Whitley Academy

ICT ACCEPTABLE USER POLICY

UPDATED: February 2016

Approved by Governors: February 2016

Next time before Governors: Autumn 2019

If you have any **questions about the** policy, please contact the Vice Principal responsible for ICT.

The school assumes the honesty and integrity of its ICT users (students and staff). Facilities are provided in as unrestricted manner as possible to offer the best possible quality of service.

It is the users' responsibility to ensure that they comply with the policy. The latest version can be found on the school's website along with the following related policies.

Online Protection
Internet Safety / Cyber Bullying
E-Safety Advice for Parents

All new students (year 7 and new admissions) will be invited to sign an agreement to abide by the policy.

All staff and students will have to accept an electronic version of the policy when logging on to a school computer. Students' refusal to follow any of this policy when pointed out by a member of staff will be treated as any other refusal to follow an instruction, in line with the schools consequences procedures. These are clearly stated in the BFL network use document.

General Policy

The user agrees not to:
Upload, download, post, email or otherwise transmit or store any content that is unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libellous, invasive of anyone's privacy, hateful or racially, ethnically or otherwise objectionable.

Impersonate any person or entity, or falsely state or misrepresent affiliation with a person or entity, including the forging of headers, or to otherwise manipulate identifiers in order to disguise the origin of any content transmitted through the School services.

Upload, download, post, email or otherwise transmit or store any content that the user does not have the right to transmit.

Upload, download, post, email or otherwise transmit or store any content that infringes any patent, trademark, trade secret, copyright or other proprietary rights ("Rights") of any party.

Upload, download, post, email or otherwise transmit or store any unsolicited or unauthorised advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes" etc. except when directly resulting from curriculum work.

Upload, download, post, email or otherwise transmit or store any material that contains software viruses or any other computer code, files or programs designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware; or telecommunications equipment.

Interfere with or disrupt the service or servers or networks connected to the service, or disobey any requirements, procedures, policies or regulations of networks connected to the service.

Collect or store personal information about others without direct reference to The Data Protection Act.

Use the School's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of a curriculum project.

Visit or use any online messaging service, "chat site", web-based email or discussion forum not supplied or authorised by the School.

Store or use any software not specifically installed on the service by an authorised person.

Visit, use, download, or store any game, either application or browser-based, without permission of the school's network manager and only for educational purposes.

The School reserves the right to refer any breach of this policy to the respective tutor / Learning Support Case Worker / Curriculum Leader and / Senior Leadership Group. This may result in the suspension of any or all parts of the services provided.

Network Services

This comprises of access to workstations (PC or Mac) in the various classrooms, labs or other areas for all users and for staff additional access in departmental offices and for those that work on the school administration network.

Storage of files for all users, including teachers and administrative staff is available on the main file server.

All users shall have complete access to any files they have created, except where ownership / authorship is in question. This is then referred to a member of the Senior Leadership Group.

Each user shall have a unique login ID and password. **The password must not be divulged to any other user or any third parties outside of the school**.

Internet Services

Each User shall have an Internet account to access the Internet via the School's Proxy Server. The Proxy Server will filter any unwarranted materials and be updated regularly to maintain this high level of filtering.

Any user repeatedly attempting to access such material will have their account locked and it will not be reopened until they have discussed the matter with a member of the Senior Leadership Group.

The School does not pre-screen content viewed by users, but relies on the filtering software. Should any site or content be discovered which does not comply to the General Policy it will be added immediately. We ask users to assist us with this by informing us of any offending material

Mail Services

All staff shall have an email account to enable them to send mail internally and externally; to take part in group conferences and to access online resources. It is viewable via the email client or via a web interface.

The size of each user's mailbox (mail storage area) will be decided by group and/or requirements to do work.

Mail sent and received externally shall be filtered for viruses, SPAM, language content and certain file types within attachments. If a user sends an email that is caught by the filters, the email will be quarantined and a request to the ICT manager must be made.

If a user repeatedly sends material that is caught on the filter the matter will be referred to a member of the Senior Leadership Group.

Any user who receives unsolicited email should forward it spam@whitleyacademy.com.

Likewise, if any user is found to be sending unsolicited emails, to other users within the school, or to external accounts, the matter will be referred to a member of the Senior Leadership Group.

Group conferences may be moderated by a variety of users, including Peer Moderation by students.

Security

Each User will be given a unique ID and password that will allow them to access their account. The same password will allow them to access their "Home Area" on one of the school's File Servers and their Internet account. Passwords for members of staff to gain access to the School's Management Information Systems (SIMS) can be changed by request of the SIMS manager.

The ID and password are solely the responsibility of the user and not to be shared with other users or third parties for any reason. If a user is found using the ID and password of another user their services may be suspended and immediately referred to their respective tutor/head of department and then the Deputy Head/Head.

The only programs that may be used within the School are those agreed on by the Network Manager and/or Senior Leadership Group and installed by a member of the Support Team. The introductions of programs (including any software containing viruses or used to disrupt any part of the network, or connected networks) onto the network is not tolerated and will be treated as intentional damage or an attempt to cause damage to School property.

All information about staff and students will be dealt with in compliance the Data Protection Act and only given to authorised agencies. Staff and students agree to abide by the Data Protection Policy.

The school reserves the right to monitor all traffic on the network, either manually or through automated software, to ensure policy compliance and to aid in resolving any issues.

By default all staff and students agree to their image or likeness to be used on the school website or in any promotional material published by the school or associated agencies unless otherwise specifically stated.

Students may not photograph, video or otherwise record other students, members of staff or members of public, whilst on school grounds, for use outside of school without explicit permission.

Treatment of Equipment

IT Services will endeavour to ensure all equipment is in working order. This is done by each classroom with IT equipment being checked and any damage recorded weekly, this is WA's "MOT" system. If persistent damage occurs it will be reported to a member of the Senior Leadership Group

Should any user find that a piece of equipment does not work correctly they are to report it to a member of the support team and not attempt to repair it themselves. Members of staff who wish to receive some training in dealing with immediate repairs may make a request to the Network Manager.

Any user who causes damage intentionally or through neglect, to any equipment may be refused the right to further use of the equipment and may be asked to cover costs towards any repairs or replacements.

Unless otherwise issued to a member of staff as part of their contract (e.g. staff laptops) any equipment taken off site is the personal responsibility of the user and you are advised to check that its loss or damage is covered by your personal insurance. All such loans will require a signature by a parent, teacher and/or Curriculum Leader.

Staff Personal Use

The level of personal use should not be detrimental to the main purpose for which it is provided.

Personal use must not be of a commercial or profit making nature.

Personal use must not be connected with any use or application that conflicts with the staff's obligations to the school.

Staff may use email for domestic and family needs during working hours providing the level of usage does not affect their level of performance.