Brockenhurst College IT & Telecommunication Systems

Regulations, Policies and Procedures Handbook


it
Brockenhurst
College
IT Services

CONTENTS

Regulations for the Use of Computer Equipment and Data Networks at Brockenhurst College — 5
General Outline — 5
Computer Misuse — 5
Copyright — 6
Data and Voice Networks — 6
Data Protection — 7
Withdrawal of Service — 7
Liability — 7
Use of Email — 7
Regulations for Network Account Holders at Brockenhurst College — 8
General Outline — 8
Accounts and Passwords — 8
Access to User Accounts — 9
Regulations for the Use of Email and Internet Systems at Brockenhurst College — 10
General Outline — 10
Internet & Email Usage — 10
Private Use of Internet and Email — 10
E-Safety Policy — 11
General Outline — 11
Contact — 12
Content — 12
Commerce — 12
Conduct — 12
Student Network Storage Quota Policy — 13
General Outline — 13
Disk Quota Allocations — 13
Student Printing Policy — 14
General Outline — 14
Printing Charges Per Page — 14
Printing Credit Initial Allocations — 14
Virus and Anti-Virus Policy — 15
General Outline — 15
College Virus Protection — 15
Off-site Virus Protection — 15
Disciplinary Policy for Student Misuse of College IT Systems — 16
General Outline — 16
Policy Detail — 16
Network Access Periods and Security — 17
General Outline — 17
Access Times — 17
Intruder Lockout — 17
Automatic User Desktop Locking — 17
Scheduled System Maintenance Periods — 17
Brockenhurst College Data Protection Policy — 19

General Outline 19
Status of the Policy 19
Notification of Data Held and Processed 19
Responsibilities of Staff 20
Data Security 20
Student Obligations 20
Rights to Access Information 21
Publication of Brockenhurst College Information 21
Subject Consent 21
Processing Sensitive Information 22
The Data Controller and the Designated Data Controller/s 22
Examination Marks 22
Retention of Data 22
Conclusion 23
Staff Guidelines for Data Protection 23
Staff Checklist for Recording Data 24
Freedom of Information Act 24
Terms & Conditions of Use for College Laptops, Tablets & Handheld Devices on Loan to Staff 25
Guidelines for Staff on Acceptable Use of College Mobile Phones 26
General Outline 26
Issue of a Telephone 26
Security 26
Costs 26
Personal Use 26
Use While Driving 27
Use When Travelling Outside the United Kingdom 27
Student, Staff and Site Security 28
Student Security, ID Cards and Personal Safety 28
Staff Security, ID Cards and Personal Safety 29
Procedure for the Use of CCTV at Brockenhurst College Sites 31
General Outline 31
Objectives of the CCTV System 31
Forms Relating to this Procedure 31
Statement of Intent 31
Operation of the System 32
Complaints 32
Access by the Data Subject 33

REGULATIONS FOR THE USE OF COMPUTER EQUIPMENT AND DATA NETWORKS AT BROCKENHURST COLLEGE

GENERAL OUTLINE

The use of college computer systems and data networks by staff, students and visitors is subject to the conditions set out in this document. These conditions have the status of disciplinary regulations and apply to all members of the college. In the context of these regulations, 'members of the college' includes all staff, students and authorised visitors.

There are three Acts of Parliament that regulate the use of computer equipment, the Data Protection Act 1984; Copyright Designs and Patents Act 1988 and the Computer Misuse Act 1990. In addition to these acts the use of public data telephone networks is regulated by the Telecommunications Act 1984.

These and several other acts (including the Obscene Publications Act 1978 as amended by the Criminal Justice Act 1994) identify a number of prohibited actions relating to the use of computers. Prohibited actions, if proven in a court of law, may lead the perpetrator to a fine, imprisonment or both. It is possible a suit for damages in the civil courts may also ensue.

The regulations are designed to remind all members of the college of their legal obligations under these Acts. It should also be stated that the use of computer software may also be subject to the terms and conditions set out in the licence agreements from the licensor, into which the college has entered and which are enforceable by the licensor in the civil courts.

Paul Shepherd : IT Services Manager *Email: pshepherd@brock.ac.uk*

COMPUTER MISUSE

1. Members of Brockenhurst College are allowed only to use those computing resources, data or voice communications facilities which have been allocated to them by the computing management.

   Definition of 'the computing management' is the Principal, College Director, IT Services Manager, Assistant IT Services Manager or Middle Manager.

2. Computing resources, including data and voice communications networks may only be used for correctly authorised purposes. Brockenhurst College computer systems may not be used for playing games, sending console messages, installing / using illegal software, using remote control software, accessing another user's account or using chat programs.

3. The computing, data and voice communications resources may only be used by the person to whom they have been granted. Members of the college community may **not** lend or give these resources to any other person unless they are explicitly authorised to do so by the computing management.

4. Members of the college may **not** access, alter, erase or add to computer material which has not been created by them, unless they are explicitly authorised to do so by the computing management.

The Computer Misuse Act makes it an offence to attempt such actions

5. Authorised users of the computer systems must take reasonable care to prevent unauthorised use of computing resources allocated to them, particularly the security of your network account password.

6. Members of Brockenhurst College may **not** use the computer systems or networks in such a way as to compromise the integrity or performance of the systems or networks.

7. Members of Brockenhurst College may not tamper with, move systems, disconnect equipment or attach peripheral devices or tamper with the network or its infrastructure. Should the equipment or systems need to be moved or modified a member of the IT Services Team should be contacted by emailing helpdesk@brock.ac.uk or by phone on Ex. 548.

