GENEVA ENGLISH
SCHOOL

ACCEPTABLE USE OF ICT POLICY FOR STAFF AND GOVERNORS

SCOPE

This policy applies to all staff members of Geneva English School including teaching and non-teaching staff, governors, regular volunteers and visiting teachers (but access to systems is not intended in any way to imply an employment relationship).

This policy sits alongside related policies that apply to staff, pupils, governors, parents and visitors, including where applicable the School's:

- Safeguarding and Child Protection Policy;
- e-Safety Policy;
- Staff Code of Conduct;
- Taking, Storing and Using Images of Children Policy;
- Privacy Notices;
- Data Protection Policy;
- Data Breach Reporting Policy;
- Data Retention Policy;
- Whistleblowing Code.

If there is anything in this policy that you do not understand or about which you are unsure, you should contact the Head of Computing without delay.

ONLINE BEHAVIOUR

In general our behaviour online should be consistent with our behaviour towards each other face to face. In line with our core values, we expect all members of the school community to show respect and thoughtfulness towards each other, both in their day-to-day interactions and conversations and also in their online communications.

Indeed we all need to be particularly careful about our online relationships and behaviour because anything that we write in an e-mail or post online has permanence, even if I delete it, and can potentially be traced or retrieved, long after it was written.

- I will ensure that all my online communications, and any content I share online, are respectful of others and composed in a way I would wish to stand by.
- I will not engage in any online activity that might compromise my professional responsibilities or bring the School into disrepute.
- I will not attempt to access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues). I understand that to do so could lead to serious disciplinary action.

- I will not use the Internet to distribute malicious software, to damage, interfere with, or gain unauthorized access to the computer systems of others, or carry out illegal activities.
- I will respect the privacy of others. I will not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without obtaining permission from the data subject.
- I will report any accidental access or filtering breach to Head of Computing, who is the school's e-Safety Officer.
- I will not download any software or resources from the Internet that could compromise the network, or are not adequately licensed. Any software requirements should be discussed with the Head of Computing, who will authorise the software installation or organise the purchasing of software licenses as appropriate.
- I will not attempt to bypass the School's internet filtering system.

USE OF THE SCHOOL'S IT SYSTEMS AND DEVICES

The School's IT systems and any school-owned digital device issued to members of staff are intended for school purposes only. Limited, occasional use of electronic media (sending or receiving) or the Internet for personal purposes is understandable and acceptable. Such use must not adversely affect the systems' or device's use for educational purposes. Members of staff are expected to demonstrate a sense of responsibility and not to abuse this privilege.

School e-mail (gmail), the internal school cloud server, school Google Drive and any school, encrypted USB drive should be used to store school resources only. The school Google Drive should be used for sharing teaching and learning resources with other members of staff. School documents and data should not be stored on personal devices.

- I will access school IT systems using my own username and password only and I will not share my username or password with anyone else.
- When accessing school documents using Google Drive, Google Classroom and Google Docs etc I will use my geschool Google account only.
- I will keep any school-owned device in my care up to date, using the School's recommended firewall and other ICT 'defence' systems. This includes updating the software on the device. The School's Mobile Device Management system (Jamf) will perform this annually.
- If I have a school-owned Macbook, I will enable the 'File Vault' encryption tool, following the instructions given to me by the Head of Computing.
- I will not save personal files (personal files, photographs, music files etc) on the school network or on any school-owned device.
- I will not open a hyperlink in any email or attachment to an email if I have any concerns about it or think it may contain a virus or other harmful program. If in any doubt, I will check with the Head of Computing.
- I will embed the School's e-Safety principles, as outlined in the Acceptable Use Policies and e-Safety Policy, into my teaching.
- When leading a school trip, I will discuss with the School Office, at least two weeks prior to the trip, the use of a school mobile phone.
- On leaving Geneva English School, I will return any school-owned device to the Head of Computing, who keeps a register and inventory.

PASSWORDS AND SECURITY

Passwords protect the School's network and IT systems. They are the responsibility of the user and in no circumstances should they be disclosed to anyone else. Passwords must be changed at the beginning of every school year and it is the responsibility of staff members to do this, even if not prompted to do so automatically. Passwords must not be obvious (for example "password", 123456, a family name or birthdays) and they should not be the same as any widely used personal passwords.

- I will not allow any unauthorized individuals to access the School's email or IT systems.
- I will not let anyone else know my passwords, or keep a list of passwords where they may be accessed, and I will change passwords immediately if they appear to be compromised. I will not attempt to gain unauthorised access to anyone else's computer or to confidential information to which I do not have access rights.
- I will always log out from a school computer before leaving it unattended, even for a short while.

DATA PROTECTION

Members of staff must respect the privacy and confidentiality of others, following any policies and guidance provided by the School on data protection.

- I will check carefully before sending that I am not misdirecting an e-mail. When sending an e-mail to a group of parents, I will be careful not to disclose personal contact details or other personal information. In a group e-mail to parents, I understand that the addresses should be written in the 'bcc' not 'cc' field.
- I will ensure that any confidential data that I wish to transport from one location to another is protected by encryption and I will follow school data security protocols when using any such data at any location.
- I will report any accidental data breaches of this nature to the School's Data Protection Officer without delay.

