Longridge Towers School

CARPE DIEM

ACCEPTABLE USE OF ICT POLICY

Introduction:

Language used in this policy is deliberate and it is done so to ensure that all pupils understand clearly that the policy applies to them. Pupils should ask a teacher or other responsible adult if a word or words need explanation. Pupils are all taught how to use electronic devices safely and how to stay safe when using online technology. There is a link on the school intranet homepage to the ThinkUKnow e-safety website. However, parents/carers should be aware that that the use of personal smart mobile technology which is 3G and/or 4G enabled is **NOT** able to be filtered through the school system and so are strongly advised to take steps to set up appropriate controls on the devices which they give to their son/daughter.

The use of the latest technology is actively encouraged at Longridge Towers School but with this comes a responsibility to protect pupils, staff and the school from risk, harm or from abuse of the system.

All pupils, therefore, must adhere to the policy set out below. This policy covers all computers, laptops, tablets and electronic devices within the school, irrespective of who owns them. It also covers any irresponsible use of technology that occurs outside of school, which by its very nature, reflects badly on the school community.

All pupils are expected to behave responsibly on the school computer network, as they would in classrooms and in other areas of the school.

The Policy:

1. Personal Safety:

    1) Always be extremely cautious about revealing personal details and never reveal a home address, phone number or email address to strangers.
    2) Do not arrange to meet with anyone you have met on the Internet – people are not always who they say they are.
    3) Do not use the school computers to make online purchases or subscriptions.
    4) Always inform your teacher or another member of staff if you have received a message or have visited a website that contains inappropriate language or makes you feel uncomfortable in any way.
    5) Do not play with or remove any cables etc that are attached to a school computer.
    6) Do not attempt to attach a device (apart from a USB stick by the front port) to a school computer without first gaining permission from the Network Manager.
    7) Do not eat or drink whilst using the computer.

2. System Security:

1) Do not attempt to go beyond your authorized access. This includes attempting to log on as another person, or accessing another person's files. NB: You are only permitted to log on as yourself.
2) Do not give out your password to any other pupil. If you suspect someone else knows your password change it immediately.
3) Be kind to the schools computer systems, they are for your benefit.
4) Pupils wishing to use their own laptops or other device in school should in the first instance contact the Network Manager.

3. Inappropriate Behaviour:

Inappropriate Behaviour relates to any inappropriate electronic communication whether email, blogging (e.g. online diaries), social networking, texting, journal entries or any other type of posting / uploading to the Internet. The following section refers to behaviour both in and outside of the School and includes both the use of home and school computer systems. We are after all, a school community.

1) Do not use indecent, obscene, offensive or threatening language when communicating electronically. Be aware that sending images which may be deemed offensive or indecent is illegal and may be treated as a criminal offence.
2) Do not engage in personal, prejudicial or discriminatory attacks on any person or persons.
3) Do not access material that is profane or obscene, or that encourages illegal acts, violence, or discrimination towards any person or persons.
4) If you mistakenly access such material please inform your teacher, another member of staff, your parents or another responsible adult immediately.
5) Do not knowingly or recklessly send or post false, defamatory or malicious information about a person or persons.
6) Do not send spam (mail that is not asked for and/or likely to be deemed rubbish by the recipient).
7) Do not use the Internet for gambling.
8) Do not bully another person or persons by email, online, via texts or by any other electronic method.
9) Do not attempt to use proxy sites (site that try to bypass school security) on the internet.
10) Do not take a photo or video footage of another pupil or member of staff without their permission.
11) Do not post a photo or video footage of any other pupil or member of staff on the internet.

5. Plagiarism and Copyright:

1) Plagiarism is taking the ideas or writings of others and presenting them as your own. Do not plagiarise works that you find on the Internet or anywhere else and use them in your own work.
2) You should respect copyright. Breaking copyright law occurs when you reproduce a piece of work that is protected by copyright (and so law). Exam boards are now

increasingly sensitive to this issue and work included for submission should be copyright free.

6. Privacy:

   1) All files on the system are the property of the school. As such, the Network Manager and staff have the right to access them if required.
   2) All network access and web browsing on the school system is logged and routinely monitored to ensure the acceptable use policy has not been broken.
   3) Should it be deemed necessary, this information can be made hard copy.

7. Software:

   1) Do not install any software on the school system.
   2) Do not attempt to download programs from the Internet onto school computers.
   3) Do not knowingly install spyware or any sort of hacking software or device.

8. **Sanctions:**

   1) Sanctions can vary depending on the severity of the offence, from a warning or withdrawal of Internet use, to suspension or expulsion. Any breach of the law may lead to the involvement of the police.

9. General and Best Practice:

   1) Think before you print – printing is expensive and consumes resources, which is bad for the environment.
   2) Always log off your computer when you have finished using it.
   3) Always remove any USB memory stick you have been using and take it with you.
   4) Always back up your work if you are not saving it on the school system. Work saved on the school system is backed up every night for you, but be careful if you only have a copy of your work on a memory stick as you could lose it.
   5) Avoid printing huge files, if in doubt ask the Network Manager.
   6) Leave your computer and the surrounding area clean and tidy.
   7) If a web page is blocked that you feel you have a legitimate use for, please ask the Network Manager if it can be unblocked.
   8) If you are leaving the school for good, please ensure you have saved any files you want to keep to a memory stick or cd to take home, as these files will be deleted.

Other Electronic Devices:

It is the policy of the School that electronic devices are not used during lesson times unless direct permission has been given to do so. This policy should be read in conjunction with the Mobile Phone: Acceptable Use Policy which provides more detailed advice about these devices.

Longridge Towers School

CARPE DIEM

Pupil:

I have read and I understand the school's ICT and Mobile Phone and Portable Communications Devices Acceptable Use policies. I will use the computer system, Internet and any mobile phones/portable communication devices in a responsible way and obey these rules at all times.

Signed: ……..

Print Name: ……..

Date: ……..

Parent / Guardian:

As a Parent or Guardian I have read this agreement. I understand that although Longridge Towers School employs the latest filtering and security technology no system can be 100% safe. I give my son/daughter permission to use the school computer system. I am also aware that the use of personal smart mobile technology which is 3G and/or 4 G enabled **CANNOT** be filtered through the school system and understand it is my responsibility to ensure that suitable filtering is made on the device I give my son/daughter.

Signed: ……..

Print name: ……..

Date: ……

Reviewed: SB 01/09/2015
Reviewed: SB 01/09/2016
Review Date: August 2017