STONAR

Staff and Pupil ICT Acceptable Use Policy *Including EYFS*

Summary of key policy details

This policy applies to all school computers, personal laptops and also any tablets / mobile devices (including phones or 'smart watches') used in school, and also to online behaviour, towards other members of the Stonar community inside and outside school.

In line with EYFS regulations **personal mobile devices are not allowed in the EYFS setting.**

Prep School pupils are not permitted to have a mobile device in school without the express permission of the Head of Prep School.

Unless directed to by a member of staff, Senior School pupils (Yr 7-11) must not use mobile devices during the school day (8am – 6pm) or at sports fixtures or on school trips. Tablets that can access mobile data are not permitted at Stonar.

Staff mobile devices should at all times be set to silent / vibrate and may not be used when moving around the school campus.

Mobile devices must never be used in: changing rooms or toilets, when moving about the school campus, at the front of school, in corridors, or the dining hall regardless of the time of day / day of the week.

Pupils' tablets/laptops may be used in lessons with class teacher's permission.

Access to the internet must be via School Wi-Fi. 'Hot spotting' is not allowed. It is forbidden to use the School network to access, create or send material, which is offensive in the normal context of a school, or in breach of the law.

It is forbidden to distribute information about a third party / member of the School Community without their permission. It is forbidden to publish or share any information that defames, undermines, misrepresents, or tarnishes the reputation of the School or its users.

Electronic communication between staff and pupils must only be part of approved school activities, and only via approved forms of communication (for example, school email, SMHW, Edmodo, Kerboodle).

Any individual found using a mobile device to cheat in examinations or other formal testing opportunities will face disciplinary action.

Pupils and staff should report any suspicious online sexual advances or threatening behaviour to the Deputy Head or Houseparent / teacher *(and also to the authorities where appropriate).*

The School may, at any time and without further notice, monitor the use of IT systems and online behaviour to maintain safety and also compliance with this policy. It is not permitted to share passwords or log on details for accessing the school network. Personal mobile devices must be clearly named and have passcodes enabled.

Stonar accepts no responsibility for the safeguarding or replacement of personally owned devices which are lost, stolen or damaged. It is recommended that individuals take out their own insurance for all such devices

Pupil commitment to adhere to the ICT acceptable use Policy: I have read this summary document and understand I can read the policy in full via the school website. I agree to adhere to these expectations. I understand that if my behaviour falls short of the school's expectations I can expect to be sanctioned for my poor behaviour choices.

Name: ……………………… Signature: ……………………… Date:……………

Policy details

Whilst Stonar embraces the use of technology for educational purposes the School also recognises its daily use in social environments and the need to protect pupils and safeguard the learning environment.

This policy should be read in conjunction with the School Safeguarding Policy; staff should also read this in conjunction with the Code of Conduct for Staff.

In addition to 'desk top' computers this policy covers, but is not limited to, all devices listed below:

Mobile telephones
Digital cameras
'Tablets'
Digital recording devices
Mobile games consoles
Laptops

The facilities offered by the Local Area Network (LAN) at Stonar are available for use by all staff and pupils. This policy applies to the use of all school owned computers / devices as well as privately owned devices used to communicate with, to or about Stonar or members of the school community. This policy is an extension of the school rules and employment laws and any breach will be dealt with through the usual channels.

This policy also applies to the use of such devices inside and outside school where such use relates to the school, its pupils or staff, connecting via the LAN, other Wi-Fi networks, mobile data or other means.

1: User responsibility

The use of any such devices shall be in line with this policy which all members of the School Community (or for younger pupils their parents) are required to read and sign to say they (or their child) will abide by before being granted access to the school network. Pupils may have one mobile device attached to the school network. Staff may have additional devices enabled with permission of a member of the Leadership Team.

2: Use of devices

Unless directed to by a member of staff, mobile devices must not be used by pupils (excluding 6th formers) during the school day (8am – 6pm) or on sports fixtures. Staff mobile devices should at all times be set to silent / vibrate.; exceptions to this are made for members of the equestrian and maintenance departments who use mobile phones as part of their role in school; furthermore, riders (pupils and staff) are advised to carry a mobile device when they are out hacking or working with horses on fields at some distance from the Equestrian Centre.

Boarders (excluding 6th formers) are required to hand in their mobile phones (and other portable devices as requested) to the duty member of staff before bedtime; they can be collected before school at morning rollcall.

In line with EYFS regulations **personal mobile devices are not allowed in the EYFS setting.**

Prep School pupils are not permitted to have a mobile device in school without the express permission of the Head of Prep School. Senior School pupils who choose to bring a mobile device with them to school should secure it in their locker when it is not being used for educational purposes.

