the shared area “Pupil Templates” drive on the Fen Ditton Server. Pupils can access and save work to their own log-on through the server; this can only be accessed by that child and the administrators.
- Do not modify or delete the files of other users on the shared areas without obtaining permission from them first.
- The ICT Co-ordinator will view any material pupils store on the school's computers, or on memory sticks/disks pupils use on the school's computers.
- Storage space on the network is limited. All users are requested to ensure that old unused files are removed from their area at the end of each academic year. Users unsure of what can be safely deleted should ask the ICT Co-ordinator for advice. In exceptional circumstances, increased storage space may be allowed by agreement with the ICT Co-ordinator.
- Users accessing software or any services available through school facilities must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.
- Be polite and appreciate that other users are entitled to differing viewpoints. The use of strong language, swearing or aggressive behaviour is forbidden. Do not state anything that could be interpreted as libel.
- If the Edmodo VLE or network is accessed from home, the Acceptable Use Policy applies.
- Homework can be completed by pupils at home and saved to the school’s Edmodo VLE should they wish; pupils are issued with unique passwords. Storage devices from home are not encouraged to prevent the potential spread of viruses.

Security Guidelines

Backups

- Files stored on the network are backed up every evening. This means files can be restored if deleted or lost in error. However, if you create and delete files on the same day then a backup will not be available to restore. Backups are kept securely on the school site in a fire proof safe.

Save Regularly

- It is very important to save work regularly (approx. every 10 minutes). The network is very reliable but problems do occur i.e. programs crash, power failures. If work is saved regularly and a PC or the network does fail for any reason, only the work done since the last save will be lost. (See above)

Use your Network Area

- Always ensure that files are saved to your network area, NOT on the local hard drive. This will ensure that your work is backed up and can be retrieved in the event of a hardware failure or theft.

Home Documents

- The school cannot accept responsibility for personal documents held on school laptops, it is the responsibility of the user to backup documents created at home or stored on the Home Docs of the laptop.

Off-site pupil data and pupil information

- Lap tops and backups (USB sticks) may be taken off site. Staff are to ensure that lap tops are used cautiously when viewing pupil data/information and images and that lap tops are logged off when left unattended. Data, images and pupil information must be removed from backups and lap tops when pupils transfer to another class to avoid records being kept of pupils that are not taught by their former teacher.

Virus Checks

- All computers in school have antivirus software, although very new viruses will not be found. If you suspect a virus please report it to the ICT Co-ordinator straight away.

E-Mail Usage

- Use of e-mail and communication by e-mail should be treated with the same degree of care you would take if you wrote a letter to the person that you are contacting by email. It cannot be regarded as purely private, only to be seen by the receiver. E-mail can be stored, forwarded and distributed to large numbers of people at the touch of a button. It is easy to forget that it is a permanent form of written communication and that material can be recovered even if seen to be deleted from the computer

When using e-mail, pupils and staff should:

- Be aware that e-mail is not a secure form of communication and therefore pupils should not send ANY personal information.
- Should not attach large files
- Must not forward e-mail messages onto others unless the sender's permission is first obtained.
- Must not open e-mail attachments from unknown senders or from computers from which virus protection may not be current or activated
- Not send e-mail messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive.
- Must not open e-mail attachments from unknown senders or from computers from which virus protection may not be current or activated
- This Guidance will apply to any inter-computer transaction, be it through web services, chat room, bulletin and news group or peer to peer sharing.

Mobile Devices

- Pupils are not permitted to bring mobile phones or devices in to school. Should there be a need for a child to bring their device in to school this should be turned off and handed to the School Office to look after during the school day and collected at 3.25pm.
- Pupils may not make personal calls from a mobile phone during the school day.
- Mobile phones may not be used to take pictures of pupils and staff (use class cameras provided by the school)
- Pupils should not send or receive email or text messages to/from their mobile device during the school day.
- Any inappropriate use of mobile devices such as cyber bullying must be reported to the Head teacher (see Cyber bullying)

- Staff should only use their mobile phones at appropriate times of the day only e.g. break times. During the school day their mobiles should be turned off or set to silent. Staff must not use personal mobile devices or cameras to take images of pupils or staff.
- Any pupil who is seen with a mobile device during the school day will have their phone removed from them to be collected at the end of the school day (in accordance with the school's Behaviour Policy). The device will be secured in the school office.

Legal Requirements

- Users must agree to comply with all software license agreements. Do not attempt to copy any software from, or by using school computers. If you have any requirements for using additional software for any reason, please contact the ICT Co-ordinator to discuss the situation. Solutions are possible! Remember also that shareware is not freeware and must be licensed for continued use.
- Computer facilities shall not be used to hold or process personal data except in accordance with the provisions of the Data Protection Act 1984. Any person wishing to use the facilities for such a purpose is required to inform the Head teacher in advance and comply with any restrictions that the school or the UK Data Protection Registrar may impose concerning the manner in which data may be held or processed.
- Copyright Designs & Patents Act - Copyright is infringed if a person acquires an unauthorised copy of a computer program. Mere acquisition, without regard to the actual or intended use, constitutes an infringement of the author's copyright. "Acquisition" includes loading a copy of a programme into the random access memory, or other temporary storage device, of a computer, or onto any form of permanent data storage medium.
- The high cost of commercially marketed software and the ease with which it can be copied make it tempting to copy software illegally. Agents for software developers are aggressively seeking to protect their rights under the law. Schools can be audited at any time. Anyone found to have unauthorised copies of software will immediately be suspended from using the IT facilities. The matter will be investigated and the necessary action taken, the school will not accept any liability whatsoever.
- "Hacking" is illegal under the Computer Misuse Act 1990. Regulations regarding unauthorised access or misuse of computing facilities are enforceable under the law, any person found attempting to or hacking the school network will be prosecuted.
- Regulations regarding the transmission, storage or display of obscene material are enforceable by law under the Criminal Justice and Public Order Act 1984 which amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network.

