Ashby School
Empowered to Learn

Student Agreement to Acceptable Use Policy for the School's Computers and Network

The full and detailed version of Ashby School's Authorised Acceptable use Policy for the school's computers and network is attached and we suggest that it is read through, for not only does it contain a comprehensive explanation but also highlights all the Information Technology services available in the school. Please keep the policy for future reference. Further copies can be downloaded from the school website.

All students are expected to follow this policy. All students will be allowed to access the internet and school's email system by default.

1. I agree not to change, alter or damage the equipment and the programmes.
2. I agree to use the printers in the correct manner, for school use only, and not to waste paper.
3. I agree to be polite when using email and all other forms of electronic communication.
4. I agree not to download or open unknown file attachments.
5. I agree to use only appropriate internet sites and avoid inappropriate sites. Furthermore I agree to use only internet sites approved by my teacher. I will not use chat rooms, offensive websites or game sites.
6. I agree not to print pages directly from a website.
7. I agree to keep my password and other personal information confidential.
8. I agree that Ashby School learning environment is provided for the use of Ashby School students and staff only.
9. I agree to report to my teacher or another member of staff if any offensive material is downloaded onto my mobile phone or any other device.
10. I agree to report to Network Services immediately if I lose any work.

Name: _____ **Form:**_____
(Block Capitals)

Signature: _____**Date:**_____

Name of Parent: _____
(Block Capitals)

Signature:_____**Date:**_____

☐ ***Please tick to confirm you have read the Authorised Acceptable use policy for students available on the school website.***
For those who do not have access to the website, the library has copies available.

Authorised Acceptable use Policy for Students

Why have an Acceptable use Policy?

The Acceptable use Policy is to ensure that students at Ashby 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 eg. equipment; printers and consumables; Internet and email; managed learning environments and websites.

The Acceptable use Policy also seeks to ensure that students are not knowingly subject to identity theft and therefore fraud. Also, that students avoid cyber-bullying, and, just as importantly, do not become a victim of abuse. We have also made unavailable certain proxy sites, as well as anonymous proxy sites, as these sites may put the school network at risk. Help us to help you keep safe.

Ashby School recognises the importance of IT in education and the needs of students to access the computing facilities available within the school. The school aims to make its IT facilities available for students both in and out of lesson times. To allow for this Ashby School requires all students and their parents/guardians to sign a copy of the Acceptable Use Policy before they receive their username and password.

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

Please read this document carefully and sign and date it to indicate your acceptance of the Policy. Access to the School's IT facilities will only take place once this document has been signed by **both** the student and parent/guardian.

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 IT 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, base units, printers, keyboards, mice or other hardware;
- the change or removal of software;
- unauthorised configuration changes;
- knowingly creating or uploading computer viruses;
- deliberate deletion of files;
- bypassing of the web filtering system.

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

1.2 Use of Removable Storage Media

Ashby School acknowledges the fact that you may wish to transfer work from school to home by using a flash memory device or a CD disk. However, Ashby School cannot guarantee that your work will be able to be transferred properly using these.

Students are advised to use the remote access system to transfer files from their designated user areas (My Documents, shared areas etc) whilst not on school network. Students should not rely solely rely on single storage device i.e. memory sticks or user area on network for

important data. Theft or failure of any such device may render the data inaccessible or corruption. It is advised to keep important data backed up to another device – your data may be at risk if you do not have working backup.

1.3 Printers and Consumables

Printers are provided for use by students in all IT suites and various other rooms. For students wishing to print in colour there are high-speed laser printers located in Reprographics. These printers are capable of printing in A4, A3, and A5 sizes. There is a small charge for this service and print out requests should be forwarded to the Reprographics Department.

In addition to the Reprographics service there are colour inkjet printers available in some rooms – such as new Art Block (D&T), Electronics and Food Technology area.

Art Rooms (C23, C24) have scanners that are capable of scanning images up to A3 size.

