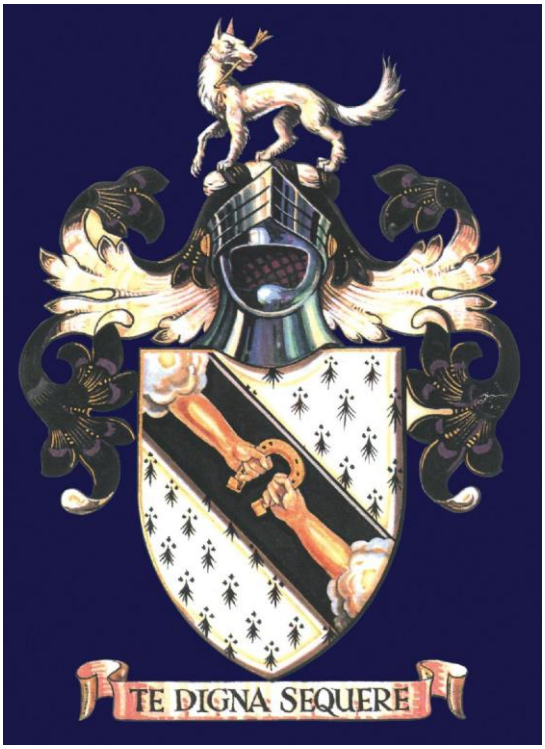
SWBGS Staff - ICT Acceptable Usage policy



The SWBGS Acceptable Usage policy is governed by the laws of the land (see Appendices) and covers all electronic devices, communications a **It applies to all resources**[See Note1] **used within school premises and to all resources provided for SWBGS Staff, students and parents in and out of school.**

*Note1: Resources includes but is not limited to:

Audio-visual equipment, Blogs, Cameras, webcams and Digicams, Computers, Computing software, E-mail, Fax, Instant Messaging/Collaborative applications, Internet and Intranet, Mobile devices i.e. laptops, mobile phones, blackberries, PDA's, etc… , Network, Printers, Remote access service, Scanners, Telephone or videophone, Text, Voicemail, Wikis

In accordance with relevant legislation you are advised that SWBGS has the capability to lawfully monitor and record your activity from any workstation or for any device using the school's facilities. This document informs the Current regulations for the acceptable use of SWBGS's IT systems and displayed on the school website. You will be liable for any action deemed necessary by SWBGS as a result of contravening these regulations.

Please Note: Contents of this policy may be changed at any time to update for legislation or to protect the school

Guidelines for all Users

The school network and Wifi systems are valuable resources that are available to all pupils and staff from their own devices and from most computers situated throughout the school. Due to the wide variety of uses by hundreds of users, a number of precautions have to be taken for your safety, the safety of others and to help ensure that all systems are kept available and in full working order:

Users are responsible for appropriate behaviour on the network and Internet, just as they are in a classroom or a school corridor. General school rules apply.

Access to the school network will be provided for you to carry out recognised school work (and social use within the limits which have been discussed in PSHCE and Assemblies AND provided such use is not conducted during lessons), on the understanding that you agree to follow these guidelines. These guidelines apply to all staff and pupils.

You should be aware of the following:

1. Computer (file) storage areas are school property.
2. All network activity is monitored and recorded.
3. All emails (even when deleted) and their history are logged and archived.
1. ICT staff use network monitoring and alerting systems to provide remote support and to ensure the school systems are being used in accordance with the school's rules
2. Members of the ICT staff may look at any files and communications to insure that the system is being used responsibly
3. ICT staff can view any school computer screen at any time from anywhere on the school network without you knowing about it.

The following are not permitted:

- Use of another person's username and password.
- Trespass in others' folders, work or files.
- Hacking or hacking with intent to cause damage.
- Downloading viruses, trojans or circulating "infected files".
- In any way enable yourself or others to gain unauthorised access to computer material (this includes instructions for gaining such access, computer codes or other devices which facilitate unauthorised access);
- Allowing another person to use your username and password.
- Sending, displaying, accessing or trying to access any obscene, offensive or hate crime material.
- Using obscene or offensive language.
- Harassing, insulting or attacking others through electronic media including on grounds of age, gender, race, disability.
- Unauthorised copying of software or violating copyright laws.
- Revealing any personal information, the home address or personal phone numbers of yourself or other people to anyone on the internet, unless specifically authorised by parent, carer or teacher.
- Downloading games or other executable programs.
- Intentionally wasting limited resources or time on unnecessary or unauthorised activities.
- Moving or changing any computer or associated equipment unless specifically requested and authorised by a member of ICT staff. Damage caused by unauthorised persons may be considered a criminal offence.
- Eating, drinking, using aerosols etc near any electronic equipment.
- Use of commercial activities by for-profit institutions.
- Carrying on a private business.
- Undertaking financial transactions on behalf of the school unless authorised.

