



**Wingfield Academy**

# **ICT Acceptable Usage Policy**

Reviewed By  
Jason Wicks  
ICT Technician

Reviewed  
September 2019

Review Date  
September 2020

Governor Ratification Date  
October 2020

## Staff and Visitors

Academy networked resources, including Bromcom and Google Suite, are intended for educational purposes, and may only be used for legal activities consistent with the rules of the Academy. If you make a comment about the Academy or others you must state that it is an expression of your own personal view.

All users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the user to take all reasonable steps to ensure compliance with the conditions set out in this policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of ICT resources to the ICT Support Team or SLT.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to the withdrawal of the user's access; monitoring and/or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the Academy's ethos and Code of Conduct.

### General

- I will only use ICT and any related technologies for professional purposes or for uses deemed 'reasonable' by the Academy, Governing Body or Line Manager.
- I will support and promote the Acceptable Use, e-Safety and Data Protection policies and help students and young people and adults to be safe and responsible in their use of ICT and related technologies.
- I understand that any users identified as a security risk will be denied access to the network.
- I will comply with ICT security policies and not disclose or share any passwords provided to me by the Academy or other related educational settings. My Wingfield account is for use by me only, I will be held responsible for activity carried out using it.
  - If I think my password has been compromised I will change it immediately and contact the ICT Support Team.
  - I understand that staff laptops are only to be used by those employed by the Academy, visitors and students must not be allowed access unless unavoidable and under direct supervision.
  - If I find an unattended, unlocked, machine logged on under another users username I will not continue using the machine – I will either lock it or log it out before logging in as myself.
  - I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
  - I will not install any hardware or software without prior permission from the ICT Support Team.
  - I understand that all my use of the Internet, email, and other technologies are not private and are monitored and logged. These can be made available, on request, to SLT, the Governing Body or Line Manager.
  - I will ensure that all electronic communications are compatible with my professional role and will only use my WingfieldAcademy.org email account for any work related business.
  - If a security problem is identified I will not demonstrate this problem to other users but will report it immediately to the ICT Support Team.

## **Data Protection and Copyright**

- I will abide by the Academy GDPR policy this includes:
  - Not revealing any personal information e.g. home address, telephone number, social networking details of any other users to any unauthorised person. I will not reveal any of my personal information to students.
  - Ensuring that personal data is kept secure and is used appropriately, whether in Academy, taken off site or accessed remotely. Personal data can only be taken off site or accessed remotely when authorised by the Academy, Governing Body or Line Manager/Supervisor.
  - Ensuring any personal data taken off site (either electronically or on a physical storage device) is encrypted or otherwise secured.
- I will respect copyright and intellectual property law.
- Images of children and young people and/or staff will only be taken, stored and used for professional purposes in-line with any policy and with prior written consent of a parent, school or Line Manager/Supervisor.
- I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the Academy Leadership Team.

## **E-Safety**

- I will not create, browse, download, upload or distribute any material that is illegal, could cause offence, inconvenience, needless anxiety, incite hatred, or brings the Academy in to disrepute. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
  - I will report any accidental access, receipt of inappropriate materials or filtering breaches/unsuitable websites to the ICT Support Team.
- I will not accept invitations from children and young people to add me as a friend to their social networking pages, nor will I invite them to be friends on mine.
- I will also be careful with who has access to my pages through friends, and friends of friends. Especially with those connected with my professional duties, such as school parents and their children.

I have read and fully understand the terms and conditions of the policy agreement and I agree to abide by the conditions.

## **Students**

All students must follow the conditions described in this policy when using academy ICT networked resources including internet access, the School Virtual Learning Environment (VLE) both in and outside of the Academy.

Breaking these conditions may lead to:-

- Withdrawal of the student's access.
- Close monitoring of the student's network activity.
- In extreme cases, criminal prosecution.

Students will be provided with guidance by staff in the use of the resources available through the school's network. School staff will regularly monitor the network to make sure that it is being used responsibly. The school will not be responsible for any loss of data as a result of the system or students mistakes in using the system. Use of any information obtained via the network is at the student's own risk.