   These regulations cover the activity commonly known as 'hacking'. Breach of any of these regulations is evidence of an offence under the Computer Misuse Act.

COPYRIGHT

Members of Brockenhurst College will comply with the provisions of the Copyright Designs and Patents Act 1988 (as amended) in relation to any computer program or data set, and shall not in any way contradict the terms of any licence agreement applying thereto.

1. Members of Brockenhurst College must **not** use 'pirated' software. It is an offence under this Act to use unlicensed software.

2. All users must ensure that they comply with the licensing arrangements of any software package that they use or load on to a College computer system.

3. Users may not make personal copies of any College software resources.

DATA AND VOICE NETWORKS

1. Members of Brockenhurst College must abide by any 'Conditions of Use' of data or voice networks, which are published by the Student Administration Manager for the protection of the integrity and efficiency of the network.

   Use of the Internet is subject to the 'Conditions for acceptable use' published by UKERNA, the managing body of the JANET network; copies of these conditions are available from the IT Services Office.

2. Members of Brockenhurst College must not cause obscene, pornographic, discriminatory, defamatory or other offensive material, or material that otherwise infringes a right or inherent right of another person to be transmitted over the college, national or public networks, or cause such to be stored in Brockenhurst College computer systems.

   It is a criminal offence to publish pornographic material e.g. by including such material in a web page. Possession of pornographic images involving a minor is a criminal offence. Whilst possession of other pornographic images is not a criminal offence, it is nevertheless an offence against College regulations. The reference to 'a right or inherent right' clearly prohibits the publishing of copyright material. It is important to note that this clause also covers material

that might be construed as infringing the rights of an individual under the Equal Opportunities Act 1984.

DATA PROTECTION

Members of Brockenhurst College are allowed to hold, obtain, disclose or transfer personal data (as defined by the Data Protection Act 1984) as permitted by the College's registration with the Data Protection Registry and in accordance with the Data Protection Principles as set out in the Act.

WITHDRAWAL OF SERVICE

1. The computing management may withdraw access to facilities from any user for the purposes of investigating a breach of these regulations. Any withdrawal of service lasting for more than two weeks will be notified to the user's tutor or line manager (as appropriate).

2. The computing management may withdraw access to facilities from any user found to be guilty of a breach of these regulations.

LIABILITY

1. Brockenhurst College accepts no liability for the correctness of any results produced using any computing facilities, data or voice networks, for any failure of equipment to produce results or for any consequential loss or damage.

   Users are advised to make and retain their own backup copies of their data. IT Services will not routinely restore data from main system backups unless in extreme circumstances.

2. Brockenhurst College will hold the user personally responsible for any costs or claims, which may arise from any use of college computing and/or communications facilities, whether authorised or not by the computing management.

USE OF EMAIL

1. The use of the College's email system is restricted to members of staff and students only. Brockenhurst College will hold the user personally responsible for any defamatory or malicious emails sent from the College systems, this also includes flood emailing other organisations systems or **"Hacking"** into such systems.

REGULATIONS FOR NETWORK ACCOUNT HOLDERS AT BROCKENHURST COLLEGE

GENERAL OUTLINE

Network accounts at Brockenhurst College are maintained by the IT Services team and are available to users once the user has signed the declaration on the Learner Agreement (Students) and Staff Record (Staff) forms. All users are bound by the regulations set out below and by the **Regulations for the Use of Computer Equipment and Data Networks at Brockenhurst College**.

ACCOUNTS AND PASSWORDS

1. Users will be assigned a unique user account based on their first initial and surname. The password will be set to a default password comprising of a capital P then the users date of birth for example **P12061981**. The first time the user logs onto the network they will be required to change it. This account may only be used by its owner. Owners may not re-assign access to network accounts and will be held responsible for all data stored on and accessed from that account.

2. Your chosen password that is allocated to the account must be kept in strict confidence and not divulged to any other person. You, as the owner of this account, will be held responsible at all times for all data stored on and accessed from that account. If you suspect that someone has gained access to your password you should inform the IT Services team who will change it for you.

3. Users who are seen or caught using chat programs, playing games, bypassing internet restrictions, sending malicious emails or generally using systems for any other purpose other than for college associated work will have their accounts disabled and will need to speak to either the IT Services Manager, Assistant IT Services Manager or Senior IT Services Officer before the account is re-enabled.

4. For users who continue to misuse the Computer Equipment and Data networks their network accounts will be disabled and upon the second offence they will be subject to an account re-enabling charge. For a list of these charges please contact IT Services.

   Implication of the Computer Misuse Act: giving your password to someone else may be seen as aiding and abetting illegal access to Brockenhurst College systems.

PASSWORD CHANGE POLICY

The security of your IT network password is strengthened as follows:

You must not re-use a password that you have used previously.

Your password must:
1. Be at least 8 characters long.
2. Contain one or more UPPERCASE characters.
3. Contain one or more lowercase characters.
4. Contain 1 or more numbers.

You should never share your password with anyone else.

If you have any questions or concerns about password security please contact the IT Services Office by visiting the Helpdesk in M07B or by phone on Ex. 548 (01590 625548).

ACCESS TO USER ACCOUNTS

1. Users must take all reasonable steps to ensure that their accounts are protected from access by others. The account owner will be held responsible for any improper use of the account. In particular, you must not allow any other person to login to your account.

