SOLIHULL

ICT Acceptable Use Policy

Owner: DSL/Pastoral Support Manager
Reviewer: Assistant Head: Digital Learning and ICT Strategy
Last Reviewed: September 2023

Version 4

As a member of the Solihull School community, you should be familiar with these rules, and agree to be bound by them. All the rules apply whether a user is logged on to the network in a Computer room, on a school or personal laptop or any other device whilst on the school premises.

1. Responsible use of Solihull School's ICT equipment and systems

- Pupils should not reset machines unless told to do so by a member of staff.
- **No games** are to be installed on any machine, except with the express permission of the Assistant Head: ICT Strategy or a Senior Leader.
- **No eating or drinking** is allowed in any area containing computers.
- Any problems with the hardware or software should be reported to your class teacher or a member of the Technical Support Team
- You must not create, display, copy or otherwise distribute offensive material. Offensive material could involve, but is not limited to, racism, pornography, bullying, radicalisation propaganda, and criminal skills including hacking. In cases of any doubt, please ask any member of staff. Please refer to the section on Bullying below for further information.
- Do not store executable files (.exe files) or other copyrighted material such as MP3 files, wallpapers, movie clips and other picture formats or movie clips in your user area.
- Pupils must not use social networking sites in school, whether using a school owned device or personal device such as a mobile phone, tablet or laptop.
- You CAN access your Solihull School email from home by going to **www.solsch.org.uk** then clicking the link and entering your email address in the space provided; the password field is your normal logon password. Alternatively, you can access your email at www.office.com and entering your email address ('@solsch.org.uk' after your username) and password once redirected.
- The content of each student's user area is exclusive to the owner as far as other students are concerned. Members of staff have the right to add files, and the ICT staff regularly check the user areas for copyrighted, offensive or otherwise unsuitable materials.
- You should treat ALL ICT resources responsibly and avoid waste by not sending documents to print unless this is necessary the work is in final draft form. All printing is monitored, and students have a monthly quota, where colour printing is more 'expensive' than black & white printing. Additional credits can be requested where there is a specific need, and the number of credits renews each month. Any unused credits do not rollover.

2. Responsible use of Student devices (Pupil laptops/ Bring Your Own Device) in school

- The use of laptops and other mobile devices* in lessons is a privilege. Students are given access to their devices within lessons at the discretion of the classroom teacher and with the sole aim of assisting learning.
- Any use of mobile devices within lessons which is not in line with assisting

learning or has not been directed by the member of staff is an abuse of this privilege and may lead to use of devices in lessons being denied. This includes playing games, accessing social media or other means of communication between students not related to learning activities being overseen by members of staff. Use of the chat function in Microsoft Teams should always be appropriate and to aid learning. Please be aware that this chat function on Teams is searchable by staff if necessary. Any miss use of this function can lead to pupils being restricted from using chat alongside other sanctions which may be imposed as appropriate.

- Access to the internet must be via the school's WiFi system and not by using hotspots, i.e. tethering devices to mobile phones. This is because UK educational establishments are required to put in place safeguards on access to the internet; a smooth wall restricting access to approved web addresses and domains. Please let your teacher know / contact **vanalderwegenm@solsch.org.uk** if you are having difficulty in accessing school WiFi making clear the precise location.
- Pupils should not customise the appearance of their profile on educational platforms used within school such as Microsoft Teams. They should not introduce a new photo or image regardless of content. Teams profiles should either have no image (revealing pupil's initials only) or the formal photo of pupils uploaded by the school.

***** Please see separate protocols on the use of **Mobile devices and photography** within school

3. Unauthorised Access

It is a **serious offence** to use the username and password of another user. Users should not reveal their password to any other user, not even an administrator or member of staff.

Users should be aware that all online activity leaves behind a trace, or 'digital footprint' that may identify the person posting, whether or not that post is then deleted. Details such as username, computer name and physical address of the device may all be recorded when posting any content to the Internet.

Users whose accounts have been disabled by an administrator must see an administrator to have it enabled at times when it is needed for lessons. Impersonation of another user via e-mail is a serious offence.

It is a serious offence to attempt to bypass the filters put in place by the school which restrict access to unsuitable material on the internet, for example, using technologies such as online proxies or VPN.

All of your files should only be saved in your **own** user area in school, OneDrive or Google Drive that have been allocated to you.

Users should report all incidents of attempted phishing / phishing to the ICT Help Desk as soon as possible **help@solsch.org.uk**. Users shouldn't forward the phishing email to this address.