Electronic devices should not be used in any situation that may cause disruption to the school day, embarrassment or discomfort to fellow members of the School Community, including pupils, staff and visitors to the school campus. For this reason devices may not be used to play music / media audibly during the school day, without the express permission of a member of staff. **Mobile devices must not be used in: changing rooms or toilets, when moving about the school campus, at the front of school or in the dining hall regardless of the time of day.** Use of all mobile devices should be in line with the school's code of conduct and behaviour expectations.

Users will also be held accountable for their actions when using any aspect of the School ICT system, whether at school or from an external site, or when using the school as a context for the communication of electronic information (e.g. publishing a website from home which may involve reference to the school, its staff or pupils). This includes keeping passwords secure to prevent unauthorised access to the school network 'Home' directory and/or e-mail.

3: Behaviour expectations

What individuals do or say online is covered by a number of laws, and increasingly people are being prosecuted for offensive and illegal comments made by electronic communications, and on social media sites such as Twitter, Instagram, Facebook etc. Please think before you post online or send!

It is at all times forbidden and potentially illegal to use any online or electronic method to send or publish offensive or untrue messages or post unpleasant comments/imagery that could intimidate, harm, or humiliate other Stonar users or their families. This includes 'trolling'. Individuals must not publish or share any information that defames, undermines, misrepresents, or tarnishes the reputation of the school or its users.

To this effect it is **strictly against school policy to use a mobile device to video, photograph, upload, distribute, store or create material containing another member of the School Community without their express permission or that of a member of staff.**

Individuals should at no time use mobile devices to bully, harass, denigrate, post or distribute private information about a third party whether that be through the use of email, messaging, telephone calls, 'apps', bluetooth, photographs or video images or social networking / blogging websites or any form of electronic or printed communication. If caught, individuals will face disciplinary action.

It is forbidden to use the school network to access, create or send material, which is

- violent or which glorifies violence
- criminal, terrorist or which glorifies criminal activity (including drug abuse)
- racist or designed to incite racial hatred
- of extreme political opinion, blasphemous or mocking of religious beliefs / values
- racist or homophobic
- could be construed as bullying or harassment
- vulgar, pornographic or with otherwise unsuitable sexual content
- crude, profane or with otherwise unsuitable language

- offensive in the normal context of a school
- in breach of the law including copyright law, data protection and computer misuse

Any individual who is caught using vulgar, derogatory, racist, homophobic, profane or obscene language or imagery 'online' or where it has been deemed that this policy has been breached and that the material in question is causing harm or distress to another member of the school community will result in disciplinary action in accordance with school policies / disciplinary procedures.

Any individual caught using a mobile device to cheat in examinations or other formal testing opportunities will face disciplinary actions in line with those as laid down by the relevant examining body and in line with the school rules.
Further to the above users of the school LAN, or school / personal ICT equipment or mobile devices must:

- not use other peoples' user identities (user names) or passwords, even with their permission or allow others to use their user name or password (on any system)
- ensure any software installed on privately owned computers is properly licensed. (The school does not have any licensing agreement to cover such software)
- not attempt to gain administrative access to the School's network.
- not enter into activities such as packet sniffing and port scanning. Reported occurrences will be treated as vandalism.
- not physically misuse or mistreat any piece of ICT equipment nor attempt to disrupt use by others or tamper with the system
- report any suspicions regarding a virus to the IT staff immediately.
- ensure devices are virus free, with antivirus software installed as appropriate. The owner of the device must ensure that updates / operating patches are applied to their device as they are released, any 'infection' passed into the network will be treated as a malicious act of vandalism if found to be the fault of the user.

Electronic contact & discussions between members of the Stonar community must be respectful at all times and communications between staff and pupils must only be part of approved school activities, and only via approved forms of communication (e.g. School email, SMHW, Microsoft Teams, Kerboodle),

4: Protecting identities online

Identity theft is an online danger that is increasing. Pupils and staff are recommended not to upload or reveal personal details of themselves, their family or other Stonar users online (e.g. address, phone number, date of birth, financial details, passwords, etc.) Images and/or comments that could embarrass school users and families should not be uploaded. School members would be aware that uploading digital photographs taken from a mobile device may reveal their precise GPS location at a given date and time, and therefore may reveal movements and locations to third parties. It is recommended to avoid using photographs to identify yourself online, and use an avatar or cartoon image as a profile picture instead.

Unauthorised access to IT systems, accessing others' social networking accounts, e-mail accounts etc., without their permission is an offence under the Computer Misuse Act

5: Reporting concerns

Pupils should report any suspicious or inappropriate sexual advances, messages or similar online behaviour to their parent, houseparent or teacher; they may also report serious or urgent suspicions to the police by using the CEOP button available on many online chat & social networking sites, or seek help via the CEOP website.

Staff should report any concerns to a member of the Leadership Team and safeguarding concerns to the Designated Safeguarding Lead for Child Protection or in their absence a member of the Stonar Safeguarding Team.

