ACCEPTABLE USE POLICY SUMMARY

The following document is a guide to what behaviour is deemed acceptable when using the schools ICT resources, and is provided to help students use these resources in a safe and secure way. Please ensure you have read through the following document and when you are happy that your child understands the agreement please sign the form below and hand in to your child's form tutor.

Below is a summary of the main issues to discuss with your child:

- Whilst access to the internet is provided to support lessons this must be used responsibly. All internet activity is closely monitored and should not be used for any of the following:
  - Online Chat/Messaging
  - Giving out personal information
  - Downloading and installing software or viruses

  Any of the above activity, in addition to anything else which is deemed an unacceptable use of the school computers, will be reported to the relevant member of staff and dealt with appropriately.
- Students are not, under any circumstance, allowed to play online games during lesson time.
- Email access is provided for use both within and outside the college but must be used appropriately and for school work only. Always ensure you are polite, use appropriate language and never reveal any personal information about yourself. Student email within the school is not considered to be private and is actively monitored. Inappropriate use of the system will be passed on to the relevant staff member.
- Never upload photos or videos taken within school grounds, or containing any members of staff, to online social networking and file sharing websites (such as Facebook, YouTube etc.)
- Never share your password with anyone, or ask anyone else for their password. If you forget your password or think someone may know it speak to a member of the IT department immediately
- Never attempt to access files or programmes for which you have not been granted access.
- If mobile phones are to be brought into school they must be switched off and placed in lockers during the school day.

Student Name: _____

Student Form: _____

Student Signature: _____

Parent / Carer Signature: _____

Date: _____

This form needs to be handed in to your child's form tutor before they can access the schools ICT facilities.

If you have any further questions regarding this Acceptable Use Policy please feel free to email ITSupport@brockington.leics.sch.uk

ACCEPTABLE USE POLICY

WHY HAVE AN ACCEPTABLE USE POLICY?

An Acceptable Use Policy is about ensuring that you, as a student at Brockington College can use the internet, email and other technologies available at the school in a safe and secure way. The policy also extends to out of school facilities e.g. equipment; printers and consumables; Internet and email; managed learning environments and websites.

An Acceptable Use Policy also seeks to ensure that you are not knowingly subject to **identity theft** and therefore fraud. Also that you **avoid cyber-bullying** and just as importantly, you **do not become a victim of abuse**. We have also banned certain proxy sites as well as anonymous proxy sites, because they put the school network at risk.
Help us, to help you, keep safe.

Brockington College recognises the importance of ICT in education and the needs of students to access the computing facilities available within the School. The school aims to make the ICT facilities it has available for students to use for their studies both in and out of lesson times. To allow for this Brockington College requires all students to sign a copy of the Acceptable Usage Policy **before** they receive their username and password.

Listed below are the terms of this agreement. All students at Brockington College are expected to use the ICT facilities in accordance with these terms. Violation of terms outlined in this document may lead to loss of access and/or disciplinary action, which will be taken in accordance with the Behaviour Management Policy of the School.

Access to the School's ICT facilities will only take place once this document has been signed by **BOTH** the **student** and **parent/carer**.

SECTION 1: EQUIPMENT

1.1 Vandalism

Vandalism is defined as **any action** that harms or damages any equipment or data that is part of the School's ICT facilities and is deemed completely unacceptable. Such vandalism is covered by the Computer Misuse Act 1990 (see Glossary). This includes, but is not limited to:

- Deliberate damage to computer hardware such as monitors, base units, printers, keyboards, mice or other hardware.
- Change or removal of software
- Unauthorised configuration changes
- Creating or uploading computer viruses
- Deliberate deletion of files.

Such actions reduce the availability and reliability of computer equipment; and puts at risk other users' data. In addition, these actions lead to an increase in repairs of the ICT facilities, which impacts upon every students' ability to use the ICT facilities. The other result of vandalism is that it incurs costs, which reduce the funds available to improve the ICT facilities the school has.

1.2 Use of Removable Storage Media

Brockington College accepts the fact that you may wish to transfer school work done at home to school using a flash memory device or a CD disk. However, Brockington College cannot guarantee that your work will be able to be transferred properly using these. We therefore encourage you to use the "My Documents and Shared Files" section of the website, or email, when transferring work between home and school.

1.3 Printers and Consumables

Printers are provided across the Brockington College for use by students. Please use the printers sparingly and for educational purposes only. Take the time to check the layout and proof read your work using the 'Print Preview' facility before printing.

All printer use is recorded and monitored and therefore if you deliberately use the printer for non-educational or offensive material you will be subject to the behaviour management measures of the school which includes the following:

- Consequences
- A warning
- Email and/or Internet facilities removed
- Letter home to parents
- Loss of access to the print facilities available within the School
- Report to the School Governors
- Report to appropriate external agencies like the Police

1.3.1 Printer Accounting

A printer accounting system is in operation across Brockington College. This assists in monitoring printer usage and reducing wastage of consumables.