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-education or offensive material you will be subject to the behaviour management measures of the school which includes the following:

- 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 eg. the Police.

1.4 Data Storage, Security and Retention

All data stored on the Ashby School network is backed up daily and backups are stored for up to eight weeks. If you should accidentally delete a file or files in your folder or shared area please inform Network Services immediately so that it can be recovered. Generally, it is not possible to recover files that were deleted more than eight weeks previously. Whilst a best effort will be made to restore data, Ashby School cannot guarantee the integrity or availability of data backups and will not be held responsible for any losses incurred as result of user error or software or equipment failure.

Students are allocated appropriate disk storage space on the Ashby School's network. Storage space (quota) may be increased upon request if required by a member of Network Services team. Students are advised to observe the following guidelines whilst using the storage space provides:

- Use your disk storage space for files related to educational and or research purposes.
- Storage of copy-right materials such as MP3 or other audio or video files is strictly prohibited and will be removed if discovered without warning.

- Do not store or attempt to run/launch any executable content – EXEs, COM, BAT,VBS, SWF files etc. unless if they are required for any courses offered at Ashby School.

- Do not store any illegal material or anything likely to incite racial or religious hatred.

- Do not store or save copies of other students work

- Never attempt to access another student's storage area

- Practice good housekeeping of your storage area and email storage – delete any files or emails that you no longer needs and empty the "Deleted Items" regularly.

2. Internet and Email

2.1 Content Filtering

Ashby School provides two layers of internet filtering designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. Inappropriate websites or content must be reported to teaching staff immediately.

Ashby School considers the use of Internet and email to be 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 three months. Usage reports will be provided to any member of staff (or parents/guardians) upon request.

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

- Only suitable material should be accessed – the Internet is not be used to download, send, print, display or transmit material that would cause offence or break the law.
- Students must not access internet chat sites. Remember you could be placing yourself at risk.
- Students must never enter personal information on a website, especially home address, mobile telephone number or passwords.
- Students must not access online gaming sites. Remember that the use of the Internet is for educational purposes only.
- Students must not download or install software from the Internet, as it is considered to be vandalism of the school's IT facilities.
- Students must not use the Internet to order goods or services from on-line, e-commerce or auction sites.
- Students must not subscribe to any newsletter, catalogue or other form of correspondence via the Internet.
- Students must not print pages directly from a website. Web pages are often not formatted for printing and this wastes resources. If students wish to use content from websites, it is recommended that the copy and paste facility is used to move it into another application, copyright permitting.
- Students must not by-pass any web filtering system.

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. All emails between students and staff should be via the school email system. The sending or receiving of messages which contains any material that is of a sexist, racist, unethical or illegal nature, or likely to cause offence, is against school regulations.

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 personal information about yourself or anyone else, especially home address, personal telephone numbers, usernames or passwords. Remember that electronic mail is not guaranteed to be private.
- Consider the file size of an attachment, a file exceeding 1MByte in size is 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.

3. External Services

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

3.1 PC Suites and Labs

There are over 1000 stations (Desktop, Laptop Trolleys, Tablets) running Microsoft network for the students to use on the curriculum network. There are various IT suites (consisting of 28-30 stations each) located in many faculties across the school site.

Each user shall have a unique user ID and password to logon to the curriculum network. Users must not, under any circumstances, divulge their password to anyone. The default password must be changed as soon as possible and it is recommended that users select a password that is at least 6 characters long comprising of letters, numbers and special characters.

3.2 Storage

Storage for files created by users is available on the school's main curriculum servers and users will have full access to files they have created unless either the ownership or authorship is in question.

3.3 Library

The Library has a trolley (with laptops and tablets) on the curriculum network for students to use. These stations are bookable on a first come first served basis.

3.4 Internet and Email Services

All curriculum networked stations have internet and email access which is filtered by a web filter and proxy server according to the school's acceptable use policy and other L A and DFE guidelines.

