

King George V College

IT Usage

**Code of Practice for College
Staff**

+

Staff Handbook



STAFF USE OF COMPUTERS AND SOFTWARE APPLICATIONS

Please note that the KGV IT Usage Policy is published on the Moodle home page. The Computer Access Handbook, published each September, is also available on the Moodle home page and contains information about the Curriculum Computer Network, KGV on-line access, accessing email from home, use of the internet and general information for all users.

This Handbook contains further information for staff:-

Code of Practice for College Staff

- Computer Security
- Laptop Computers
- Unacceptable Practices
- Removable Media
- Internet & Email
- Remote Access & Remote Working

Data Protection Act

- Data Management Policy

Curriculum Network Issues

- Contacting IT Support
- IT Disciplinary Issues

The JISC Legal Information Service has published an article that covers IT among other duties of care. The article can be found at:-
<http://www.jisclegal.ac.uk/publications/Dutyofcare.htm>

CODE OF PRACTICE FOR COLLEGE STAFF

The college needs to ensure that members of staff use computer equipment and its applications in such a way as to

- minimise the risk of damage to property (including files and software) and
- ensure that all legal responsibilities of individuals and the college are met.

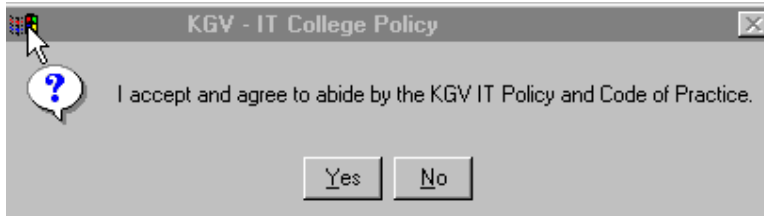
The College, its Managers and staff are increasingly liable for the inappropriate action of members of the college community. This can include:

- Sexual/racist harassment e.g. downloading objectionable material
- Copyright infringement of software, documents or photographs
- Misrepresentation and libel, particularly in emails
- Data misuse and inappropriate storage of personal information

All staff must be aware of, and enforce, this Code of Practice.

All members of the college are therefore asked to read this booklet and to make sure that they are aware of acceptable and unacceptable practice. Note that parts of the text also appear in the college Staff Handbook.

The College Curriculum Network also asks all users to accept responsibility for compliance with the College IT Policy and Code of Practice as they log on.



Staff must be aware that their activities may be monitored and the work they produce in the course of their employment is the property and copyright of the college. In particular staff should note that the college network enables IT managers to view individual computer screens remotely, to view records of internet sites visited and view emails. This may be necessary in the event of prolonged staff absence, or if there is reason to believe that communications are illegal or libellous. However, none of these will be undertaken in respect of college staff without the specific written authorisation of the Principal, giving reasonable cause. A fully detailed document 'Institutional Access' is available from Personnel.

Employees of the college wishing to make private contact with those outside the college are recommended to use the telephone facilities if they do not wish communication to be monitored. Phone calls will not be monitored other than date, time and contact number provided by the telephone company.

CODE OF PRACTICE FOR COLLEGE STAFF

Computer Security: all networks

- Access to hardware, software, and data is restricted to those who have right of access.
- Care should be taken to avoid unauthorised access: for example computers should not be left unsupervised with programs open.
- The Network Managers are responsible for setting access rights within the systems. Any additional access must be requested through the relevant Network Manager and recorded.
- All staff have access to confidential information on the network. Passwords should be changed at least once per term, must be at least eight characters and include at least two character types (letter, number, non-alphanumeric character e.g. * & # \$). Passwords must not be disclosed to any third party. Network Managers should place a clearly marked, sealed copy of their administrator password in the college safe in case of absence.
- As far as is possible, confidential data should not be stored on the hard drive of individual workstations: such information should normally be confined to a secure file server, located in a secure place away from open access.
- Software should be installed only by persons authorised by the College Network Managers. The use of unauthorised software is forbidden.
- IT Managers should also refer to the Code of Practice for IT Managers.

Laptop Computers

Laptops computers are provided to some staff to enable them to connect to the college network, either from within the college or as a terminal from home. Staff must not use their laptop computer to store private or KGV data (see Data Security Policy) and users must also be aware of the following:-

- Take care when transporting your laptop between home and college – think of your personal safety as well as possible damage to the computer.
- Do not allow the laptop to be used by others.

