CASTLE ROCK HIGH SCHOOL

CASTLE
ROCK
HIGH SCHOOL

# ICT Acceptable Use Policy for Students

Updated March 2019

**Why have an Acceptable Use Policy?**

An Acceptable Use Policy is about ensuring that you, as a pupil at Castle Rock High School 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 cyberbullying and just as importantly, you do not become a victim of abuse. We have also restricted access to the majority of proxy sites as well as anonymous proxy sites, because they put the school network at risk.

*Help us, to help you, keep safe.*

Castle Rock High School 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 Castle Rock High School requires all students to accept the terms of the Acceptable Usage Policy before they receive their username and password.

Listed below are the terms of this agreement. All students at Castle Rock High School 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.

Please read this document carefully before indicating your acceptance of the Policy. Access to the School's ICT facilities will only be allowed one you have accepted the terms of the policy.

## 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. 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, workstations, notebooks, printers, keyboards, mice or other hardware.
- Moving, unplugging or otherwise tampering with the school's configuration of hardware devices and associated cabling.
- Change or removal of software.
- Unauthorised configuration changes.
- Creation or uploading of 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

Castle Rock High School accepts the fact that you may wish to transfer school work done at home to school using a USB flash memory device or a CD/DVD disk.

However, Castle Rock High School cannot guarantee that your work will be able to be transferred properly using these.

We therefore encourage you to use your personal Office 365 OneDrive or email when transferring work between home and school. Such systems are inherently more reliable and secure than physical storage devices.

## 1.3 Printers and Consumables

The printing system in place at Castle Rock High School aims to encourage fair and efficient use of the printing facilities. The printing facilities are made available to students solely for the printing of schoolwork and homework. Printing of personal documents is not allowed.

Students are allocated a £1.00 printing allowance on the first day of every month. Unused purse balances cannot be carried over to the next month.

The balance of your printing allowance can be checked by examining the PaperCut app, which is displayed on the Windows desktop for all student users.

If a student is deemed to have misused their printing privileges by printing inappropriate or non-schoolwork related content, their printing account may be restricted or disabled.

### 1.3.1 Printing Costs

Printers that are available for student use each have an associated cost per page. The cost for printing to mono printers

is £0.01 per page.

The cost for printing to colour printers is £0.05 per page.

### 1.3.2 Printing Efficiently

As the school's printing budgets are limited, it is very important that students follow certain basic steps when printing, to avoid wasting money:

- **Think** – do you really need to print this document?
- **Check** – thoroughly proof read and run a spell-check on your document before deciding to print it. Ensure that your name is on the document somewhere.
- **Preview** – use the Print Preview feature to see how your document will look when printed. Now is the time to delete blank pages, adjust positioning of images, etc.

- **Print** – Make sure that you select the correct printer from the list of available printers. Does your document need to be in colour? Mono printing is much cheaper for the school and costs you less credits.
- **Collect** – remember to collect your work from the printer – if there is a problem with the printer, ask your teacher to call the ICT Dept.

Standard laser printers are denoted by 'PRN' prefixing the printer name, followed by the print driver designation (Mono or Colour) and the physical location - e.g. "PRN-Mono-Humanities".

Multi-Function printers are denoted by the prefix of 'MFD', again followed by Mono or Colour, and the device's physical location.

All print devices in the school are capable of double-sided (duplex) printing, where both sides of the page are printed on. Students are encouraged to make use of this functionality whenever possible, as it saves the school a significant amount of money when used.

*Double-sided (duplex) printing is now automatically selected as the default software option when sending a document to print. Please be aware of this and remember to choose Single-sided printing if you do not require a double printout.*

### 1.3.3 Alternatives to Printing

All students are strongly encouraged to use the alternative methods to printing, that are available to them:

- **Office 365 OneDrive** – every student has their own personal OneDrive cloud storage account. Documents uploaded to OneDrive are secure stored and are available anywhere via the internet.

Please do not hesitate to contact a member of the ICT Department if you require any assistance with the above.

### 1.4 Data Security and Retention

All data stored on the Castle Rock High School network is backed up daily and backups are stored for an indefinite period.

If you should accidentally delete a file or files in your folder or a shared area, please inform the Network Manager immediately so that it can be recovered. Generally, it is not possible to recover files that were created and deleted on the same day prior to the daily overnight backup.

## 2. Internet and Email

### 2.1 Content Filtering

Castle Rock High School provides advanced layers of 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 or the Network Manager 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 records are stored for up to at least 3 months. 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 to be used to download, send, print, display or transmit material that would cause offence or break the law.
- Do not attempt to circumvent the school's filtering systems by accessing proxy websites, anonymizers or remote access services.
- Do not attempt to 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.
- Do not access online gaming sites in lesson times. Remember that your use of the Internet is predominantly for educational purposes only.
- Do not download or install software from the Internet, as it is considered to be vandalism/modification of the School's ICT facilities.
- Do not use the Internet to order goods or services from online, ecommerce 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.

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, or illegal nature, or likely to cause offence, should not take place.

All email messages are monitored by the Castle Rock IT team and are subject to profanity checking and other keyword searches.

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 25 MegaBytes in size are generally considered to be

excessively large and you should consider using other methods to transfer such files (e.g. OneDrive).

- 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.

## 3. External Services

Castle Rock High School provides a number of services that are accessible externally, using any computer with an Internet connection. You should use this facility only for educational activities only and in accordance with the following guidelines.

### 3.1 Webmail (Office 365 Outlook)

Webmail 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.

- Webmail is provided for use of Castle Rock High School 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. Castle Rock High School accepts no responsibility for damage caused to any external equipment or software, as a result, of using the webmail service.

## 4. Privacy and Data Protection

### 4.1 Passwords

- Never share your password with anyone else or ask others for their password.
- A password policy is enforced by the computer system. Passwords must be a minimum of 7 characters and contain at least three of the following;
  - Upper case letters
  - Lower case letters
  - Numerical characters (0 through 9)
  - Special characters i.e. !@$£&
- Passwords cannot contain the user’s login name or three or more consecutive characters from their first or last names.
- When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you and be easily guessed. Generally, longer passwords are better than short passwords.
- If you forget your password, inform the Network Manager or ICT Technician 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 hacking 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

- Castle Rock High School 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.
- Castle Rock High School will seek to ensure that personal data sent over the internet will be encrypted or otherwise secured.

## 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. Castle Rock High School specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

## 6. Mobile Technologies

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.

In order to reduce the opportunity for those behaviours that could possibly cause upset, all students that choose to bring a mobile device onto school property must hand it into the school office prior to morning registration and the beginning of timetabled school hours. The device can then be collected at the end of the day. Emergency access to the mobile device during timetabled school hours will be supervised by members of staff. Any student found to be in possession of a mobile device during timetabled school hours will be subject to immediate confiscation of the device, which must then be collected by prior arrangement by the student's parent or carer.

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

## Glossary

### Computer Misuse Act

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 and fellow pupil's password and access their learning account without permission
- Unauthorised changes to computer material e.g. if you change the desktop 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 2002

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.

**By accepting the terms of this policy, you agree to the following:**

I understand and agree to the provisions and conditions of this agreement. I understand that any disobedience to the above provisions may result in disciplinary action and the removal of my privileges to access ICT facilities. I also agree to report any misuse of the system to a staff member and I understand that misuse may come in many forms but may be viewed as any messages sent or received that indicate or suggest pornography, unethical or illegal activities, racism, sexism inappropriate language, or any act likely to cause offence.