ACADEMY ICT ACCEPTABLE USE POLICY (Staff & Volunteers)

Formulation date: May 2013.
Revised September 2015
Revised September 2019

Full Local Governor Board: September 2019

Next review date: September 2021

ICT Acceptable Use Policy (Staff and Volunteers)
(Revised Sept 2019)

Why have an Acceptable Use Policy?

An Acceptable Use Policy is about ensuring that you, as a member of staff/volunteer at *Newbridge High School (part of Apollo Partnership Trust)* can use the internet, email and other technologies available at the Academy in a safe and secure way.

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 sites which put the Academy network at risk.
Help us, to help you, keep safe.

Newbridge High School strongly believes in the educational value of ICT and recognises its potential to enable staff and volunteers in delivering and supporting the curriculum. *Newbridge High School* also believes that it has a responsibility to educate its students; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and other related technologies. To this end the expectation of *Newbridge High School* is that both staff and volunteers will play an active role in implementing Academy and departmental internet safety polices through effective classroom practice.

Newbridge High School recognises that for staff and volunteers to effectively deliver and support the curriculum they must be able to make use of the ICT facilities of the Academy and have the opportunity to expand and develop the teaching material and otherwise associated with their work. However, *Newbridge High School* expects that both staff and volunteers will at all times maintain an appropriate level of professional conduct in their own use of the School's ICT facilities.

Listed below are the terms of this agreement. Staff are expected to use the ICT facilities of the Academy in accordance with these terms. Violation of these terms is likely to result in disciplinary action in accordance with The Trusts Disciplinary Procedures for Employees.

Please read this document carefully and sign and date the accompanying to indicate your acceptance of the terms herein.

1. Equipment

1.1 Academy Computers

All computers and associated equipment are the property of *Newbridge High School* and must be used in accordance with this policy which adheres to the Computer Misuse Act 1990 and the Data Protection Act 2018 (see Glossary). The Academy and the Network Manager assumes responsibility of maintenance of all hardware and software. Mis-use of equipment includes, but is not limited to the following:

- Modification or removal of software
- Unauthorised configuration changes
- Creation or uploading or computer viruses or other malware
- Deliberate deletion of files.
- Creation or uploading of unauthorised software

Any of these actions reduces the availability and reliability of computer equipment, puts other users' data at risk and increases downtime caused by repairs, thus delaying other essential work such as upgrades or enhancements.

1.2 Laptop Computers

Laptop computers are issued to all teaching staff and support staff as required. Laptops remain the property of *Newbridge High School* all times, and their usage is subject to the following guidelines:

- The equipment remains the property of *Newbridge High School* at all times and must be returned to the Academy at the end of the lease agreement or contractual period.
- Maintenance of the equipment is the responsibility of the School. All maintenance issues must be referred to *The ICT Department*, through the usual channels.
- All installed software MUST be covered by a valid license agreement held by *Newbridge High School*.
- All software installation MUST be carried out by *The ICT Department* in accordance with the relevant license agreements.
- No software should be removed, uninstalled or disabled under any circumstances. Any software problems should be reported through the usual support channels.
- Antivirus software must be updated regularly. For laptop computers, it will be necessary to connect them to the Academy network to update the antivirus software. This should be done at least weekly.
- The user of the equipment is responsible for all personal files and data stored on the equipment. Backup of the data is the responsibility of the user. It is strongly recommended that all data is regularly backed upn to the *Academy* network.
- It is not recommended that removable storage is used. Staff/Volunteers should liaise with the Network Manager for guidance on how this can be safely managed.
- It is recommended that the school's facility to transfer files is used.
- The user of the equipment must not encrypt <u>any</u> data or password protect any files so as to ensure future usage of the equipment.
- *Newbridge High School* cannot be held responsible for loss of data in the event of either a hardware or software failure or user error.
- From time to time, it may be necessary for *The ICT Department* to perform software updates and maintenance for which the equipment must be made available in Academy when reasonably requested. **This will usually take place during a half-term.**

1.3 Printers and Consumables

Printers are provided across the Academy for educational or work-related use only. All printer usage can be monitored and recorded.

- Always print on a black & white printer unless colour is absolutely essential

- Proof-read your document on-screen and use the 'Print-Preview' facility to check the layout before printing.
- Do not print unnecessarily or waste ink or paper.
- Avoid printing directly from the Internet where possible. Internet pages are often not suitably formatted for printing and may cause wastage of paper and other consumables.
- Do not print any personal data using the school facilities, unless express permission has been given and any charges paid for.

1.3.1 Printer Accounting

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

1. Departments are charged for printer credits which are consumed when documents are printed.

Consumption

Type (A4 single sided)	Cost
Black & White	*4 pence*
Colour	*8 pence*

1.5 Data Security and Retention

All data stored on the *Newbridge High School* network is backed up daily and backups may be stored in accordance with Apollo Partnership Trust's Retention Policy. If you should accidentally delete a files or files in your folder or shared area, please inform *The ICT Department* immediately so that it can be recovered.