All students and staff have a unique email address on the school system to enable them to communicate with other staff members and students, both in school and externally. Microsoft Outlook 2010 (full client) is available in school for email access and Outlook Web Access

(OWA) is available to access email remotely ie. outside of school network(s). More information on how to access these services can be found on the school's Intranet site under the 'Students' section.

3.5 Easylink (Home Access Plus)

Easylink system provides remote access to files and resources stored on the school's network via the Internet. This is provided to students and staff for the purpose of file transfer between home and school as well as for students to access other lesson specific resources.

- EasyLink is provided for use of Ashby School staff and students only. Access by any other party is strictly prohibited.
- By using EasyLink, you signify that you are a student or employee Ashby School and that you have been authorised to use the system by the relevant authority.
- Observe security guidelines at all times. Never reveal your password to anyone
- EasyLink should only be used to transfer files associated with educational or research activities, relevant to the subjects you are studying. Any other use is strictly prohibited.
- All files must be virus checked before being transferred via EasyLink

3.6 Availability

The stations are available for students to use during lesson times (if the lesson requires the use of PCs/tablets) and also from 9.00am to 4.00pm.

Staff and students can get remote access to their documents and email from the school's servers using Easylink (see external services for section for more information). This service is available 7 days per week, 365 days per year. Any planned outages will be communicated to staff and students. In the case of unforeseen circumstances such as loss of power (power cuts etc) these facilities may be temporarily unavailable and best effort will be made to inform staff and students of unavailability.

3.7 Wireless network access for Sixth form Students

The school has a wireless network which allows Sixth Form students to access the Internet, email, and their documents (My Documents) from their own laptops.

Students wanting to connect to the wireless network must first register at the Network Services office in C Block and have their laptop configured by the Network Services team.

3.8 Service Uptime and Reliability

Ashby School has put in measures to provide contingency for the computer systems; such as uninterrupted power supplies, which allow services to be shutdown without data corruption in the event of a power outage, and multiple disk configurations to protect against data loss and corruption.

Ashby School will provide best effort to make sure that all services such as email, internet and data storage as well as applications are available at all times.

Any maintenance and network outages will be communicated to all staff to ensure that the message is passed on to students. Network Services will try to minimise the disruption and inconvenience any outage may cause.

3.9 Web Email (Outlook Web Access)

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 can be shown to parents/guardians upon request) 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 Ashby 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. Ashby School accepts no responsibility for damage caused to any external equipment or software as a result of using the web-email service.

3.10 Learning Environment Software (Realsmart)

Ashby School learning environment (realsmart) provides a web-based portal allowing users access to personalised learning resources and lesson materials. Realsmart solution makes use of Google Apps for Education which provides storage services as well as document creation tools. Use of this service should only be in accordance with instructions from your subject tutor and in accordance with the following guidelines:

- Ashby School learning environment is provided for use of Ashby School 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 Ashby School learning environment is a remote access service is provided by Realsmart. Ashby School can make no guarantees as to service availability or quality.

4. Privacy and Data Protection

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 Network Services 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. 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 IT facilities you will be denied access to the systems and be subject to disciplinary action.

4.3 Storage and Safe Transfer of Personal Data

- Ashby School holds information on all students and in doing so we must follow the requirements of the Data Protection Act 1998 (see Glossary). This means that data

held about students 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.

- Ashby School will seek to ensure that personal data sent over the internet will be encrypted or otherwise secured when using external services such as Webmail.

5. Service

Ashby School will endeavour 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 own errors or omissions. Use of any information obtained via the school's IT system is at your own risk. Ashby School specifically denies any responsibility for the accuracy of information obtained whilst using the IT systems.

6. Mobile Technologies

For reasons of safety and security students 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 other students.

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 students 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 it is advisable that students limit their use of mobile technologies to necessary communication during specified breaks during the school day.

