

# Churston Ferrers Grammar School

## Acceptable Use Policy for Network & Internet

Revision 25 January 2008

### **General Statement**

The school has invested very heavily in state-of-the-art Computer Rooms and it is essential that clear guidelines are set out that will ensure the safe and efficient use of the system and its many component parts.

We have a broadband connection to the Internet via the 'South West Grid for Learning'. In supplying this link, the Swgfl implicitly apply their own conditions of use, which may be found on the staff internet link site.

In order to be able to use the system at all, all users must accept the stated conditions (below) and also agree to all aspects of best practice. Permission to use the School's I.C.T. facilities will only be given after agreement by users to the terms and specifically a continued adoption of those practices. Failure to comply fully at any time may be deemed to have broken the rules of acceptable use and permission to use the system is thereby suspended.

Users must have read, understood and accepted the school's published policy for the network & internet. The 'Computer Misuse' and 'Data Protection' acts also apply in law. Users should also be mindful of current copyright legislation. Serious abuse may be construed as a criminal act and further proceedings may result.

A summary of the conditions of use is printed in each student's planner. They and their parents must have read and subscribed to the terms therein. The summary makes very clear how the rules are to be applied and interpreted as also what will happen if they are disregarded. These points are reprinted at the end of this policy for staff information.

### **Computer equipment**

1. Staff are responsible for keeping in good order any computer hardware (laptop or pda) loaned to them and for ensuring that any fault or damage found on equipment is reported to the IT technical team.
2. No software should be copied onto or removed from any computer hardware without the required software license being presentable to the ICT technical team during the annual inspection audit.

## Passwords

1. Users must use ONLY their own valid username and personal password to log on to the school Network, the Internet, Moodle, FTP or Email. The password will not be divulged to anyone, at any time! Users must immediately report to the I.T. technical team, if at any time their access to any of these resources is compromised. If it is evident that validation has been refused, then the person must seek help immediately from I.T. staff to resolve the issue. Any attempt at or actual use of another user's identity / username / password will automatically nullify this contract and is further an infringement of the 'Computer Misuse Act'.
2. Terminals must never be left unattended when signed-on to the system. If it is necessary to deal with an immediate concern the computer must be locked using the windows software facility by pressing Ctrl+Alt+Delete and choosing lock computer.
3. Passwords must not be disclosed to unauthorised persons. Passwords should be a minimum of 5 characters in length and changed regularly. Forgotten passwords will be reset by the network manager. The frequency of password change depends upon the access rights granted to each individual user, nature of the data and the level of security required to ensure the integrity of the system. Our current password policy is as follows:
  - **Staff** can request a system password change through the network manager at any time. The SIMS terminal service **requests a monthly** alphanumeric password change. Passwords on the network, email & assessment system should be changed **termly**. If staff are aware of, or are concerned that their password security has been compromised, they must immediately inform the network manager.
  - **Students** will be issued a randomly generated alphanumeric password which should be changed if you suspect someone knows your password. Students are unable to manually change the password. Students have no access rights to confidential data. Students passwords will be changed **annually**.

## Use of Equipment

1. All computer facilities (ICT suite, laptop and pda) are made available to staff to carry out their professional duties. Use of the equipment at home for personal use, providing internet safety measures are in place is acceptable. The equipment should be kept safe and when not being used in a secure and locked environment at all times.

2. Repairs and disposal of equipment concerns should be passed through to the network manager who has sole responsibility in ensuring the equipment is made good and disposed of appropriately in accordance with current statutory regulations.
3. Staff may be issued with a Laptop on loan. This requires the signing by them of the further terms and conditions associated. A special form is provided. Some students may be given permission to bring their own portable computers to school by the Head of Sixth Form. This requires specific permission and the affirmation of a further 'Student Laptop Contract'.
4. The use of such equipment must be for educational purposes only. No attempt must be made by a student to use a personal computer, PDA etc. to connect to the school Network unless authorised to do so and having already completed a laptop contract.

### **Use of the Intranet**

1. Under no circumstances will files other than non-executable files produced by the student themselves be allowed to be copied onto the Network. Only sensible naming of files will be tolerated. Deliberate unauthorised access to, copying alteration, or interference with computer programs or data is not allowed. Users will only access those drives specifically allocated to them, e.g. A or 'Floppy Drive', H or 'Home Drive', P or 'Picture Drive', T or 'Temporary Drive'. Under NO circumstance must attempts be made to access any other areas on the system.
2. If any unusual desktop or application appears, it is the direct responsibility of the user to alert ICT staff. Only those applications where a start menu short-cut is provided are authorised. Users will only ever log on to a single station at one time and ensure it is reset correctly before they leave.
3. Students may only enter a Computer Suite with the permission of a member of staff. No unsupervised access to the rooms will be allowed. Students will use computers designated for pupil use only. No student will attempt to use any machine marked or obviously for staff use or in a non-designated area.
4. No damage should be made to the computers, associated equipment or suites in general. Machines will not be moved, nor should any be switched on or off without permission. All equipment is to be handled in an appropriate manner, such as to maintain it in the best possible condition. No food, drink, sweets nor any other substance likely to be detrimental is ever to be brought into the I.T. suites, whether in bags or openly. The machine, mouse, keyboard, chair etc. are to be replaced in a tidy fashion after use.
5. No attempt is ever to be made to access internal components of machines, nor introduce foreign objects. Any physical defects or errors must be reported

immediately to a member of staff, or else liability may rest with the last registered user. Anyone proven to have intentionally damaged equipment may well be reported for criminal damage and certainly be obliged to compensate financially for any loss. They will be barred from the system.