2. Internet and Email

2.1 Content Filtering

Newbridge High School 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 discover any websites containing inappropriate or offensive content, please report these to *The ICT Department* so that they can be filtered.

2.2 Acceptable use of the Internet

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

- Transmission of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws
- Only access suitable material – Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.

- Respect the work and ownership rights of people outside the School. This includes abiding by copyright laws.

- **Do not access Internet chat sites**. These represent a significant security threat to the School's network.

- **The use of online gaming sites is strictly prohibited**. These consume valuable network resources that may adversely affect the performance of the system.

- Do not print out pages directly from a website. Web pages are often not suitably formatted for printing and this may cause significant wastage of paper. If you wish to use content from websites, consider using the copy and paste facility to move it into another application, copyright permitting.

- Do not attempt to download or install software from the Internet. *The Network Manager* assumes responsibility for all software upgrades and installations.

- Staff are reminded that ALL Internet access is logged and actively monitored and traceable.

- **You are STRONGLY advised to be very careful whilst using social media sites such as Facebook, Twitter, Tumblr etc.** Anyone found to be referring to professional matters linked to the Academy on these sites will be subject to Disciplinary Procedures. You are not permitted to allow individual students at this Academy or ex-students up to the age of 18, to be 'friends' on any of these social media sites.

2.3 Email

Staff are provided with an email address by the School. This may be used for *any legitimate educational or work-related activity*. Staff should use the email in accordance with the following guidelines and are reminded that the Academy retains the right to monitor email communications at any time if this is deemed necessary.

The sending or receiving of messages which contain any inappropriate material is strictly forbidden. This material includes, but it not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, or any other use which may be likely to cause offence. Disciplinary action will be taken in all cases.

- Messages relating to, or in support of any illegal activities may be reported to the authorities.

- Whilst it is possible to attach files to an email message, staff are advised that email is not generally suited to transferring large files. Whilst there are no hard and fast rules regarding file sizes that can be attached to an email message, files exceeding approximately 5MByte in size are generally considered to be excessively large and staff 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 or other forms of malware that may cause loss of data or damage to the Academy network.

- Staff should not send personally identifiable information by email, as it is not a secure medium.

3. External Services

Newbridge High School provides a number of services that are accessible externally, using any computer with an Internet connection. These should be used strictly for educational or work-related activities only and in accordance with the following guidelines.

3.1 Remote Server

The remote Server provides remote access to files and resources stored on the Academy network, via the Internet. This service is provided to staff to enable access to school systems from off-site.

The use of *Remote Server* is subject to the following guidelines. Use of the service is closely and actively monitored.

- *Remote Server* is provided for use of *Newbridge High School* staff only. Use by students or any other party is strictly prohibited.
- By using the Remote Server you signify that you are an employee of *Newbridge High School* and that you have been authorised to use the system by the relevant Academy authority.
- Observe security guidelines at all times. Never reveal your password to anyone
- All files must be virus checked before being transferred to our system

Staff using their own facilities at home should abide by the principles and practices on safe and secure internet practice and use of email, as set out in this Policy.

3.2 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. Staff should use email in accordance with the following guidelines and are reminded that the *Academy* retains the right to monitor email communications at any time if this is deemed necessary.

- Web-email is provided for use of *Newbridge High School* staff and students only. Access by any other party is strictly prohibited.
- By using Web-Email, you signify that you are an employee of *Newbridge High School*, and that you have been authorised to use the system by the relevant Academy authority.
- Observe security guidelines at all times. Never reveal your password to anyone
- Remember to treat file attachments with caution. File attachments may contain viruses or other forms of malware 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. *Newbridge High School* accepts no responsibility for damage caused to any external equipment or software as a result of using the web-email service.

3.3 Additional Web Based Applications

Newbridge uses a range of software and Web Based systems, which include PARS, INSIGHT, Google Apps, Eclipse and our Cashless Catering system etc.

If you have been given access to any software you are only entitled to use it whilst employed at or studying at Newbridge.

You must use all software with caution and take responsibility in keeping your data safe, accurate and up to date.

You must not share your password with anyone nor let someone use your account to gain access to any of the systems.

Google Apps

Mail is provided by Google Apps – You must agree to their acceptable use policy to use this service:

You agree not to, and not to allow third parties or Your End Users, to use the Services:

- to generate or facilitate unsolicited bulk commercial email;
- to violate, or encourage the violation of, the legal rights of others;
- for any unlawful, invasive, infringing, defamatory, or fraudulent purpose;
- to intentionally distribute viruses, worms, Trojan horses, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- to interfere with the use of the Services, or the equipment used to provide the Services, by customers, authorized resellers, or other authorized users;
- to alter, disable, interfere with or circumvent any aspect of the Services;
- to test or reverse-engineer the Services in order to find limitations, vulnerabilities or evade filtering capabilities;
- In addition to this Newbridge insists that the use of this service is subject to the following guidelines. Staff should use email in accordance with the following guidelines and are reminded that the *Academy* retains the right to monitor email communications at any time if this is deemed necessary.
- Web-email is provided for use of *Newbridge High School* staff and students only. Access by any other party is strictly prohibited.
- By using Web-Email, you signify that you are an employee of *Newbridge High School*, and that you have been authorised to use the system by the relevant Academy authority.
- Observe security guidelines at all times. Never reveal your password to anyone
- Remember to treat file attachments with caution. File attachments may contain viruses or other forms of malware 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. *Newbridge High School* accepts no responsibility for damage caused to any external equipment or software as a result of using the web-email service.