3. Plagiarism

Pupils should not share or distribute their work to other users unless directed to do so by a member of staff. To pass the work of another off as that of your own is a serious offence, particularly when related to coursework for examinations and may result in disqualification from all exams in that series. It may also represent a breach of copyright (see 6, below). Plagiarism also includes the unauthorised or uncredited use of Artificial Intelligence or AI platforms such as ChatGPT. This is also a breach of this policy, **unless your teacher gives you express permission to use a Generative AI platform** as part of a specific homework or task. Any form of bullying including the use of laptops/devices to do so is not tolerated at Solihull.

4. Unauthorised Modification

It is a serious offence to destroy work (files) of another user, create or introduce a virus or other malicious code to cause a system malfunction. Users must not attempt to reconfigure the computer, place shortcuts, aliases, software or clip art on to any local hard disk. Program files must not be downloaded from the Internet. **Application software** must not be brought into school. However, it is permitted to access work on any compatible medium (eg USB pen drives, memory sticks, OneDrive, Google Drive or any other cloud-based storage).

5. Bullying (inc. Cyber/Online Bullying)

The school does not tolerate bullying in any form, whether that be verbal, physical, online or via technology (i.e. cyberbullying / online bullying) . Such bullying may include racist, sexist or homophobic language, for example, or sexual harassment. If you are the victim of such behaviours, please report it to a member of staff. Anyone found to be taking part in such behaviour can expect to be managed in line with the Behaviour and Discipline Policy and Anti-Bullying Policy, Safeguarding and Child Protection Policy.

6. Copyright

Many of the programs and files which you access on the local hard disk, over the network and over the Internet, are subject to copyright. In case of any doubt, you should seek permission from the owner of the material before using it. This includes images, audio and video.

7. Criminal Justice Act

It is illegal to store and/or transmit pornographic or offensive material, using technologies including but not restricted to, email, internet enabled device, digital camera, digital media etc. If in any doubt, please seek advice from a senior member of staff.

8. Counter Terrorism and Security Act 2015

It is imperative that we are all watchful and aware of the potential for ICT to be used to radicalise and draw people into terrorism. If in any doubt, please seek advice from a Designated Safeguarding Leading and/or a member of the School Leadership Team in line with the Safeguarding and Child Protection Policy.

9. Legal Responsibility

Solihull School accepts no responsibility for the malfunctioning of any ICT equipment, and any subsequent losses. However, every care is taken to ensure the highest quality of service. Please ensure that you have back-up copies of any valuable files before accessing them from within school. The School makes back-ups of user areas every evening. Users should be aware, (as mentioned under Section 1 point 9), that staff have access to their user areas. Electronic mail is monitored manually on an ad hoc basis for suitability, and you are advised that by signing the Acceptable Use Policy form, you agree to this action. This notification is required by the Data Protection Act and Regulation of Investigatory Powers Act. All incoming and outgoing e-mail is scanned for viruses automatically.

10. Disciplinary Action and Sanctions

Users who breach these conditions will be warned of the unacceptable nature of their actions. The specific offence will be made known to the user, and a record will be kept electronically. Breaches may be dealt with by the Senior Leadership in line with the Behaviour and Discipline Policy or Staff Behaviour Policy.

11. ICT Specific Sanctions

The measures taken will depend upon the seriousness of the offence. Normally, a verbal warning will be issued for a minor misdemeanour, but further sanctions may be taken against those who repeatedly offend, or where the nature of the offence is more serious. These sanctions include restricting access to the school network for a time, or permanently. In serious cases, the matter will be referred to a member of the School Leadership Team and/or the Executive Headmaster. If a pupil, parents will be notified of instances of accessing unsuitable material and in the most serious cases; it may be that exclusion (see Behaviour and Discipline Policy) and/or police involvement is required.

12. Education, Training and Help

Technology is constantly changing, and with it are new risks and abuses of technology such as cybercrime in its many forms. As a new member of the school, you should receive some basic training on using our systems, and familiarisation

with the Acceptable Use Policy (AUP). This details the School's expectations when using technology. Further training for pupils takes place within the Preparatory School and Lower School years in Computing lessons, and via year wide WPD training, which address different and escalating risks at an age appropriate time. For staff, there is an annual Data Safety briefing by the Assistant Head: ICT Strategy and training on a departmental or individual basis is available on request. The school has a number of CEOP trained staff, including Mrs Sarah Hardy (DSL/Pastoral Support Manager), Mrs V Patel (Head of Computing and ICT) Mrs LEM Rooney (Head of Wellbeing and Personal Development) and Mrs A Longden (Prep School ICT Subject Leader). However, all colleagues can be approached for advice, and if the answer is not known, it can be referred to the relevant member of staff.