6. Printing resources will be granted to laser print all reasonable school coursework, homework and research. Printing will not be allowed directly from electronic sources such as Encarta or the Internet. To print, all files must be saved to the home drive with a short sensible name. Multiple copies cannot be printed nor more than 5 pages at a time. All users are allocated regularly allocated print credits.
7. No information or data is to be sent using any part of the Network and the access granted here from within or outside of the system, to any other user, which may be construed to give cause for concern or offence to that user, be racist, sexist, etc., be in general bad taste, bring the reputation of the school into disrepute, or be in any way unlawful.

### **Use of Internet based services**

1. The Network and ICT services provided by the school remains the intellectual property of the school and no right of privacy is allowed. Home folders, Email and Moodle accounts are all open to scrutiny by I.C.T. Staff. Email is provided through Google mail and staff may, if they choose, use it for personal correspondence but should be aware that the school reserves the right to audit the account. All file movement and access to resources is monitored and any security violations will be recorded.
2. Internet access is provided for genuine educational use and academic research only. There is no absolute right of access granted to commercial sites or those that might have questionable content. Staff are provided with unfiltered access in accordance with the Swgfl Acceptable use policy. Non-educationally based games will not be played under any circumstances. I.C.T. will use filtering to block sites which have potentially harmful or questionable content. However, new sites appear continually - just because a site may be accessible, it does NOT imply that CFGS implicitly approve of the content. Such lapses must be immediately reported. Common sense, good taste and judgment must also always be exercised. Copyright laws must always be respected when using material found on the internet. Printing directly from the Internet is not approved and wholesale copying of material cannot be justified and may lead to accusations of Plagiarism.
3. In accessing the CFGS Network / Intranet from outside the school site, e.g. from home, the exact same terms of reference will apply. Access rights are NOT to be shared with any other party. No programme or tool or device of any

description is to be run, remotely or otherwise, which may compromise the network in any way, whatsoever.

4. When using School laptops and connecting to the internet Staff should ensure that reasonable security precautions are taken by using the installed virus scanner software. Also that no confidential data is stored on the laptop hard drive without file password protection. The same policy applies to all portable storage devices. Further guidance is available from the IT technical team.

### **Information Contained in Student planners**

The internet, Moodle (our online classroom), an email account and the school network are provided by the school for legitimate and appropriate use. You must read and sign below to show that you have understood the contract and will abide by its rules and principles.

### **Rules**

1. No food or drink is to be brought into IT rooms.
2. Equipment should never be moved or unplugged.
3. Computers should not be switched on or off without permission.
4. You can only enter a computer room with permission and under the supervision of a member of staff.
5. The network remains the intellectual property of the school and no right of privacy is allowed.
6. Laptops may only be brought into school on completion of a laptop contract. These are available from the network manager.
7. Mobile phones can only be used with the permission of the teacher.
8. To print work the file must have been saved in your work space with an appropriate name. Multiple copies of work cannot be printed.
9. Colour printing must be put on the T drive and a request put in to reprographics.

**You are abusing the school network and internet facility if you do any of the following:**

- Bypass the school filtering rules by using any website designed to allow unfiltered internet access;
- Log on to the network or the internet using another person's username and password;
- Attempt to find out anyone else's username and password;
- View or navigate any website with inappropriate content, including social chatrooms, games and pornographic or offensive material;
- Edit, delete or move another person's files or folders;
- Tamper with the network settings in any way;
- Introduce inappropriate or offensive material to any drive on the school network;

- Introduce any software program that could corrupt, damage or modify the school network, including viruses;
- Physically damage computer equipment;
- Steal computer equipment.

### **Statement of Procedures in the Event of Abuse**

**If you abuse the system**, your parents will automatically receive a letter outlining the abuse. The school may then decide to:

- Take away your right to use the network and/or the internet for a certain period of time;
- Give you the job of ICT monitor in ICT rooms at break times, so that you contribute to the running of the school network;

*or*

- Use any other sanction that is deemed appropriate to the abuse.

**If you abuse the system more than once**, it will be seen as a deliberate disregard for the school's network policy. Your parents will automatically be asked to come into school to discuss the abuse.

Normal school sanctions will apply if material that you view or share causes harm (or has the potential to cause harm) to other students or staff in the school. These sanctions may include any consequence that the school decides is appropriate, including a fixed-term suspension.

I.C.T. Dept. January 2008