If you are sent inappropriate material eg. images, videos etc report it immediately to a member of staff.

7. Bring your Own Devices (BYOD)

Mobile Technology is an accepted part of modern life and as such should be a part of School life. It offers a valuable resource for use in the classroom and has numerous educational opportunities from photographing notes for use later to browsing the Internet. As with all technology it can present risks if used inappropriately. Ashby School embraces technology, but within the safety of an agreed usage policy and some simple boundaries.

Throughout this section, the word *device* is used to describe any mobile phone, tablet computer, laptop, mp3 player or other device capable of communicating with either the Internet and/or mobile telephone networks and/or taking video/photographs/sound recordings. Well-known examples of these that are likely to be owned by students include iPhones, iPads and laptop computers.

The School takes no responsibility for the security, safety, damage, theft, insurance and ownership of any device used within the School premises that is not the property of the School. We will investigate the theft not the loss. If a device is stolen or damaged while on School premises, it is to be reported to reception immediately, in order that the incident can be logged.

Use of personal BYOD devices is at the discretion of the School and should not be seen as a right. Students' own devices can be used in the classroom at the teacher's discretion.

All BYOD devices shall only contact the Internet and local area network *via* the school wireless network. All internet access via the school's network (including BYOD) is logged.

The use of cellular data (e.g. GPRS, EDGE, 3G, 4G, etc) to access the Internet in School is strictly prohibited. All access must be by the School wireless network which is appropriately filtered. It is a condition of BYOD use under this policy that students are responsible for disabling cellular data on their device when on the School site.

The use of cameras and recording equipment, including those which may be built in to certain devices, to make images or sound recordings of individuals, is prohibited unless with prior permission of any individual(s) being photographed/recorded.

The School does not approve any apps or updates that may be downloaded onto any device whilst using the School's wireless network and such activity is undertaken at the owner's risk, with the School having no liability for any consequent loss of data or damage to the individual's device.

We encourage users to protect their own devices e.g. with the use of password or PIN as appropriate. Students are responsible for the use of their own device(s) while on the School site. Pupils are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

Privately-owned devices should not be used in a manner that would portray the School in an unfavourable light or bring the school into disrepute.

Devices should not be used to intimidate, abuse or perform any unfavourable acts against, staff, students or any person associated with the School.

- The use of a personal device is not to be a distraction in any way to teachers or pupils. Personal devices must not disrupt class in any way.

- The use of personal devices falls under Ashby School's Acceptable Use Policy (this policy).

- Pupils shall not use personal devices outside of their classroom unless otherwise directed by their teacher e.g. on school visits or activities.

- Pupils shall make no attempts to circumvent the school's network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security.

- Pupils shall not distribute pictures or video of pupils or staff without their permission (distribution can be as small as emailing/texting to one other person or as large as posting image or video online).

Any costs/fees incurred while using devices are not chargeable against the School and are the sole responsibility of the owner.

When on the School site and switched on, all BYOD must be set to silent. ??

Charging devices of any kind may not be used in School. ??

Consequences for Misuse/Disruption (one or more may apply):

- Access to the wireless network will be removed.
- Device taken away for the period.
- Device taken away and kept in the front office until parent picks it up.
- Student is not allowed to use personal devices at school.

Serious misuse of Internet capable devices is regarded as a serious offence within the School's Behaviour Management Policy and will be dealt with in accordance with this policy. ??

8. Glossary

Computer Misuse Act

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

- Unauthorised access to computer material eg. if you find or guess a fellow student's password and use it.
- Unauthorised access to deliberately commit an unlawful act eg. if you guess a fellow student's password and access their learning account without permission
- Unauthorised changes to computer material eg. 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 personal information held is used for specific purposes only. The rule applies to everyone in the school including Governors and volunteers.

The Act covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data held about individuals in the school. The Act applies to information stored in both paper and 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 I3
- 3T 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 IT records and files.

Policy revised April 2016