Sanctions

- If pupils break the rules as laid down by this policy they will lose temporary or permanent use of the school systems. Parents will be informed and if the law has been broken the police will be informed and the school will assist the police with any prosecution.
- If staff break the rules as laid down by this policy they will lose temporary or permanent use of the school systems and will be subject to disciplinary proceedings. If the law has been broken the police will be informed and the school will assist the police with any prosecution.

Pupils with Additional Learning Needs

- The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

Video-Conferencing and Webcams

- The use of webcams to video-conference will be via E2BN which is a filtered service. Publicly accessible webcams are not used in our school setting.
- Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.
- Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always supervised by a member of staff and a record of dates, times and participants held by the school.
- Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).

Managing Allegations against Adults Who Work With Children and Young People

- In order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies we will refer to the Managing Allegation Procedure. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.
- Allegations made against a member of staff should be reported to the Senior Designated Person (SDP) for safeguarding within the school immediately. In the event of an allegation being made against a Head teacher, the Chair of Governors should be notified immediately.

Local Authority Designated Officer (LADO) - Managing Allegations:

- The Local Authority has designated Officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

Disciplinary Procedure for All School Based Staff

- In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

Additional Information

- Please be aware, at such time that you leave Fen Ditton Primary School, your user account and any associated files, your email address and any associated emails will be removed from the school system and will no longer be accessible. The school cannot continue to receive emails sent to your email address.
- If Pupils want a copy of any files within their user area or area of the VLE, they may, during the last month of Year 6 at Fen Ditton Primary School, seek support from the ICT Co-ordinator who can copy their files to disk or memory stick.
- If pupils, staff or parents do not understand any part of this Acceptable Use Policy, please ask the Head teacher for further guidance.
- A copy of this policy can be accessed by visitors on the Fen Ditton School Website.

Named Personnel

Our Named Governor for ICT Acceptable Use is Rob King (also Safeguarding Governor)
The Person Responsible for E-Safety and Acceptable ICT Use is Mr Mark Askew (Head teacher)
Policy Reviewed by Mrs Angela Nicholls (ICT Co-ordinator) – February 2017

Appendix 1.1
Acceptable Use Policy   Code of Conduct

Fen Ditton C. P. School

Staff, Governor and Visitor

I understand that this AUP is regularly reviewed and that there are consequences if I do not follow it.

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head Teacher or **Mrs Angela Nicholls** (School e-Safety Coordinator.)

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorized by the Head or Governing Body.
- I will not install any hardware of software without permission of the head teacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ………………………………… Date ……………………

Full Name ……………………………………………………………… Job title………………………………………………………………………

Appendix 1.2

Acceptable Use Policy **KS1 Primary Children**

I will read and follow the rules in the AUP

I understand that this AUP is regularly reviewed and that there are consequences if I do not follow it

- I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy
- I will use school computers for school work and not to upset or be rude to other people
- I will only use my school 2simple 2email accounts as assigned by my teacher in school
- I will not open or download any attachments without checking with an adult
- I will only go on websites that my teacher tells me to
- I will tell my teacher straight away if I go on a website by mistake
- I will tell a teacher straight away if I see a website that is not my work or receive messages from people I don't know.
- I will look after school ICT equipment and tell a teacher straight away if something is broken or not working properly
- I will not try to download or install any software on school computers
- I will only use the username and password I have been given for my year group
- I will save only school work on the school network and will check with my teacher before printing
- I will log off or shut down a computer when I have finished using it

- I understand that all of my work and internet activity on school ICT equipment can be seen
- I understand that I must follow these rules or I may get in trouble

- **Parent/Carer's Signature** ……………………………………….. **Date………………….**
- **Child's Name ………………………………………. Child's signature……………………………**

Appendix 1.3

Acceptable Use Policy KS2 Primary Children

I will read and follow the rules in the AUP

I understand that this AUP is regularly reviewed and that there are consequences if I do not follow it

- I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy
- I will only use school ICT equipment for my school work and not to upset or bully other people or create a bad impression of my school
- I will take responsibility for my own use of all ICT equipment and will use it safely, responsibly and legally *eg:*
    - I will only use my school Edmodo account in school to message pupils/adults
    - I will not open/download any attachments without checking with an adult
    - I will make sure that my work does not break copyright
    - I will not go on any unsuitable or illegal web sites on purpose e.g. rude images, violence and racism. If I go on any by mistake I will tell a teacher straight away
    - I will tell a teacher if I can see a website that is inappropriate or receive any unwanted messages (such as spam)
    - I will look after school ICT equipment and report any damage to a teacher straight away
- I will not try to get past any security measures in place to protect the school network
- I will only use the usernames and passwords I have been given and I will keep them secret (including Edmodo usernames and passwords)
- I will use Edmodo to transfer files between home and school. If I have to use a flash drive (USB memory stick) in school I will ask for an anti-virus check on it before I open my files
- I will save only school work on the school network and will check with my teacher before printing
- I will log off or shut down a computer when I have finished using it
- I understand that all of my work and internet activity on school ICT equipment can be monitored and that there are consequences if I do not use the equipment sensibly, safely and responsibly
- **Parent/Carer's Signature .... Date………………………………**
- **Child's Name ……………………………………………………… Child's Signature……………………………..........**