John Willmott School – Acceptable Use Policy Statement

At John Willmott School students and teachers work together to form a challenging learning environment, mutual respect, responsible attitudes to each other, to work and to property is the foundation of the School's culture.

The Computer system at John Willmott is the property of the School and is a resource shared by all students and staff. Computer facilities, including mobile units, are made available to further student education and to staff to enhance their professional activities, including teaching, research, administration and management.

The School's Acceptable Use Policy has been drawn up to protect all parties – the students, the staff and the School. A copy of the School's Acceptable Use Policy is available on the VLE. It will be kept up to date and the latest version will be available on the VLE.

Key Points:

The School reserves the right to examine or delete any files, including emails, that may be held on its computer system; and to monitor or to restrict access to any Internet sites visited.

Students and Staff using the School's computer system should sign a copy of the Acceptable Use Statement and return it to their tutor or to the IT Operations Manager as appropriate.

- All Internet activity should be appropriate to staff professional activity or student education
- Access to the School servers and the Internet should only be made via the user's authorised account and password, which should not be made available to any other person
- Activity that threatens the integrity of the School IT systems, or activity that attacks or corrupts other systems is forbidden
- Users are responsible for all e-mails sent and for contacts made that may result in e- mails being received
- Copyright of materials must be respected
- Use for personal financial gain, gambling or political purposes is forbidden
- Use of the network to access inappropriate material is forbidden
- Video, audio or photographic recording of staff or students whilst on School property, to be used outside of the School or for activities other than those authorised by the School is forbidden

The School reserves the right to use images of any student or member of staff in various materials including the publicly available website.

If you do not wish this then please place a tick in this box [ ]

PLEASE SIGN AND DATE BELOW:

Name ..... Tutor Group ..... (students only)

Signed:……..... Date .....

John Willmott School - Computer Network Acceptable Use Policy

If you have any questions about the policy, please contact the IT Operations Manager.

The School assumes the honesty and integrity of its IT users. Facilities are provided in as unrestricted manner as is feasible in order to offer the best possible quality of service.

It is the users' responsibility to ensure that they comply with the policy. The latest version is made available on the school VLE.

All staff and students will be invited to sign an agreement to abide by the policy.

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 behavioural code.

1. 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, lewd, obscene, libelous, 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, 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 computer network by a member of IT Support.

Visit, use, download, or store any game, either application or browser-based, without permission of a supervising teacher, and only for educational purposes.

The School reserves the right to refer any breach of this policy to the respective Mentor / Tutor / Head of Department and / or member of the Leadership Team. This may result in the suspension of any or all parts of the services provided.

2. Network Services

This comprises of access to desktops, laptops, tablets, mobile devices or other devices (PC, Mac, Linux and other platforms) in the various classrooms, labs or other areas for all users, and for staff additional access in departmental offices for the purposes of School Administration.

Storage of files for all users is available on the School network.

All users shall have complete access to any files they have created, except where ownership / authorship is in question. This is then referred to the relevant Mentor / Tutor / Member of the Leadership Team.

Each user shall have a unique username and password. The password must not be divulged to any other user or any third parties outside of the School.

There are systems in place to monitor all network usage and as such there is no expectation of privacy on the school's network.

3. Internet Services

Each User shall have access the Internet via the School's BGFL 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 Leadership Team.

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 to the deny list. Users should report offending material to IT Support by supplying the complete website address.

Whilst the school makes every effort to filter material as defined in the General Policy, the school cannot be held liable for any failure to filter such material due to the nature and proliferation of such sites on the internet.

There are systems in place to monitor all internet usage and as such there is no expectation of privacy on the school's network regarding internet access.

4. Mail Services

If a user sends an email that contains content as defined in the general policy, their account shall be locked and not released until they the school has received authorisation from a parent or guardian and then only in consultation with a member of the leadership team.

If a user repeatedly sends material as defined in the general policy the matter will be referred to a member of the Leadership Team.

Any user who receives unsolicited mail can inform the IT Manager who will endeavor to trace the originator and report them to their Service Provider.

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 Leadership Team.

Users email can be monitored by IT support at the request of the Headteacher, Governing Body or other legal agencies.

There are systems in place to monitor all email usage and as such there is no expectation of privacy on the school's network regarding email services.

5. Security

Each User will be given a unique username and password that will allow them to access their account.

The username 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 username and password of another user their services may be suspended and immediately referred to their respective Mentor / Tutor / Head of Department and then to a member of the Leadership Team.

The only programs that may be used within the School are those agreed on by the IT Manager and / or Leadership Team and installed by a member of IT Support. The introduction 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 including but not limited to user's individual saves areas, either manually or through automated software, to ensure policy compliance and to aid in resolving any issues.

While the school takes every precaution to ensure adequate backups of all data stored on its servers, users should be mindful of ensuring they have taken appropriate steps to safeguard their own work.

6. Treatment of Equipment

IT Support will endeavor to ensure all equipment is in working order, should any user find that a piece of equipment does not work correctly they are to report it to a member of IT Support and not attempt to repair it themselves.

Any user who causes damage directly or indirectly intentionally, through neglect or through any other actions 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.

7. Photography and School Promotion

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 inside or outside of the school without explicit permission.

Photographs taken of students or staff either on the school premises or on activities such as field trips should be stored on the school systems which are secured against un-authorised access.

Those photographs should only be used for the purposes for which they are intended. When the student(s) leave the school or the images are no longer required, they should be deleted from the school systems in accordance with the Data Protection Act 1998.