4.0 Privacy and Data Protection

4.1 Passwords

- Never reveal your password to 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. It is advisable to use a 'strong' password. A strong password is one which contains a combination of upper and lower-case letters, numbers and other punctuation characters. You can substitute numbers and letters for other characters that look similar, such as '3' for 'E', '1' for 'I' or '@' for 'O', '!' for '1' etc. This will help to make your password much more difficult to guess. Remember that passwords are case-sensitive.
- If you forget your password, please request that it be reset via *The ICT Department*
- If you believe that a student or other staff may have discovered your password, then change it *immediately*.

4.2 Security

- Never attempt to access files or programs to which you have not been granted authorisation. 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 *The ICT Department.*
- Any user identified as a security risk will be denied access to the system and subject to disciplinary action in accordance with the Trusts Disciplinary Procedures Employees.

5.0 Management and Information Systems

Access to MIS software is available through the school network and via remote access. Usage of MIS software is subject to the following guidelines:

- Password security is vital. If you believe that your password has been discovered by a student or other member of staff, please request that it be reset via *The ICT Department*.
- If you leave your computer unattended, particularly in a classroom, either log out or lock it by using the CTRL-ALT-Delete keys and then choosing "Lock Workstation". Once this is done, you will need to re-enter your password to gain access to the computer.
- If you are using MIS software on a computer in a classroom connected to an interactive whiteboard and projector, please be aware that any student information you display on your screen may also be displayed on the whiteboard if the projector is turned on. To ensure protection of sensitive data, pleas ensure that projectors are turned off or disconnected before using MIS software.
- Where staff are working at home and connect remotely to the school's MIS system then all of the above considerations also apply. Staff must ensure that their home internet connection is secure from outside access particularly if a wireless network is used. Additionally staff should take due care of any material which they print at home.

6.0 Support Services

All ICT hardware and software maintenance and support requests should be submitted to *The Network Manager and ICT Department* using one of the following methods:

- Telephone: *The ICT Department on 222 (Internal) or +44 (0) 1530 276 442 (External)*
- Email: helpdesk@newbridgesch.uk
- In person at the *ICT Office*

Newbridge High School will make every effort to ensure that all technical or operational problems are resolved within a reasonable time.

6.1 Software Installation

The Network Manager and ICT Department assumes responsibility for all software installation and upgrades. Staff may request the installation of new software packages onto the network, but this will be subject to the following:

- A minimum of *1 day* is required for packaging and installation of new software.
- Software cannot be installed on the *School's* network without a valid license agreement. This must be supplied with the software package.
- Please check the licensing terms of the software package carefully to ensure that it is suitable for use on the Academy network. If you are unsure, please ask *The ICT Department* for assistance or contact the software supplier. A relevant and valid license agreement document will be required before any software packages can be installed.
- All software installation media and license agreements are held centrally within the *Academy* to aid in license tracking and auditing. Installation media cannot normally be released except by special agreement.
- When purchasing new software for use on the *Academy* network, please check its suitability, compatibility and licensing terms with *The ICT Department*. Purchase orders for new software will normally be authorised only with the agreement of *The Network Manager and ICT Department.*

6.2 Service Availability

Whilst every effort is made to ensure that the systems, both hardware and software are working correctly, the Academy 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 *Academy* ICT system is at your own risk. *Newbridge High School* specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

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 another user's password and use it.
- Unauthorised access to deliberately commit an unlawful act e.g. if you guess another user'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 2018

  The Data Protection Act was updated in May 2018 and is the UK's implementation of the General Data Protection Regulation (GDPR). It ensures that information held about you is used for specific purposes only. These rules apply to everyone in the school.

  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 protection.

Other policies:

- **Anti-bullying policy**
- **E-safety policy**
- **GDPR Policy**
- **Social Media policy**
- **Safeguarding and child protection policy**

Return slip

MEMBER OF STAFF/VOLUNTEER

I understand and agree to the provisions and conditions of the ICT Acceptable Use policy agreement. I understand that any violations of the above provision may result in disciplinary action and revocation of privileges. I also agree to report any misuse of the system to *The Network Manager*. I agree to use the Internet and electronic communications systems in compliance with the terms outlined in the ICT Acceptable Use policy and understand that my Internet access and any electronic communications may be logged or monitored.

NAME

_____

SIGNATURE

_____

DATE

_____

RETURN TO SCHOOL OFFICE – THANK YOU