USE OF PERSONAL DEVICES AND WORKING REMOTELY

For further detail, see the Remote Working and Use of Personal Devices Policy

All official school business must be conducted on school systems, and personal email accounts should not be used for school business. Where permission is given for use of personal devices, they must be password protected. They must not be left unlocked when unattended and must have up to date antivirus software and security updates installed. The Head of Computing will help staff connect their device to the School's wireless network and access school systems such as the school database, storage platforms and e-mail but cannot provide support for the device.

Wearable technology that connects directly to the Internet without touching the school networks must not be used to access school data, including e-mail.

- If I wish to use a personal device for school purposes (e.g. for school e-mail) I will consult first with the Head of Computing.
- I agree that if I use a personal device in school, it will be for legitimate reasons and will not interfere with my productivity or my school duties.
- I will read and observe the School's separate policy on Remote Working and the Use of Personal Devices, which is published on the Staff Message Centre.

PHOTOGRAPHY

The use of a personal mobile phone to take pictures of pupils (or that contain images of pupils incidentally) either in or out of school is prohibited. This is to protect members of staff from allegations of inappropriate behaviour.

If a personal phone is used inadvertently in this way, any images must be uploaded to the GES Cloud at the earliest opportunity and deleted from the personal device with no copies having been kept or transmitted elsewhere. The School may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy.

- When taking images of pupils (or that contain images of pupils) in school or on school trips I will always use school-owned cameras or iPads and comply with the School's policy on Taking, Storing and Using Images of Children, which is published on the School's website.

MONITORING

Staff should be aware that school email and use of the Internet (including through the School WiFi) will be monitored regularly by the Head of Computing for safeguarding, conduct and performance purposes. Both web history and school email accounts may be accessed by the School where necessary for a lawful purpose, including the investigation of serious misconduct, welfare concerns, concerns about extremism and for the protection of others.

- I understand that connecting my own personal digital device to the school WiFi network will result in the School's monitoring:
  - The name of my device;
  - The date and time the device was last used on the network;
  - The IP address of my device.
- I understand that in the event of a Data Subject Request, everything that I commit to a digital system, including e-mails, may be disclosable to the person about whom I am creating a record. See also the School's Data Protection Policy.

E-MAIL AND SOCIAL NETWORKING

Staff should not use their personal e-mail or social media accounts to contact pupils or parents regarding school business. School documents or school e-mails must never be sent from a personal e-mail account.

Staff should not assume that electronic communications or electronic files are completely private. Accordingly, if there is personal or sensitive information to transmit, other means of communication should be considered.

Staff should remember that any messages or information sent on school-owned devices via an electronic network, for example internet mailing lists, social media, and specifically the GES Facebook and Community Facebook pages, are statements identifiable and attributable to the School.

When using social media (e.g. on a school trip), members of staff should not name children, or disclose their location if off-site.

Social networking sites, such as Facebook, YouTube, Instagram and Twitter, are part of the world in which we now live, but their use is not without danger. Members of staff must be aware of these in order to avoid possible significant professional problems.

Staff must not 'add' current pupils on social media channels, as this can be misinterpreted and can lead to allegations of misconduct. We strongly advise that this should continue when you leave Geneva English School and are no longer a member of staff. Staff may only accept social media 'friend requests' from former pupils who are over 18 years old.

Members of staff should be aware that their school e-mail accounts will be closed (and the contents deleted) within one month of leaving the School. Important information that the

School needs to keep should be held on the relevant personnel file and not kept in personal folders, archives or inboxes. It is the responsibility of each account user to ensure that important information is retained in the right place or, where applicable, provided to the right colleague. No important information should therefore be lost as a result of the School's e-mail deletion protocol. If in doubt, members of staff should speak to the Head of HR and/or the Head of Computing.

For further information and guidance, see:

- The School's Use of Social Media Policy;
- Guidance on the Use of E-mail Communication at GES;

both of which are published on the School's website.

IT SUPPORT AND MAINTENANCE

All ICT equipment is covered under the manufacturer's limited warranty. Insurance is in place to cover accidental loss or damage. If equipment is lost, damaged, or stolen, the member of staff responsible for that equipment must immediately report this to the Head of Computing and describe the circumstances surrounding the loss, damage, or theft of the device.

- In the event of hardware or software failure, I understand I should bring my school-owned device to the Head of Computing, who will assess the issue and if necessary use the services of our external consultants (ART Computer).
- I agree that I am liable for the cost of damages caused by:
    - unreasonable use, abuse, neglect, and alterations;
    - improper service, improper installation, and improper connections with other peripheral devices (for example linking to printers, servers etc. which are not school approved equipment);
    - loss or misplacement that is not accidental.

BREACHES OF THIS POLICY AND CONCERNS ABOUT ONLINE BEHAVIOUR

If members of staff become aware of a breach of this policy or the e-Safety Policy, or if they are concerned that a member of the school community is being harassed or harmed online, they should report it to the Head of Computing, who is the School's e-Safety Officer. If it is a matter of safeguarding or child protection, the Designated Safeguarding Lead must be informed without delay.

The School reserves the right, at its discretion, to review any employee's school-owned electronic device to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other school policies, to assist in the investigation of wrongful acts, or to comply with any legal obligations of the School in its role as employer or generally.

I have read and understood this Acceptable Use of ICT Policy for Staff and Governors and undertake to comply with it. I understand that a deliberate breach of this policy will be dealt with as a disciplinary matter using the School's usual procedures.

Name: ____

Date: ___________________

Signed: ____

Please return a signed copy of this policy to the Head of HR

Author: Ronan McStravick, Head of Computing & Digital Strategy and e-Safety Officer
Created: August 2018
Review date: July 2019