   If you need to share access to files and data with another user, then you should use the shared area on the network, specifically designed for this purpose or use my.brock.

2. The IT Services Team may examine any files, including mail files, if there is reason to believe that College regulations have been contravened in any way.

3. Large files on any student areas, which do not appear to be part of any coursework assignment, may be deleted at short notice to recover, disk space. This will apply, in particular, to graphic files and movie files (AVI, MOV, GIF, TIF, JPEG etc).

Once you have read these regulations you should retain this copy for your records, ensuring you have signed the declaration on the Learner Agreement (Students) or Staff Record (Staff) Forms.

REGULATIONS FOR THE USE OF EMAIL AND INTERNET SYSTEMS AT BROCKENHURST COLLEGE

GENERAL OUTLINE

The use of Email internal / external and Internet systems at the College by staff, students and visitors is subject to the conditions set out in this document. These conditions have the status of disciplinary regulations and apply to all members of the College. In the context of these regulations, 'members of the College' includes all staff, students and authorised visitors.

The purpose of these regulations is to provide the College and 'members of the College' with safe and secure systems to use and ensures that all individuals are aware of the legal rights of the College.

The College has the right to monitor any and all aspects of its telephone and computer systems that are made available to you, and may intercept and/or record any communications including telephones, email or internet communications.

To ensure compliance with this policy or for any other purpose under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations Act 2000 and the Regulation of Investigatory Powers Act 2000 Chapter 23, all 'members of the College' are hereby required to expressly consent to the College monitoring procedures. By signing either the Learner Agreement form in the case of students or by signing the Staff Record form in the case of staff and visitors you are hereby giving your express consent to the College's monitoring procedures.

INTERNET & EMAIL USAGE

Any Internet and email accounts are the property of the College and are designed to assist you in the performance of your College work. You should therefore have no expectation of privacy in any use of computer systems, or e-mail's sent and received, whether it is of a business or personal nature.

It is inappropriate for 'members of the College' to use email either College or Web Based mail and the Internet to access, download or transmit any material which might reasonably be considered to be obscene, abusive, sexist, racist or defamatory, including junk/spam email.

You should be aware that such material may also be contained in jokes sent by emails. Such misuse of electronic systems will be considered misconduct and will, in certain circumstances, be treated as gross misconduct and subject to the disciplinary procedure.

PRIVATE USE OF INTERNET AND EMAIL

Private use of both email and the Internet is permitted but must not be abused. However, members of the College who use College Internet facilities to conduct personal business or transactions online, for example online banking or online shopping, do so at their own risk.

While every effort is made to secure its IT Systems, the College will not accept any responsibility for personal losses incurred while using its systems.

Private/personal use of both email and internet should be kept to a minimum your line manager will advise you if they believe your usage is excessive.

E-SAFETY POLICY

GENERAL OUTLINE

The Colleges e-Safety Policy reflects the importance it places on the safe use of information systems and electronic communications.

- **e-Safety** encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate students and staff about the benefits, risks and responsibilities of using information technology.
- **e-Safety** concerns safeguarding children and young people in the digital world.
- **e-Safety** emphasises learning to understand and use new technologies in a positive way.
- **e-Safety** is less about restriction and more about education and about the risks as well as the benefits so we can feel confident online.
- **e-Safety** is concerned with supporting children and young people to develop safer online behaviours both in and out of College.

The Internet is an unmanaged, open communications channel. The World Wide Web, email, blogs and social networks all transmit information using the Internets communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Some of the material on the Internet is published for an adult audience and can include violent and adult content. Information on weapons, crime and racism may also be unsuitable for children and young people to access. Students need to develop critical skills to evaluate online material and learn that publishing personal information could compromise their security and that of others. The College has a duty of care to enable students to use on-line systems safely.

The College needs to protect itself from legal challenges and ensure that Staff work within the boundaries of professional behaviour. The law is catching up with Internet developments: for example it is an offence to store images showing child abuse and to use email, text or instant messaging (IM) to 'groom' children or young adults.

The College protects itself by making it clear to students, staff and visitors that the use of College equipment for inappropriate reasons is "unauthorised" and ensure that all users are governed by the Regulations, Policies and Procedures as set out in this document.

The rapid development and accessibility of the Internet and new technologies such as personal publishing and social networking means that e-Safety is an ever growing and changing area of interest and concern.

The Colleges e-Safety Policy operates in conjunction with all other College policies, including Behaviour, Child Protection and Anti-Bullying.

CONTACT

Contact via the Internet can mean that people have access to people and groups anywhere in the world. This can often have very positive advantages however, be aware that if you are making contact with people you do not know, you should limit the amount of personal information that can be viewed. Unprotected personal profiles could make you subject to online grooming, racial hatred, online bullying and potential assault. If you feel unsure about contact that you have made via the Internet please report the person either to the police, your parents (if applicable), your Tutor or a member of Student Services at the College. If the contact has been made via a social networking site (e.g. Facebook) you can report the user via the website.

CONTENT

It should be remembered that once any information/photographs are posted on social networking sites they become the property of the site. This means that although the image/information may be deleted by you, a copy of it is still owned by the respective site and you no longer have control of this information/image. If you publish inappropriate material online you are at risk of prosecution.

COMMERCE

Please be aware that it is very easy to be drawn into online gambling, financial scams and inappropriate advertising. Remember if it appears to be too good to be true it will be too good to be true! Be careful about signing up for offers using bank cards/credit cards without reading all the terms and conditions. Do not publish your personal details or financial details online without being sure it is a secure website. This is normally indicated by the padlock sign on the webpage.