It is the personal responsibility of every student to take all reasonable steps to make sure they follow the conditions set out in this policy. Students must also accept personal responsibility for reporting any misuse of the network to the ICT Support Team.

Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the Academy's ethos and Code of Conduct.

## **General**

- It is my responsibility to respect and follow all of these conditions which will help to keep me and others safe while using ICT.
- I will not share my username or password with anyone.
- I will save my work and log off properly after I have finished with the computer.
- I will ensure that my password is secure and I will not share this password with anyone.
- I will not access or create any material that may cause upset to others.
- If I am unsure about opening or downloading any attachments or contents of an email, I will seek advice from the ICT Support Team.
- I will keep my personal information safe from other people.
- I will not access trespass in to other user's files and folders without permission.
- I will not use portable media (like memory sticks) on the network without gaining permission from my teacher.
- I will treat other people and ICT equipment with care and respect.
- I will not reveal any personal information e.g. home address, telephone number about myself or other users over the network.

## **Data Protection and Copyright**

- I will only take, store and use images of children, young people and/or staff for an agreed project or purpose.
- I will only use images outside the network if I have permission from the people in the image and a member of staff.
- I will only use images that have been approved by a member of staff.
- I acknowledge that my teachers and support staff have read access to my documents and can access them for the purpose of marking work or investigating suspected issues.

## **E-Safety**

- I will not browse or download anything illegal and forward or share any material that could cause upset to anyone.
- If I do come across any such material I will report it immediately to a member of staff.
- I will not attempt to circumvent the security and filtering system.
- I will not attempt to access any unsupervised/unauthorised chatrooms or areas.
- I will only communicate with others online sensibly.
- I will not send or encourage others to send abusive messages through e-mail or other services.
- I will make sure that any online or offline activity will not cause the school/centre, staff and any other user, distress or embarrassment.
- I know that all use of the network is monitored if abuse is suspected.

I have read and fully understand the terms and conditions of the policy agreement and I agree to abide by the conditions.

## **Internet Safety Policy**

To ensure a safe internet experience for all staff and students all access must be filtered to prevent access to unsuitable material and the network secured against external threats. To accomplish this Academy uses multiple layers of security.

**In Class-** All computers accessed by students have monitoring software installed (Impero), this provides both active and passive protection. Any website or other content that the software considers inappropriate will be automatically blocked; this includes material brought in on USB sticks or other removable storage devices. Any infractions are brought to the attention of the teacher, along with any minor issues the software spots. A screenshot is automatically taken which can be used as evidence. The teacher can see every application and website in use by his/her class in real-time.

**Network-** All access to the web is via the Academy's Fortinet firewall; this provides block-list, content analysis and virus scanning of all web traffic. These definitions are updated daily to ensure the Academy is protected against the latest threats.

With the exception of internet banking and other financial services, all traffic will be analysed; this includes traffic to secure web servers (HTTPS). If the content of the page is deemed unsuitable then access is blocked. All access is logged; these logs are kept for one year.

All servers and workstations are protected by anti-virus software. All wireless access is protected by WPA2 encryption with a maximum length randomly generated passphrase.

## **Internet Connection**

Our internet connection is provided through Virgin Media. Firewall rules effectively isolate the school network, only allowing access to central servers. Direct access to the Internet is blocked; all web access must go through the Fortinet firewall ensuring a base level of filtering to all users.

## **E-Mail**

All students and staff have an e-Mail account. Students are restricted to send/receive e-mail to/from to a pre-allowed list. E-mail accounts are provided for education use only and accounts can be accessed by staff with SLT approval if abuse of the resource is suspected. All e-mail is filtered for abusive content before being delivered.

Staff are supplied with an e-mail account to use for all educational business. This is to minimise the risk of receiving unsolicited or malicious e-mail and avoids the risk of personal profile information being revealed to anyone else. This account should not be used for personal use.