You will be given 70 credits per term. If you require more than this, you can purchase additional credits at a cost of 50p per 50 credits (paid for at the cabin).

Consumption

Type	Credits
Black & White	1 Credit
Colour	10 Credits

Initial Allocation

Users	Credits
Students	70 Credits

Pricing

Users	Price
Students	50p per 50 credits

1.4 Data Security and Retention

All data stored on the Brockington College network is backed up daily and backups are stored for up to at least two weeks. If you should accidentally delete a files or files in your folder or shared area, please inform a member of the IT department *immediately* so that it can be recovered. Generally, it is not possible to recover files that were deleted more than 2 weeks previously.

SECTION 2: INTERNET & EMAIL

2.1 Content Filtering

Brockington College provides internet filtering, designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. If you come across any inappropriate website or content whilst using the ICT equipment, **you must report it to a member of staff *immediately.***

The use of Internet and email is a privilege and inappropriate use will result in that privilege being withdrawn.

2.2 Acceptable use of the Internet

All Internet access is logged and actively monitored and details are stored for up to, at least 2 months and usage reports can and will be provided to any member of staff upon request.

Use of the Internet should be in accordance with the following guidelines:

- Only access suitable material – the Internet is not be used to download, send, print, display or transmit material that would cause offence or break the law.
- Do not access Internet Chat sites. Remember you could be placing yourself at risk.
- Never give or enter your personal information on a website, especially your home address, your mobile number or passwords.
- Online games websites should, under no circumstance, be accessed during lesson times and may only be used during supervised lunch-time clubs.
- Do not download or install software from the Internet, as it is considered to be vandalism of the School's ICT facilities.
- Do not use the Internet to order goods or services from on-line, e-commerce or auction sites.
- Do not subscribe to any newsletter, catalogue or other form of correspondence via the Internet.
- Do not print pages directly from a website. Web pages are often not properly formatted for printing and this may cause a lot of waste. If you wish to use content from websites, consider using the copy and paste facility to move it into another application, copyright permitting.

2.3 Email

You will be provided with an email address by the School, and the expectation is that you will use this facility for legitimate educational and research activity.

During lessons e-mail should only be used when instructed by your teacher, and for educational purposes only. E-mail can also be accessed during your own social time but please carefully follow the guidelines laid out below.

You are expected to use email in a responsible manner. The sending or receiving of messages which contain any material that is of a sexist, racist, unethical, illegal or likely to cause offence should not take place.

Remember when sending an email to:

- **Be Polite** - never send or encourage others to send abusive messages.
- **Use appropriate language** - remember that you are a representative of the School on a global public system. What you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language.
- **Do not reveal any personal information about yourself or anyone else**, especially home addresses, personal telephone numbers, usernames or passwords. Remember that electronic mail is not guaranteed to be private.
- **Consider the file size of an attachment,** files exceeding 5MByte in size are generally considered to be excessively large and you should consider using other methods to transfer such files.
- **Do not download or open file attachments unless you are certain of both their content and origin**. File attachments may contain viruses that may cause loss of data or damage to the
  School network.

2.4 Cyber-Bullying

In the event of a cyber-bullying incident the same procedures will be followed as for all other incidents of poor behaviour (see Behaviour Policy).

In all cases details of the incident and action taken will be recorded.

The prime concern will be the protection of the victim. Action will continue until the issue is satisfactorily resolved and the bullying ceases. Parents /carers will be kept informed of action taken. The action will be reviewed and modified in light of circumstances and whether the bullying continues.

Strategies to support the victims will involve staff and students. A variety of approaches will be used to achieve this.

If it is a serious incident exclusion will be considered.

Bullying incidents will be logged and monitored regularly.

A Governor will be nominated to have responsibility for maintaining an overview of behavioural and bullying issues.

SECTION 3: EXTERNAL SERVICES

3.1 Web-Email

Web email provides remote access to your email account from home or anywhere with an Internet connection. Use of this service is subject to the following guidelines. Use of the facility is closely and actively monitored and any abuse or misuse will result in the facility being withdrawn and/or other disciplinary action being taken against you.

- Web-email is provided for use of Brockington College staff and students only. Access by any other person is not allowed.
- Never reveal your password to anyone.

- Remember to treat file attachments with caution. File attachments may contain viruses that may cause loss of data or damage to the computer from which you are working. Do not download or open file attachments unless you are certain of both their content and origin. Brockington College accepts no responsibility for damage caused to any external equipment or software, as a result, of using the web-email service.

3.2 Managed Learning Environment Software

The 'It's Learning' Virtual Learning Environment (VLE) provides a web-based portal allowing users access to personalised learning resources and lesson materials. Use of this service should only be in accordance with instructions from your subject tutor and in accordance with the following guidelines:

- The VLE is provided for use of Brockington College staff and students only. Access by any other party is strictly prohibited.
- Never reveal your password to anyone or attempt to access the service using another student's login details.
- The 'It's Learning' remote access service is provided by itslearning.com and Brockington College can make no guarantees as to service availability or quality.