CONDUCT

Sometimes people carry out activities which are deliberately meant to upset, offend or intimidate someone. These could be via a social networking site, a website or mobile phones. Cyber-bullying is a real issue; if you believe you are being bullied please talk to your Tutor, parent (if applicable) or someone from Student Services.

STUDENT NETWORK STORAGE QUOTA POLICY

GENERAL OUTLINE

Brockenhurst College IT Systems run centralised storage in the main Data Centre, this disk storage is for all students and staff to store their data files centrally which means they are secure and backed up nightly.

Disk storage is expensive when it is centralised this is because of the need for it to be of high specification as it is constantly in use 24/7.

Due to the large number of students, disk storage limits have to be controlled; this is achieved by allocating storage quotas to each student. The following quotas are in force:

DISK QUOTA ALLOCATIONS:

Student Category	Storage Quota
General 6th Form Student	500Mb
PhotoMedia 6th Form Student	1Gb
Computing & IT 6th Form Student	1Gb
Art 6th Form Student	1Gb

Note : In exceptional circumstances as a short term temporary measure, IT Services can increase an individual students storage allocation, however this is only done in cases where coursework deadlines are approaching and is only temporary until the student has completed housekeeping on their data files to reduce the storage being used.

STUDENT PRINTING POLICY

GENERAL OUTLINE

To reduce paper consumption/wastage and reduce College costs, network printing is now being limited by charging students for printing above an annual allocation of 300 black and white pages.

Once you have used your initial allocation, additional batches of 20 pages at £1 per batch can be purchased from the LRC or Student Services.

Having purchased additional printing units, you should take your receipt to IT Services located in Room M07B or the ILT Centre located on the first floor of the LRC to have the credit applied to your account.

Please note that any unused additional printer credits purchased during the academic year will not be refunded.

PRINTING CHARGES PER PAGE:

Type of print	Cost per page	Type of print	Cost per page
A4 Black and White	5p	A3 Black and White	10p
Colour Laser	30p	Colour Inkjet	15p

PRINTING CREDIT INITIAL ALLOCATIONS:

All students have the following printing credit allocations applied to their network accounts at the beginning of each new academic year:

Student Category	Printing Credit Allocation	
General 6th Form Student	300 Credits	(£15.00)
PhotoMedia 6th Form Student	600 Credits	(£30.00)
Computing & IT 6th Form Student	600 Credits	(£30.00)
Art 6th Form & Graphics 6th Form Students A-Level A2-Level	 800 Credits 910 Credits	 (£40.00) (£45.50)

VIRUS AND ANTI-VIRUS POLICY

GENERAL OUTLINE

- As the College computer systems continue to develop and access to staff and students increases, there is an ever-growing risk from computer viruses infecting the systems. There are many ways that such viruses can move from one machine to another.

The most common transfer methods are through USB Memory Sticks being brought into the College from external sources, files downloaded from the Internet and files received through Internet e-mail.

Some viruses can cause minor damage and inconvenience to a computer and others cause far more serious damage. Therefore it is necessary for virus protection software to be implemented on all College systems, both network and stand-alone machines and all servers.

COLLEGE VIRUS PROTECTION

- The College has a site licence agreement for Microsoft System Center EndPoint Protection. EndPoint Protection is used to protect the workstations, both on and off the network.
- Sophos AntiVirus is used to protect all servers.

Every effort has been taken to ensure that all systems are, and remain, virus free. It is impossible to guarantee that a new virus will not infect files or systems in the future.

It is essential that all staff, students and visitors who use any College systems and wish to use their files at home, must ensure they have taken adequate precautions on their home computers to prevent viruses being transferred to them.

You must purchase and install your own Anti-Virus software for your home machine. The College cannot accept any liability caused through a virus being transferred from a College system.

OFF-SITE VIRUS PROTECTION

- All students and staff are advised that they should purchase an anti-virus product from their computer retailer. The recommended products you could purchase are:

Microsoft Security Essentials

AVG Antivirus

Avast Antivirus

DISCIPLINARY POLICY FOR STUDENT MISUSE OF COLLEGE IT SYSTEMS

GENERAL OUTLINE

This policy has been put in place to safeguard College IT systems and genuine users. The policy is targeted at those users who use the systems for anything other than College associated work.

The policy came into effect on the 1st March 2001. All students will be made aware of the policy through tutor notes and there will be no exceptions to the recommended disciplinary action.

POLICY DETAIL

- **First Offence :** Students using the system in an inappropriate way will have their network account disabled and will need to see the IT Services Manager, Assistant IT Services Manager or the Senior IT Service Officer. The relevant Head of Division will be informed. The student will receive a warning and have to sign a form stating that they have re-read the regulations and agree to abide by them.

- **Second Offence :** Students offending for a second time (and on any subsequent occasions) will have their account disabled by the IT Services Manager, Assistant IT Services Manager or the Senior IT Service Officer. The student will be informed of the reason and be given a payment form.

The account will only be re-enabled once a re-enabling charge of £5.00 has been paid and the payment form has been stamped and returned to the IT Services office.

Persistent offenders will be required to have a formal interview involving their Head of Division and Parents. If the further offences occur, students will be required to pay the higher rate re-enabling charge of £10 per additional offence.

Students downloading, storing or viewing pornography will be suspended and Staff will be subject to the Colleges disciplinary procedure.

