The Place Independent School
E-safety home/school agreement

Parent/ Guardian name: _____

Pupil name:_____

E-safety agreement: As the parent or carer of the above pupil, I grant my permission for my child to have access to use of the Internet, school approved e-mail account and other ICT facilities at school.

I know that my child has signed an e-safety agreement form and that they have a copy of the '12 Rules for Responsible ICT Use'.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access e-mail, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent/ guardian signature: _____

Date: _____

The Place Independent School
12 Rules for Responsible ICT Use

Keeping safe: stop, think, before you click!

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework.

- I will only delete my own files.

- I will not look at other people's files without their permission.

- I will not bring files into school without permission.

- I will ask permission from a member for staff before using the Internet and will not visit Internet sites I know to be banned by the school.

- I will only e-mail people my teacher has approved.

- The messages I send, or information I upload, will always be polite and sensible.

- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.

- I will not give out personal information – such as my name, address, phone number, or e-mail – or send photographs or videos to people I don't know and trust.

- I will not arrange to meet someone I have only been in touch with online, unless I have my parent's or carer's permission and they can be present.

- I will keep all my login and password details to myself.

- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher/ responsible adult.

Child's name: _____

Signature: _____

Use of Computers, Confidentiality, the Internet and social utility sites

Young people's privacy is respected, their dignity encouraged and information confidentially handled. Staff and young people are kept safe and identities are protected.

The PLACE Independent school will take positive steps to protect the confidentiality of information stored on computer and to prevent unauthorised access and inappropriate use.

Due to the sensitive nature of the work we undertake, we need to protect ourselves personally, as well as the company and our young people.

The PLACE Independent school will provide children and young people with computers, printers and access to the internet. These facilities will not be abused, and the child or young person's and welfare is paramount. The PLACE Independent school will ensure children and young people are safeguarded.

What we do

Computer users will:
- Take appropriate measures to eliminate unauthorised access to the computer at the time of logging on by enabling the security features available with the machine
- Enable the computer's screen save facility so that the screen is blanked at regular intervals which reflect the amount of passing people.
- Never leave sensitive or confidential material on their screen when the computer is unattended.
- Ensure the computer screen is not easily visible to visitors.
- Delete information once details have been printed if not required to be kept in dedicated files on the computer.

Social Networking sites

- All employees must not use a computer to access any social networking sites during contact time with a young person or at any time during their working hours.

- All employees who use such sites out of work time should not disclose any information relating to their place of employment. There should be no mention of any matters related to work, i.e., situations that have occurred, names of houses, names of staff members, names of young people, etc on any

employee's home page. There should be no mention of work related issues whatsoever. To do otherwise will be in breach of confidentially in addition to failure to follow to instruction.

- Young people within our education should not be encouraged to access such sites. If a young person visits such a site in your company you should not take part in such activity and must record that the young person has accessed such a site in the young person's daily log and report to DSL, due to this breaching school computer security features. A young person should not be granted permission under any circumstances to access social media during school hours. If a young person should access social media they should be supervised closely and this should then be recorded on a school incident form, including details of the site which was accessed and then time it was used.

- All employees should never accept or instigate any contact on any such sites, including emails from the young people within our education, either presently or historically. Any such attempts at making contact with you should be immediately reported to your line manager.

We are encouraging all employees to be very aware that such social utility sites leave individuals vulnerable to the disclosure of personal information and therefore we are reminding everyone that they should use such sites with care and attention relating to who they make contact with and levels of security settings.

The PLACE Independent school staff must ensure:
- Young people are supervised when using IT Equipment.
- Computer equipment is looked after and any faults are reported straight away.
- Computers and printers are switched off when not in use.
- Young people share the facilities and take into account the needs of others.
- Staff and young people handle the equipment gently.
- Nobody eats or drinks in close proximity to the equipment.
- Young people don't send abusive, threatening or intimidatory e-mails or messages to anyone.
- Young people don't download files etc... without permission.
- Young people don't access illegal pornographic material.
- Young people don't tamper, try to repair, or relocate any equipment.
- Qustodio monitoring system is activated at all times to ensure the safe use of internet access.
- Qustodio monitoring is active on EVERY device that is used by young people, including any personal devices used (safeguarding requirement, see BYOD policy).

This Policy will be reviewed annually or sooner if Risk Assessments raise concerns.

This policy is use in conjunction with the schools E-Safety home/school agreement and the schools 12 rules for responsible use of ICT and BYOD policy.

Author: Cate Tumman
Current Policy: Jan 2022
Next review: Jan 2023