Additional Information

- The School's wired, wireless networks, Internet access and school email are provided for users to conduct genuine research and communicate with others. All your activity and the sites you visit are recorded. Remember that access requires responsibility at all times.

  - All users are required to log on using only their own personal username, which will remain with them throughout their time at the school. Use of another person's username and password is considered a criminal offence under the Computer Misuse Act 1990 and/or depending on offence any other Act listed in the appendices.

  - Unauthorised Trespass in others' folders, work or files. All unauthorised access is considered a criminal offence under the Computer Misuse Act 1990 and/or depending on offence any other Act listed in the appendices.

  - Users passwords must not be made available to anyone else. If you think someone has learned your password then change it immediately. Change your password at regular intervals; at least once a term and using a minimum of twelve (12) characters, including numbers and letters. Do not write your password on anything you leave unattended.

  - Remember a school is a public place. Always make sure that you have completely logged off or locked the computer before leaving it unattended. Failure to do so will be considered a contravention of school policy and if an offence has been committed by some other person, may be considered as facilitating the Misuse of Computer, which is also a criminal offence

  - Under the Data Protection Regulations 2018, Personal Data must not be inappropriately shared or communicated to anyone else. Please ensure when processing personal data your screen cannot be seen by someone else and that you follow the guidelines in the school's Data Protection Policy

  - Damage to data, computers, computer systems or computer networks, including unauthorised damage or interference to any files or program is not permitted and may be considered a criminal offence under the Computer Misuse Act 1990.

  - Programs must not be installed on a computer except by a member of the ICT administration department.

  - The installing, copying or transmitting of obscene material is not permitted and may be considered a criminal offence under the Obscene Publications Act 1959/1964.

  - If a "virus alert" occurs when transferring work files from a memory stick, please inform a member of the ICT staff immediately.

  - Computer equipment may not be taken off-site without formal authorisation.

  - During the day when not in use, computer screens should be switched off to save electricity however the computers should be left logged off but powered up. Computers will be shutdown by the ICT systems at the end of the day after maintenance.

Sanctions

Remember that the use of the School's IT facilities in a way which contravenes the School's regulations may be treated as a disciplinary offence and lead to the penalties established by those regulations.

1. Violations of the above rules may incur disciplinary action in line with existing school practice on inappropriate behaviour

2. When applicable, police or local authorities may be involved.

File Security

- The school uses Google Apps for Education for email, storage and other applications. Google drive provides unlimited drive space in the cloud for each school user while they are a member of the school. All staff and students are directed to save their work on their Google drives as their main storage area.

- Additionally all users have their own area for storing their work on the school's network servers (usually designated the "H" drive). This means that they can access their work from any school network station.

- To reduce the chances of the server hard disk filling up and crashing the whole network, the amount of disk space for each user is limited to normally 1GB. Overflowing this limit will cause the user to be locked out until sufficient files have been deleted or uploaded to their Google drive.

- Users are not permitted to use memory sticks; users must go to the ICT administrators' office to request the archiving of files to memory sticks, if required.

- Users are not permitted access to station and network drives other than those provided at login; nor are they permitted to alter or save files outside their own area (except in the authorized shared areas).

- Network stations may not be booted up from USB or CD. Unauthorised users (anyone excluding ICT administration staff) attempting to do so will be in breach of the Computer Misuse Act

- An automatic regular search will be made for any executable program and zip files stored in user areas. These will be noted, automatically logged against the user and the user notified. If the user cannot provide a satisfactory reason for them, the authorities will be notified and appropriate action will be taken.