NETWORK ACCESS PERIODS AND SECURITY

GENERAL OUTLINE

This procedure will ensure the integrity of the College network and users data stored in the user areas. In the case of Staff members placing work in staff shared areas, this will mean that work cannot be deliberately altered or deleted by unauthorised users.

All authorised users are allocated network accounts and their access permissions are based upon category of system user be that Staff or Student.

It is accepted good practice that users should log out of their workstations to avoid unauthorised access to their files.

Where Network Account holders leave their workstations connected to the network, unauthorised access to network accounts and contravention of the UKERNA policy on Acceptable use of the Internet can occur.

To minimise disruption, as well as reminding staff and students about security of their network accounts, access to the college network is now time constrained. The purpose of this procedure is to ensure that workstations that connect to the College network are automatically logged out of the system during hours of College closure.

ACCESS TIMES

All full time students, community Education students and staff are able to access College systems 24 hours a day Monday to Friday accept where essential work is scheduled prior to 8.30am.

Saturday and Sunday are reserved for maintenance periods unless scheduled classes are due to run.

AUTOMATIC USER DESKTOP LOCKING

After a workstation has been left idle for a period of 15 minutes, the user's screen will automatically be locked, to unlock the screen the user must press ctrl, alt and delete then input their account password. Users are advised to save their work on a regular basis as if the workstation is switched off whilst the screen is locked they will lose any work that was not saved.

SCHEDULED SYSTEM MAINTENANCE PERIODS

Due to an increasing demand for access to systems during the College day and evenings, it is becoming increasingly difficult to run maintenance sessions on the main systems.

IT Services use scheduled maintenance periods to undertake essential work.

Maintenance periods willbe:

Monday to Friday.	Before 08:30am.
Saturday & Sunday.	All day with the exception of when scheduled classes are in session.

Note: Whilst users may be able to gain access to systems during these times, they should be aware that service could be lost without warning.

BROCKENHURST COLLEGE DATA PROTECTION POLICY

GENERAL OUTLINE

Brockenhurst College needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Brockenhurst College must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act).

In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Brockenhurst College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the college has developed the Data Protection Policy.

STATUS OF THE POLICY

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College. Any failure to follow the policy can therefore result in disciplinary proceedings.

Any member of staff, who considers that the policy has not been followed in respect of personal data about them self, should raise the matter with the designated data controller. If the matter is not resolved it should be raised as a formal grievance.

NOTIFICATION OF DATA HELD AND PROCESSED

All staff, students and other users are entitled to

- Know what information the college holds and processes about them and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the college is doing to comply with its obligations under the 1998 Act.

Brockenhurst College will therefore provide all staff and students and other relevant users with a standard form of notification. This will state all the types of data the college holds and processes about them, and the reasons for which it is processed. The college will do this at least once every three years.

RESPONSIBILITIES OF STAFF

All staff are responsible for

- Checking that any information that they provide to the college in connection with their employment is accurate and up to date.
- Informing the college of any changes to information, which they have provided e.g. changes of address, telephone number.
- Checking the information that the college will send out from time to time, giving details of information kept and processed about staff.
- Informing the college of any errors or changes. The college cannot be held responsible for any errors unless the staff member has informed the college of them.

If and when, as part of their responsibilities, staff collect information about other people, (i.e. about students course work, opinions about ability, references to other academic institutions, or details of personal circumstances) they must comply with the guidelines for staff, which are at Appendix 1.

DATA SECURITY

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should be

- Kept in a locked filing cabinet; or
- In a locked drawer; or
- If it is computerised, be password protected; or
- Kept only on disk which is itself kept securely.

STUDENT OBLIGATIONS

Students must ensure that all personal data provided to the college is accurate and up to date. They must ensure that changes of address, etc are notified to the Information Systems Office/other person as appropriate. Students who use the college computer facilities may, from time to time, process personal data. If they do they must notify the data controller. Any student who requires further clarification about this should contact the data controller.

RIGHTS TO ACCESS INFORMATION

Staff, students and other users of the college have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the college "Access to Information" form and give it to the data controller/their personal tutor or the Information Systems Manager.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing using the standard form attached at Appendix 2.

The college will make a charge of £10 on each occasion that access is requested, although the college have discretion to waive this.

Brockenhurst College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

PUBLICATION OF BROCKENHURST COLLEGE INFORMATION

Information that is already in the public domain is exempt from the 1998 Act. It is the college policy to make as much information public where possible, and in particular the following information will be available to the public for inspection:

- Name and contacts of college governors
- List of staff
- Photographs of key staff

The college's internal phone list will not be a public document. Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the designated data controller

SUBJECT CONSENT

In many cases, the college can only process personal data with the consent of the individual. In some cases, if the data is sensitive, **express consent** must be obtained. Agreement to the college processing some specified classes of personal data is a condition of acceptance of a student onto any course and a condition of employment for staff. This includes information about previous criminal convictions.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The college has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the courses offered. The college also has a duty of care to all staff and students and must therefore make sure those employees and students who use the college facilities do not pose a threat or danger to other users.

The college will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The college will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

Therefore, all prospective staff and students will be asked to sign Consent to Process form, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

PROCESSING SENSITIVE INFORMATION

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the college is a safe place for everyone, or to operate other college policies, such as the Sick Pay policy or Equal Opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will:

Be asked to give express consent for the college to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the **Vice Principals Office**.