6: Logons

By logging onto the School network and any other School IT systems, staff and pupils agree to the guidelines and policies for ICT use at Stonar. They are responsible for any activity that takes place using the School logon or any other password protected system. Passwords for the School network and any other online facility must be kept secret and must be changed regularly. IT support must be informed if any member of the School Community believes someone has obtained their passwords. Passwords should be difficult to guess, and should not be seen by others. It is good practice to have different passwords for different systems rather than the same password for all. Do not log on to a computing device or any ICT system using another person's password, or use such devices or systems that have been left logged on prior to your use. At the end of a session, all members of the school community should exit and close any IT systems and always log off computers and any password protected sites.

7: Consequences of Unacceptable Use

Stonar will act strongly against anyone whose use of ICT could bring the School into disrepute or risks the work of other users; this remains valid even if the incident occurs outside School. The consequences of misuse, abuse, illegal use or the breaking of any of the rules, as set out in this policy will be dealt with by the Head, Head of Prep or the Deputy Head and could include referral to outside agencies such as the Police as appropriate.

If the device is suspected of being used to bully, harass or transmit offensive material it may be searched by a member of staff, in accordance with the school's search policy; and this may result in the deletion of the offending material.

Pupils who infringe any of the expectations set out within this policy could face having the devices in question confiscated and permissions to access the School network revoked. Any pupil device that is used inappropriately in school is liable to be confiscated. Staff must record any confiscations via Daybook. Confiscated devices should be labelled with pupils name and passed to the Receptionist; in most circumstances, pupils can collect confiscated devices from reception at the end of the day.

Repeated infringements or refusal, by a pupil to hand over the mobile device when asked to by a member of staff will be seen as a serious infringement of the School's policies. Such infringements will be recorded via daybook and sanctions will be issued following consultation with the Deputy Head. Such sanctions may include the loss of network privileges or an extended period of confiscation.

Should the infringement pertain to a Child Protection matter, the device will be handed directly to the DSL who will log receipt of the device and act in accordance with the relevant school policy and advice from external agencies.

8: Theft or damage

All devices should make use of security features to ensure that they cannot be accessed by a third party should they become lost; thereby eliminating the ability of a third party to distribute unsolicited information by pretending to be the owner of the device.

Pupils and staff are solely responsible for the safekeeping of their devices and should ensure that they are kept securely and clearly marked with the owner's name so they can be returned to their owner if found.

Items that are found and are not clearly marked or identifiable will be handed to the Deputy Head. Pupils' and staff will be made aware that such devices are held in lost property. Unclaimed / unnamed devices will be held in lost property for up to and no longer than one term, after which time they will be disposed of.

9: Email

School email addresses are supplied to staff (for all work related communication) and pupils. The School currently allows use of third party email access such as Hotmail, G.mail and ISP supplied webmail facilities for all private emails from staff. The School cannot accept responsibility in any way for the content of email transmitted or received by this method.

10: Monitoring & Filtering

The welfare of pupils is of paramount importance; Stonar uses various technologies to monitor both internal and external Internet and e-mail traffic whilst respecting privacy at all times. The School reserves the right to inspect data files and network logs if automatic detection of illicit content is triggered.

Manual investigation of email transmissions will only be carried out with the permission of the Head, Deputy Head or Head of Prep. Emails are automatically forwarded to IT Support when detecting viruses, forbidden words, forbidden attachment file types.

Although Stonar School cannot control the content of the Internet, the School uses third party software to block sites, which are illegal. Inevitably all such sites cannot be blocked, but the vast majority are and the filters are constantly updated and amended to prevent unacceptable media entering the school system. Parents are encouraged to contact the IT staff if they have any concerns over the use of email or the internet by their child.

11: Liability

Stonar accepts no responsibility for the repair or replacement of mobile devices that are lost, stolen or damaged whilst on school property or during extra-curricular activities, trips or when travelling to and from School on School transport. It is recommended that staff/parents/guardians take out their own insurance for all such devices.

The School makes no guarantee, whether expressed or implied, for the information carried over the network or internet service it provides. Although the systems offer a very high level of protection, the School cannot be held responsible or accept liability for any damage or loss of data, or the consequences of such damage or loss, whilst any member of the School is on the school system. The School accepts no liability for any damage caused by any type of computer virus, however it originates. The School accepts no liability in the unlikely event that damage is sustained to a privately owned computer as a result of its being connected to the network.

Any questions regarding this policy should be directed to the Head.
This policy should be read in conjunction with the school Safeguarding Policy

Previous versions: May 2017, May 2018, May 2019
Reviewed by the Advisory Body and approved by the Directors: June 2020

Signed: D.P. Jones *(Director)* *(Head)*

Due for review by the Directors : May 2021