CODE OF PRACTICE FOR COLLEGE STAFF

Unacceptable Practices

None of the following should be undertaken by any member of the college staff without clear authorisation from the Principal or the relevant Network Manager (Curriculum, MIS or Finance).

- Interfering with the set up of any hardware or software on computers
- Changing any system settings or preferences other than standard changes enabled within software ('Word', 'Excel' etc.) and the personal desktop settings. Other changes to network settings would need the agreement of the Network Manager.
- Downloading or bringing into college any files/programmes containing viruses, pornography or other offensive material
- Installing software onto workstations or a network drive.
- Making pirate copies of any software or other media (MP3, MP4, DVD etc)
- Improperly copying other people's work
- Interfering with or corrupting the computer data or work of others
- Attempting to repair any equipment that appears faulty
- Using someone else's login
- Sharing or divulging passwords
- Removing any equipment or materials

CODE OF PRACTICE FOR COLLEGE STAFF

Internet and E-Mail

All use of the College Internet facilities by employees of the College in pursuit of their work is free of charge to the employee.

Normally, use of the Internet involves negligible additional cost to the College. So long as this is the case, employees of the College are permitted to use the Internet for personal reasons provided the following conditions are met:

- Personal use should normally be outside working hours, and any use in College time should not be detrimental to the member of staff's work in the College.
- Employees should never use the Internet to access or download any offensive or inappropriate material, for example pornographic or racist material.
- If employees use the College Internet facilities in such a way as to involve disclosure of personal or financial data (e.g. credit card details), the College will bear no responsibility for the security of this information.
- Permission should be sought before any Internet operation by an employee incurs expense to the College.
- College employees should not use the College Internet and e-mail facility for commercial purposes, such as in operating a separate business.

Staff are also able to use the College e-mail facility for personal use, but as with phone calls and internet use, personal e-mail correspondence should normally be outside working hours or at reasonable times which do not interfere with the member of staff's work in the College.

All e-mails being sent from the College include an automatic disclosure advising that the contents of the e-mail are not necessarily the views of the College.

Misuse/abuse of internet or email facilities could result in disciplinary action being taken against a member of staff.

Web Sites

Given the public accessibility of information on Internet sites, the College will ensure that personal details and pictures relating to staff and/or students fully protect the personal rights of each individual.

The Staff Handbook contains guidelines on disclosure of personal information on college websites.

CODE OF PRACTICE FOR COLLEGE STAFF

Remote Access & Remote Working Policies

KGV provides the following remote access facilities:-

General

- College Web Site Access

KGV Students

- College Web Site Access
- KGV Online - timetables, attendance and progress reports
- Email – Outlook Web Access
- Moodle – Online VLE
- KGV Remote Desktop access

KGV Staff

- College Web Site Access
- Email – Outlook Web Access
- Moodle – Online VLE including staff area
- VPN / Remote Desktop access

- No unauthorised person or machine shall be permitted to gain access to the college resources
- Remote machines, used by staff or students, must be located in a secure place and logged off when not in use
- College resources shall be used only for the purpose for which they are authorised.
- Home computers, used to access the KGV VLE and VPN, must have effective and up to date anti virus software installed.
- IT Network Managers are responsible for all aspects relating to Access Controls and Security – see the Code of Practice for IT Managers.

Data Protection Act

Anyone processing personal data must comply with the eight enforceable principles of good practice. Data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept longer than necessary
- secure
- processed in accordance with the data subject's rights
- not transferred to third parties unless they are authorised and have adequate data protection.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual, although in some limited circumstances exemptions will apply. If there is any doubt over an action, the advice of the College's Data Protection manager should be sought.

CODE OF PRACTICE FOR COLLEGE STAFF

Data Management Policy

'KGV Data' is information about KGV staff, students and resources (funds, space etc.) that is captured and used by members of the college community on a day to day basis.

Examples of systems/databases that contain KGV Data include but are not limited to:-

College Admissions System	Student Record System
Human Resource System	Financial Accounting System
Budget	Property Management
Student References	College Web Site
Moodle	Staff Resource Material

Specifically excluded are notes and records that are the personal property of individuals. e.g. medical records, private teaching notes.

Ownership

The College owns all KGV data

Access

The college's data controller is responsible for defining access permissions.