THE DATA CONTROLLER AND THE DESIGNATED DATA CONTROLLER/S

Brockenhurst College as a body corporate is the data controller under the Act, and the corporation is therefore ultimately responsible for implementation. However, the designated data controllers will deal with day to day matters.

This college has 2 designated data controllers. They are Alex Scott and Limor Feingold.

EXAMINATION MARKS

Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. The college may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned to the college.

RETENTION OF DATA

The college will keep some forms of information for longer than others. Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so. In general information about students will be kept for a maximum of five years after they leave the college. This will include:

- Name and address,
- Academic achievements, including marks for coursework and
- Copies of any reference written.

All other information, including any information about health, race or disciplinary matters will be destroyed within 3 years of the course ending and the student leaving the college

The college will need to keep information about staff for longer periods of time. In general, all information will be kept for [five] years after a member of staff leaves the college. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. A full list of information with retention times is available from the data controller.

CONCLUSION

Compliance with the 1998 Act is the responsibility of all members of the college. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to college facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated data controller.

STAFF GUIDELINES FOR DATA PROTECTION

1. All staff will process data about students on a regular basis, when marking registers, or college work, writing reports or references, or as part of a pastoral or academic supervisory role. The college will ensure through registration procedures, that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the 1998 Act. The information that staff deal with on a day-to-day basis will be standard and will cover categories such as:

   - General personal details such as name and address,
   - Details about class attendance, course work marks and grades and associated comments.
   - Notes of personal supervision, including matters about behaviour and discipline.

2. Information about a student's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the students consent. If staff need to record this information, they should use the college standard form.

   e.g. recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties.

3. All staff have a duty to make sure that they comply with the data protection principles, which are set out in the college staff handbook and the college Data Protection Policy. In particular, staff must ensure that records are:
   - Accurate;
   - Up-to-date,
   - Fair,
   - Kept and disposed of safely, and in accordance with the college policy.

4. The college will designate staff in each area as 'authorised staff'. These staff are the only staff authorised to hold or process data that is:
   - Not standard data; or
   - Sensitive data.

   The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is necessary:
   - In the best interests of the student or staff member, or a third person, or the college; and
   - He or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances

   This should only happen in very limited circumstances. E.g. student is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the student is pregnant or a Jehovah's Witness.

5. Authorised staff will be responsible for ensuring that all data is kept securely.

6. Staff must not disclose personal data to any student, unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller, or in line with the college policy.

7 Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with college policy.

8 Before processing any personal data, all staff should consider the checklist.

STAFF CHECKLIST FOR RECORDING DATA

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the student been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?
- Have you reported the fact of data collection to the authorised person within the required time?

FREEDOM OF INFORMATION ACT

The Freedom of Information Act 2000, which came into effect on 1st January 2005, allows a member of the public to request information about the College and its activities, with the expectation that this information will be provided within 20 working days. Any member of Brockenhurst College who is asked to provide such information (whether or not the Freedom of Information Act is mentioned) should direct such a request to the Freedom of Information Officer.

Note that requests for personal data will need to be dealt with under the terms of the Data Protection Act, and such data are as a result likely to be exempt from disclosure.

The College has a "Model Publication Scheme" to be found at http://www.brock.ac.uk/freedom-of-information which explains how a wide range of data can be accessed directly.

TERMS & CONDITIONS OF USE FOR COLLEGE LAPTOPS, TABLETS & HANDHELD DEVICES ON LOAN TO STAFF

The equipment will not be treated as a benefit if the terms below are adhered to. However if the terms are not adhered to the equipment will be deemed to be a benefit and you will be liable for a tax charge.

The College wants to facilitate staff in their role with appropriate equipment but requires you to agree to the following arrangements prior to the loan of a portable computer or handheld device.

- You are expected to make significant use of the equipment in your College work.
- You should only use the equipment for College purposes.
- You are required to ensure the security of the equipment at all times. The use of a Kensington lock is not sufficient. College insurance covers equipment when it is offsite (e.g. in your home or car) but this cover is conditional on your taking reasonable care and theft precautions (please note that cover would only be provided if there was forcible entry into e.g. a locked room, cabinet or car boot and that even then cover would be unlikely if the equipment was left visible). Should the circumstances of any loss, damage or theft of your equipment not be covered by College insurance, you may be liable to pay up to £1,000 to the College for its replacement or repair.
- You will be required to bring the equipment into College for formal inspection by IT Services. The College has the right to inspect the equipment at any time. Inspection will take place once a year.
- The equipment remains your responsibility until returned to the IT Services Manager and the agreement below is signed off. Under no circumstances should you pass the equipment to anyone else.
- Should the equipment develop an operational fault or damage, you should return it immediately to IT. Support Services with all associated items e.g. Carry Case, Network Card. You should not attempt repairs yourself.
- You are required to keep the equipment in a satisfactory condition.
- You must return your equipment to the IT Services Manager at the end of your period of employment at Brockenhurst College.

LAPTOPS, TABLETS, HANDHELD DEVICES, AND THE DATA PROTECTION ACT

One of the Principles of the Data Protection Act (1998), states that 'Personal data should be kept safe from unauthorised access, accidental loss or destruction'.

Personal data in this context could refer to any data where it would be possible to identify the individual to whom the data refers. This could include confidential information such as assessments of either staff or student performance.

The College's registration under the Data Protection Act allows you to have such data on the laptop. In the light of recent thefts of laptops, you should consider carefully the implications of the Act.

