UNICORN SCHOOL

IT ACCEPTABLE USE AND eSAFETY POLICY (PUPILS)

This policy applies to all pupils at Unicorn School, including those in the EYFS.

This policy links to the Privacy Notice and the Data Protection policy.

RESPONSIBILITY

Staff Member:	Deputy Head/Bursar
Governors' Committees:	ICT/Risk & Compliance

Revised:	**June 2022**
Reviewed by Committee:	**November 2022**
Noted by Governors:	**November 2022**

IT ACCEPTABLE USE and eSAFETY POLICY (PUPILS)

OVERVIEW

Unicorn School provides access to internet, which is an important tool for school administration, teacher preparation and the educational development of all pupils.

However, along with the right to use these facilities comes the responsibility to use them appropriately. Therefore, use of the facilities must not be without restrictions, because the internet is essentially an unregulated medium. This policy describes the rules to be followed when using the internet and related technologies.

If any of the rules are contravened the School has the right to withdraw access to the IT equipment and the Head will be informed. In the case of a pupil, parents will also be informed.

PASSWORDS

All pupils in Yellow Class and above are allocated a user account (with no password) by the Head of Computing which gives them limited access to the School's computer system. During Green Class, a simple password is introduced which is increased in length during Blue. In Violet, password security forms part of the Computing curriculum and stronger passwords are introduced. The Head of Computing is responsible for explaining to the pupils the importance of:

- Choosing appropriate passwords
- Not sharing password information with others
- Not disclosing any personal identifying details on the internet

Pupils can save work on their individual account on the Q drive – this is the only access the pupil has to the School's drives.

THE INTERNET

- Unicorn School's computer and wireless network allow access to the internet through a real-time on-site managed filter service provided by Elmbrook Computers called the Untangle Next Generation Firewall. Although the web filtering is quite efficient, it is not 100% effective.

- Pupils only have access to computers when a member of staff is present and they are instructed to notify that adult if they see anything strange.

- At any time, the Head of IT may access an account and monitor website access, or saved files. This procedure is in place as a means of monitoring internet usage.

- All Unicorn pupils are under the permitted age to hold accounts on social media platforms, and access to such sites by pupils is not permitted on the School's computers, laptops and iPads.

- Any improper use of the internet is strictly prohibited. Improper use includes, but is not limited to, accessing or downloading any information deemed unsuitable to have in a school environment, in particular:

    - Pornographic material
    - Racist material
    - Depictions of violence
    - Harassing or defamatory material
    - Material that may target or influence pupils to participate in radicalism or extremism
    - Other material deemed offensive
    - Executable files or programs e.g. shareware, freeware, screensavers etc

- Information must not be plagiarised from the internet. A reference must accompany any data used.

- Computers must not be used to engage in hacking and other related activities.

- There must be no attempt to disable or compromise the security of the School's information.

- Pupils must inform the Head of IT of any virus warning or threat immediately.

- Staff must be aware of copyright implications if they download music or video files, and instruct pupils accordingly.

- Staff must be aware of copyright implications if they download shareware, freeware or other files, and instruct pupils accordingly.

Pupils must:

- Immediately tell a teacher if they see anything they are unhappy with or receive messages they do not like;
- Only be allowed to use the internet under supervision during class time in their classrooms, Computing lessons, or IT activity clubs;
- Not give out any personal information such as typing name and home address in a website form. If this type of information is requested then the pupil must tell a teacher;
- Not be allowed to access social media sites;
- Let the teacher know immediately if they see a virus warning or threat;
- Ask permission before entering any web site and give an educational reason for using the site: The only exception is if the teacher has pre-screened the site.

eSAFETY

IT and online resources are increasingly used across the curriculum. The School believes it is essential for eSafety guidance to be given to the pupils, parents and Staff on a regular and meaningful basis. eSafety is embedded within our curriculum and the School continually looks for new opportunities to promote eSafety.

- The School has a framework for teaching internet skills in Computing;
- The School also provides opportunities within a range of curriculum areas to teach about eSafety;
- At least twice a year assemblies are given on e-safety;
- Staff receive training on eSafety issues;
- The School invites outside experts to run regular workshops on e-safety for children throughout the School;
- The School also invites outside experts to run regular parent workshops on e-safety;
- Pupils are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also taught where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button.
- Cyberbullying will not be tolerated and any instances will immediately be dealt with under the Anti-Bullying policy.

Parents are encouraged to discuss IT awareness and eSafety with their children. On a regular basis, all parents are asked to complete the Primary Pupil IT Acceptable Use form on behalf of their child(ren) – see Appendix. This exercise is co-ordinated by the Deputy Head.

Amended CM June 2021

APPENDIX

Primary Pupil IT Acceptable Use
Agreement / eSafety Rules

- I will only use IT in school for school purposes.
- I will only use my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my IT passwords.
- I will only open/delete my own files.
- I will make sure that all IT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of IT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

Dear Parent/ Carer

IT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any IT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mr Gladstone or Mrs Walcot.

✂----------

Parent/ carer signature

We have discussed this and ……..(child name) agrees to follow the eSafety rules and to support the safe use of IT at Unicorn School.

Parent/ Carer Signature …….

Class …….. Date ……