3.3 Social Networking and File Sharing Sites (Facebook, Youtube etc.)

Whilst accessing social networking sites (Facebook etc.) is restricted within the school environment we appreciate the large number of students who will be using this in free-time outside of school. Please bear in mind that including any details about the school you attend on your profile not only introduces a very serious safety risk it also makes you a representative of the school. As such we strongly recommend you do not post any such details to any social networking sites.
Any behaviour which could bring the school into disrepute may result in computer access being restricted and further disciplinary action being taken.

The uploading of any photos or videos taken within schools grounds or containing any member of staff is not allowed under any circumstance.

SECTION 4: PRIVACY

4.1 Passwords

- **Never** share your password with anyone else or ask others for their password.
- When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you, such as your name or address. Generally, longer passwords are better than short passwords.
- If you forget your password, inform a member of the IT department immediately.
- If you believe that someone else may have discovered your password, then **change it immediately** and inform a member of staff.

4.2 Security

- **Never** attempt to access files or programs to which you have not been granted access to. Attempting to bypass security barriers may breach data protection regulations and such attempts will be considered as hack attacks and will be subject to disciplinary action.
- You should report any security concerns immediately to a member of staff
- If you are identified as a security risk to the School's ICT facilities you will be denied access to the systems and be subject to disciplinary action.

4.3 Storage and Safe Transfer of Personal Data

- Brockington College holds information on all pupils and in doing so, we must follow the requirements or the Data Protection Act 1998 (see Glossary). This means that data held about pupils can only be used for specific purposes and therefore all data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Brockington College will seek to ensure that personal data sent over the internet will be encrypted or otherwise secured.

SECTION 5: SERVICE

Whilst every effort is made to ensure that the systems, both hardware and software are working correctly, the school will not be responsible for any damages or loss incurred as a result of system faults, malfunctions or routine maintenance. These damages include loss of data as a result of delay, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Use of any information obtained via the School's ICT system is at your own risk. Brockington College specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

SECTION 6: MOBILE TECHNOLOGIES

6.1 Acceptable Use of Mobile Devices

For reasons of safety and security pupils should not use their mobile phone or any other technology in a manner that is likely to bring the school into disrepute or risk the welfare of a child or young person.

The development of mobile technology is such that mobile phones and other similar devices connected to mobile networks have enhanced features which include: picture messaging; mobile access to the Internet; entertainment in the form of video streaming and downloadable video clips from films, sporting events, music and games etc. The capabilities of 3G mobile phones also means that adults working within the school environment may be sent inappropriate images or videos, or be encouraged to send back images or video of themselves using integrated cameras.

If you are sent inappropriate material e.g. images, videos etc report it **immediately to a member of staff** within the school.

6.2 Mobile Phones

If mobile telephones are brought into school they must be switched off and kept in lockers at all times to ensure they cause no disruption to teaching and learning. The school, it's staff and governing body takes no responsibility for loss or theft of any mobile phones which students choose to bring into school.

6.3 Tablet PCs and Notebooks

As a college we appreciate students have increasing access to personal mobile devices which can be beneficial to education. As a college we strongly advise all students to leave any high value devices at home as correct and appropriate ICT facilities will be provided to students whenever necessary. Any devices which are brought into school must be used appropriately and responsibly, and only when specific permission is agreed with the class teacher. The school, it's staff and governing body takes no responsibility for loss or theft of any Tablet PC's and Notebooks which students choose to bring into school.

GLOSSARY

Computer Misuse Act (1990)

The Computer Misuse Act makes it an offence for anyone to have:-

- Unauthorised access to computer material e.g. if you find or guess a fellow pupil's password and use it.
- Unauthorised access to deliberately commit an unlawful act e.g. if you guess a fellow pupil's password and access their learning account without permission
- Unauthorised changes to computer material e.g. if you change the desk-top set up on your computer or introduce a virus deliberately to the school's network system.

Data Protection Act (1998)

The Data Protection Act ensures that information held about you is used for specific purposes only. These rules apply to everyone in the school, including teaching staff, support staff, volunteers and governors.

The Act covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data held about individuals in the school. The Act not only applies to paper files it also applies to electronic files.

The principles of the Act state that data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Kept no longer than necessary
- Processed in accordance with data subject's rights
- Secure
- Not transferred to other countries without adequate provision.

RIPA – Regulation of Investigatory Powers Act (2000)

If a request for authorised access is made to the school they will provide the appropriate access to your ICT records and files. The Act legislates for using methods of surveillance and information gathering to help the prevention of crime, including terrorism. RIPA makes provision for:

- the interception of communications
- the acquisition and disclosure of data relating to communications
- the carrying out of surveillance
- the use of covert human intelligence sources
- access to electronic data protected by encryption or passwords

If a request for authorised access is made to the school, we will provide the appropriate access to your ICT records and files.