Access to Software

- At logon all users receive desktop icons and start-menu-shortcuts to all the main application programs and common utilities, on the wired network, set up for each of the curriculum subjects. This provides shortcuts/icons to programs that are relevant to the study of that subject as well as any shared documents provided by the subject teachers.

- Users can only access software and other resources as made available to them through these subject shortcuts. For example, pupils do not have access to the Staff areas but all staff do not have access to Admin areas . Use of the main software packages is continually audited for each user.

- Sites visited on the Internet are also audited, and filtered by our Internet Service provider and our own filtering appliances. Attempts to access sites blocked by the ISP or school are in breach of the school policy. Where a site is blocked and is required for school work, the ICT staff may be requested to ask for the site to be unblocked by a member of staff.

Access to Printers

- To encourage good management and reduce wastage of ink and paper, the number of print credits for each user is currently £20.00.

- Attempts to print beyond this credit limit are automatically denied by the system. Staff may request more credits which will be charged to their department. Currently 5 credits are used for a black print A4 page and 20 credits are used per page for expensive printers and for colour printing.

Your Input

We welcome your input in respect of suggesting material which should be filtered or unfiltered, although Sir William Borlase's Grammar School maintain the right to ultimately determine what is and is not filtered.

Appendices

Computer Misuse Act 1990

The "Computer Misuse Act 1990" covers three offences

- Simple hacking, that is the unauthorised entry to computer facilities via a computer.
- Unauthorised access with criminal intent, that is hacking with the intention of perpetrating a more serious crime and covers facilitating access to others.
- Unauthorised amendment or damage to data and covers among other things the introduction of viruses and time bombs.

Anyone convicted of an offence under this act can expect a fine of unlimited amount plus a prison sentence ranging up to a maximum of 5 years.
Anyone suspecting that an offence has been committed should refer the matter to the Headteacher.

Data Protection 1998 and (Charges and Regulations) 2018

The Data Protection Regulations (2018) concerns the processing of information about living individuals. It gives rights to those individuals about whom information is recorded and demands good practice in handling information about people.

Every person or organisation holding personal data (data controller) must be registered with the Information Commissioner. SWBGS is registered as a data controller. Any use of personal data beyond the descriptions listed in School's registration is illegal.

You must:

- only use personal data for a School related purpose;
- ensure that the use of School related personal data is restricted to the minimum consistent with the achievement of academic purposes;
- contact the School's Business manager or Data Protection Officer before conducting any activity which involves the collection, storage or display of personal data through the School's IT facilities.

Malicious Communications Act 1998

Under Section 1 of this Act it is an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person.

The Telecommunications Act 1984

It is a similar offence to send 'by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character' and is an imprisonable offence with a maximum term of six months and/or a fine up to £5000.

Protection from Harassment Act 1997

Stalking, Offensive or threatening communications can also be charged under the Protection from Harassment Act. This can carry a sentence up to 5 years imprisonment.

Sex Discrimination Act 1975: discrimination on the grounds of sex by dismissing an employee or submitting them to "any other detriment"

Race Relations Act 1976: ditto on racial grounds

Disability Discrimination Act 1995: ditto on grounds of disability

Criminal Justice & Public Order Act 1994: intentional harassment for causing another person harassment, alarm or distress by using threatening, abusive or insulting words or behaviour

Obscene Publications Act 1959 and 1964

It is an offence to publish an obscene article or to have an obscene article in ownership, possession or control with a view to publishing it or, where the data is stored electronically, to transmit that data.

Copyright, Designs & Patents Act 1988

The "Copyright, Designs & Patents Act 1988" provides the same rights to authors of computer programs as literary, dramatic and musical authors have to their works. Those rights extend for the life of the author and for fifty years after the author's death.

Software is generally not sold outright to the purchaser. Instead the purchaser is granted the right to use it as laid down in the user licence. It is normally expected that only one person at a time will have access to and use the software concerned. A network licence may be purchased, normally at a reduced rate, for a defined number of users. A site licence may be available to cover all (unlimited) users within the premises.

It is thus illegal to make copies of software without the copyright owner's consent, or to duplicate software loaded on a hard disk for use on any other personal computer unless allowed for under the licence.

Anyone convicted of an offence under this act can expect a fine of unlimited amount plus a prison sentence ranging up to a maximum of 2 years.