1. Files on the laptop should be limited to those on which you are currently working.
2. Once you have completed work on a file, you should copy it to your network account, and delete the original from the laptop's hard drive.
3. Having deleted the file, you should also ensure that you empty the "recycle bin" using the icon on the laptop's desktop.
4. You should not use the laptop as backup for files on the network.
5. You should consider the use of passwords to protect your Word and Excel files. Both applications have an Options button on their Save dialogues, where you can set a password which will need to be entered before the file can be opened. As usual, choose passwords which you can remember, but don't write them down.

GUIDELINES FOR STAFF ON ACCEPTABLE USE OF COLLEGE MOBILE PHONES

GENERAL OUTLINE

These guidelines apply to any portable telephony device, including 'smartphones', used to communicate voice or data over a mobile telephony network.

ISSUE OF A TELEPHONE

a. Mobile telephones are provided to staff where the nature of their work requires wide mobility and simultaneous access to the public telephone network.
b. All requests for a mobile telephone must be made by a Middle Manager and authorised by a Director on the basis of appropriate supporting evidence and justification.
c. Telephones will be ordered, issued and asset audited by IT Services.
d. Holders of mobile telephones will be required to sign on receipt to confirm agreement with these Acceptable Use guidelines.

SECURITY

e. Telephones MUST NOT be loaned or entrusted to any other person – the security of the phone and operating costs remain the responsibility of the individual to whom it has been issued.
f. The telephone is NOT covered by College insurance. You must ensure that it is covered by your household or vehicle insurance.
g. Loss or theft must be reported to IT Services immediately.
h. You must present the telephone for inspection by IT Services when requested to do so.
i. Should the telephone be damaged or become faulty you should return it to IT Services – under no circumstances should you attempt to repair it yourself.

COSTS

j. All operating costs of the mobile phone are the responsibility of the relevant department.
k. Costs will be re-charged by the Finance Office monthly in arrears to an agreed budget and provision should be made by the budget holder to ensure that sufficient funds are retained to cover these costs.
l. All queries about charges should be directed to the Finance Office.
m. Planning information for budget holders about tariffs and other costs associated with operating a College mobile telephone is available from IT Services.

PERSONAL USE

n. Telephones should normally only be used in connection with College business.
o. If personal calls or data communication are made a record must be kept and these must be notified to the Finance Office so that costs can be identified and invoiced.
p. Bills are monitored on a monthly basis by the Finance Office and exceptions will be reported to the relevant Director for investigation.
q. Premium and subscription services and text alerts (e.g. football results, news headlines etc.) should not be used on College mobile telephones.

USE WHILE DRIVING

r. HANDHELD MOBILE TELEPHONES MUST NOT BE USED WHILE DRIVING UNDER ANY CIRCUMSTANCES.
s. If you need to make or receive voice or data calls when travelling in a car you should do so only when safely parked with the engine switched off.
t. In the unlikely event that your work requires you to be available to communicate while driving you should contact the IT Services Manager for advice about legally-compliant adaptive equipment.

USE WHEN TRAVELLING OUTSIDE THE UNITED KINGDOM

u. Wherever possible you should avoid making mobile telephone calls or data communications while travelling abroad.
v. In any event it is essential that you contact IT Services BEFORE you travel to request the latest guidance on coverage and costs of 'international roaming' for voice and data. This guidance is subject to regular change as tariffs are varied by the network operators.
w. Guidance may also be sought as to alternative telephone and internet service options in the countries to be visited.
x. Previous sections above provide information about the processing of charges and about your liability for personal calls.

Any questions about these Guidelines should be directed to the IT Services Manager.

STUDENT, STAFF AND SITE SECURITY

STUDENT SECURITY, ID CARDS AND PERSONAL SAFETY

The College takes Student Security and Personal Safety very seriously; all students must adhere to the following guidelines:

- On your arrival at Brockenhurst College are issued with a Student ID Card, holder and lanyard. You are required to wear your ID card at all times whilst on the College campus or other College sites, this is to protect students, staff and visitors by ensuring that only authorised members of the College are on these sites.
- From time to time College staff will carry out student ID card spot checks, as part of these checks you will be stopped and questioned if you are not wearing your ID card.
- It is your responsibility to ensure you remember to bring your card into College each day. Temporary cards are not issued. If you lose or forget your ID card and need a replacement there will be a charge of £10.
- Students are not permitted to lend their card to other students. Your card is used for ID, borrowing books from the Library and sitting exams.
- You must take full responsibility for any valuables that you bring into the College.
- Your personal safety and security is of utmost importance whilst you are at College. Please don't take any personal risks and always make sure that somebody knows (Tutor or friend) where you are at all times when you are on College sites.
- Close Circuit TV cameras (CCTV) are positioned in key areas around the College sites as part of our security measures to enable the detection and prevention of any criminal activity.
- If you witness any untoward behaviour or have any concerns relating to your safety or security please report them immediately to the nearest member of staff or to your Personal Tutor.
- If you have any questions or are unsure about any of the above you can discuss this with your Personal Tutor or another member of staff.

STAFF SECURITY, ID CARDS AND PERSONAL SAFETY

As members of staff working at the College it is important that you are always aware and report any security issues or possible personal safety concerns. You should not put yourself at risk or in potentially dangerous situations; both staff and student security and personal safety should be paramount.