Access Controls, Backup and Security

IT Network Managers are responsible for all aspects relating to Access Controls, Backup and Security – see the 'Code of Practice for IT Managers'.

User Responsibilities

All data users are expected to:-

- Access KGV Data only in their conduct of KGV Business.
- Provide data only to parties who are other appropriate employees willing to abide by these guidelines.
- Obtain and process data in a fair and lawful manner.
- Only store data relevant to the operation of the college.
- Not store data longer than necessary.
- Keep data secure.
- Review information created to ensure their results are accurate and the data has been interpreted correctly.
- Respect the confidentiality and privacy of individuals whose records they access.
- Respect the Copyright of all data they would seek to add to KGV systems.
- Observe any ethical restrictions that apply to the data being accessed.
- Abide by applicable laws or policies with respect to access, use or disclosure.
- Use passwords, as defined, and keep them secure.

Data Classifications

1. Low Sensitivity (General Use)

This is Data that would not adversely affect an individual or the college if it was used inappropriately, e.g.

- Class lists
- Teaching materials
- Student work
- Management information reports which do not identify individual learners
- Any data which has been made a matter of public record

2. Medium Sensitivity (Internal Use)

This is data that would have some adverse affect on an individual or the college if it was used inappropriately, e.g.

- Personal Sensitive Data as identified by the Data Protection Act (1988) specifically data relating to racial or ethnic origin, political opinions, religious beliefs, membership of trade union organisations, physical or mental health, sexual life, offences or alleged offences.
- Data that would be likely to cause damage or distress to an individual or the college if it were lost or stolen e.g. Staff human resources data or student exam or assessment results which are not a matter of public record
- Data which is considered sensitive, personally confidential or commercially confidential. For example, data or materials pertaining to existing or planned courses which may be of interest to a competing organisation.

3. High Sensitivity (Confidential Use)

This is data that would have a significant adverse affect an individual or the college if it was used inappropriately, e.g.

- Exams data
- Finance and Funding data
- Learning Support Student Information
- Staff and Student personal information
- HR data
- IT Administrative details

Transfer of KGV Data

The transfer of medium or high sensitivity KGV data out of the college is forbidden unless authorised by the college's data controller. The college provides staff with secure remote access to college data and there is no requirement for data to be removed from the college via memory sticks, e-mail or other media.

Transferring data via e-mail or memory sticks is not secure.

If you have obtained permission to transfer medium or high sensitivity college data via these methods then the IT department will advise on how to do this securely.

CURRICULUM NETWORK ISSUES

Contacting IT Support

Please use the following methods to contact IT Support:-

Telephone	ext 561
Email	ITSupport@kgv.ac.uk
Visit	Room C39

Hardware problems or IT Security Incidents can be recorded directly – use the Inform folder on your desktop, and select **Computer Register**. Click on either **Enter New Fault** or **Report Security Incident**. You can also use the **Computer Register** to check on the progress of a fault.

Do remember that all the IT Support staff are always pleased to offer advice.

CURRICULUM NETWORK ISSUES

IT Disciplinary Issues

We need to deal with the more serious problems of computer related misconduct by students in a way that ensures we react in a consistent manner and that relevant staff are informed. It is recommended that staff use the 'Computer Misuse' form available from Harry Carr so that incidents are recorded and dealt with in a consistent way.

Please remember that removal from network resources is a serious penalty that does restrict the student's ability to attend IT lessons and submit coursework.

Suggested Penalties for Computer Misuse

Offence	Penalty
Use of another student's login	1 week ban from LRC computers
Allowing other to use login	1 week ban from LRC computers
Use of unauthorised files	1 week ban from LRC computers
Use of chat lines	1 week ban from LRC computers
Playing computer games	1 week ban from LRC computers
Repeated offences	Up to 1 month LRC ban
Continued repetition of offences	Permanent ban from LRC
Sending offensive or inappropriate E-mail messages	1 month ban from LRC computers
Downloading, storing or transmitting offensive or pornographic materials depending upon materials found.	1 week up to a permanent network ban. Parents informed.
Deliberate damage to the network either software or hardware	Permanent ban and misconduct investigation

Issues that may involve a criminal offence must be passed immediately and directly to a member of the SMT.

The imposition of sanctions is administered on-line by IT and LRC staff. Tutors receive an automatic email notification and individual student history can be viewed by all staff via the Network Admin Discipline icon on the desktop.