All staff must adhere to the following guidelines:

- Staff ID Card, holder and lanyard must be warn at all times whilst on the College campus or other College sites, this is to protect students, staff and visitors by ensuring that only authorised members of the College are on these sites.
- You must take full responsibility for any valuables that you bring into the College.
- Close Circuit TV cameras (CCTV) are positioned in key areas around the College sites as part of our security measures to enable the detection and prevention of any criminal activity.
- If you have any questions or concerns you should discuss them with your line manager, IT Services Manager or Assistant IT Services Manager.
- Please remember that staff ID cards are also your electronic key cards to doors that are equipped with electronic door locks. Key carded rooms at Brockenhurst College include all IT Rooms and other rooms, both classrooms and staff work areas.
- Rooms that have electronic locks can only be accessed by authorised cardholders and only members of College staff, Cleaning Staff and Approved Contractors are authorised users.
- The system has been put in place to safeguard the equipment and to prevent unauthorised entry to rooms. Should you have any questions or queries about the system please contact a member of IT Services in M07B.
- Students are not permitted in any of the IT rooms during break or lunchtimes unless supervised by a member of staff.
- At the end of each lesson the member of staff using the room must ensure all students leave and ensure the room is secured. This means that key carded rooms will only be used when a member of staff is present.
- Staff ID/Key cards are your responsibility you must ensure its safekeeping. Staff are not permitted to lend their card to anyone else, this includes other members of staff and students.
- Should the card be lost or stolen please report it to IT Services immediately and you will then be issued with a new card.
- In the event of a member of IT Services not being available to deal with your problem please contact a Site Officer or the Estates Office. However, please do not ask them to open a room for which you do not have authorised access.

- Students, who require use of computers during break or lunchtime periods etc., should use the ILT Centre.
- Periodic checks on rooms will be carried out by IT Services and Estates staff, to ensure students are not using rooms unsupervised, and to ensure that key carded rooms have not been left open. Unsupervised students will be asked to leave.
- Key carded room doors should not be wedged/propped open for any reason, by doing so breaches the Colleges security and fire prevention policy. All doors are fire doors and as such prevent fire from spreading rapidly through the rest of the building.
- It is your responsibility to ensure you remember to bring your card in to work each day, IT Services and Estates are unable to issue you with a temporary card just for one day.

PROCEDURE FOR THE USE OF CCTV AT BROCKENHURST COLLEGE SITES

GENERAL OUTLINE

The purpose of this Procedure is to regulate the management, operation and use of the closed circuit television (CCTV) system at Brockenhurst College, hereafter referred to as 'the College'.

The system comprises a number of fixed and dome cameras located around the main College campus. All cameras are monitored from several Monitoring stations and are only available to selected staff on the Administrative Network.

This Procedure follows Data Protection Act guidelines and will be subject to review annually to include consultation as appropriate with selected College committees.

This Procedure should be viewed with a copy of the CCTV Code of Practice document issued by the Information Commissioner's Office (ICO).

The following documents together with this Procedure document make up the full CCTV Compliance Register for Brockenhurst College:

- Data Protection Policy for Brockenhurst College
- CCTV Procedure for Brockenhurst College
- CCTV Code of Practice
- CCTV Operational Requirements Manual

This CCTV system is owned by the College.

OBJECTIVES OF THE CCTV SYSTEM

- To protect the College buildings and their assets
- To increase personal safety and reduce the fear of crime
- To support the Police in a bid to deter and detect crime
- To assist in identifying, apprehending and prosecuting offenders
- To protect members of the public and private property
- To assist in managing the College

FORMS RELATING TO THIS PROCEDURE

Form Description	Ref. Number
College Evidence Access Release Form	CEAR1
Data Subject Access Request Form	DSAR1
Monitoring Staff Declaration Form	MSD1

These forms can be obtained from the IT Services or Estates department.

STATEMENT OF INTENT

The Colleges CCTV System will be registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.

The College will treat the system and all information, documents and recordings obtained and used as data which is protected by the Act.

Cameras will be used to monitor activities within the College and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well being of the College, Staff, Students and Visitors.

No static cameras are focussed on private homes, gardens and other areas of private property.

Unless an immediate response to events is required, staff managing the system must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained using the College's forms for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recorded images will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Recorded images will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect all incidents taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner, have been placed at all access routes to areas covered by the College CCTV system. For information relating to the operation, maintenance and general day-to-day running of the colleges CCTV system please email CCTVController@brock.ac.uk.

OPERATION OF THE SYSTEM

The System will be administered and managed by the IT Services Manager or designated Deputy, in accordance with the principles and objectives of this Procedure.

Responsibility for the day-to-day monitoring of the system lies with the Estates department.

Responsibility for the management and maintenance of the system lies with the IT Services Manager or designated Deputy and the IT Services staff.

The Control Rooms will only be accessed by IT Services and Estates department employees.

The CCTV system will be operated 24 hours each day, every day of the year.

Images are retained for a maximum of 30 days, once the 30th day has been reached the recordings are overwritten.

COMPLAINTS

Any complaints about the College's CCTV system should be addressed the Director of Finance and Customer Services.

Complaints will be investigated and issues arising from the investigation will be addressed accordingly and the relevant remedial action taken.

ACCESS BY THE DATA SUBJECT

The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including that obtained by CCTV. Requests for Data Subject Access should be made on the application form available from the IT Services or Estates department. Form Reference: DSAR1.

NOTES


it
Brockenhurst
College
IT Services

BROCKENHURST COLLEGE
Lyndhurst Road, Brockenhurst, Hampshire SO42 7ZE
Telephone: 01590 625500 www.brock.ac.uk