

ACCEPTABLE USE POLICY

|  |  |
| --- | --- |
| Reference this policy is aligned to with LCC | **n/a** |
| Agreed with Support Staff Trade Unions | **n/a** |
| Adopted by the Governing Body | **Sep 2020** |
| Next Review Due | **Sep 2024** |
| Agreed with Teacher Trade Unions and Professional Associations | **n/a** |

### **Why have an acceptable use policy?**

An Authorised Acceptable Use Policy is about ensuring that you, as a member of staff/student/volunteer/Governor at Welland Park Academy can use the Internet, email and other technologies available at the Academy in a safe and secure way. The policy also extends to out of school facilities e.g. equipment; printers and consumables; Internet, social media and email, managed learning environment and websites.

We will use the term, ‘all users’ throughout this policy, this covers: staff, students, volunteers, Governors.

An Authorised 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.

Welland Park Academy strongly believes in the educational value of ICT and recognises its potential to enable all users in delivering and supporting the curriculum. Welland Park Academy 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 Welland Park Academy is that all users will play an active role in implementing the Academy’s Acceptable use Policy.

Welland Park Academy recognises that for all users 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 material associated with their work. However, Welland Park Academy expects that all users, will at all times, maintain an appropriate level of professional conduct in their own use of the Academy’s ICT facilities.

Listed below are the terms of this policy. All users 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 Welland Park Academy Disciplinary/Behavioural Procedures in accordance with the latest General Data Protection Regulations 2018 (GDPR).

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

### **Equipment**

**Computers**

All computers and associated equipment are the property of Welland Park Academy and must be used in accordance with this policy which adheres to the Computer Misuse Act 1990, Data Protection Act 1998 & the GDPR 2018. The Operations Manager assumes responsibility for 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.
* The uploading of computer files to the Academies network

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.

**Portable devices**

Portable devices are issued to all staff as required. Portable devices remain the property of Welland Park Academy all times, and their usage is subject to the following guidelines:

* The equipment remains the property of Welland Park Academy at all times and must be returned to the School at the end of the contractual period.
* Maintenance of the equipment is the responsibility of the Welland Park Academy. All maintenance issues must be referred to ICT Support through the usual channels.
* All installed software MUST be covered by a valid license agreement held by Welland Park Academy.
* All software installation MUST be carried out by ICT Support 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 or Internet 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 up, either to an encrypted memory stick or to the Welland Park Academy network. Where removable media is used the user must ensure that these media have not been used to download materials that are at risk of damaging the network. It is recommended that the IT Services team transfers files for users.
* The user of the equipment must not encrypt any data or password protect any files so as to ensure future usage of the equipment. The encryption of all data will be undertook/supervised by the Operations Manager using Welland Park guidelines.
* Welland Park Academy 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 IT Services to perform software updates and maintenance for which the equipment must be made available in School when reasonably requested.

### **Use of removable storage media**

**Staff/Governors/Volunteers**

All use of removable media must be agreed by the Senior Leadership team in discussion with the Operations Manager. This needs to be considered on an individual basis. All users will be directed to use their 365 cloud account, where possible.

**Students**

Whilst students may use removable memory devices to transfer files between home and Academy, Welland Park Academy cannot guarantee the correct operation of any removable media or the integrity of any data stored on it. Welland Park Academy cannot guarantee the correct operation of removable memory devices on the system, although every effort is made to ensure that this facility is available. Students are advised to consider use of 365 cloud for file transfer between Academy and home where possible.

### **Printers**

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.

### **Data security & retention**

All data stored on the Welland Park Academy 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 IT Services immediately so that it can be recovered. Generally, it is not possible to recover files that were deleted more than 1 week previously.

### **Internet & email**

**Content Filtering**

Welland Park Academy 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 IT Services so that they can be filtered.

**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 Academy. This includes abiding by copyright laws.
* Do not access Internet chat sites. These represent a significant security threat to the Academies network.
* The use of unauthorised online gaming sites is 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 Operations Manager assumes responsibility for all software upgrades and installations.
* Staff are reminded that ALL Internet access is logged and actively monitored and traceable.
* The duration of data being stored on the Academy network is an issue that the Academy’s Finance Director/Operations Manager will need to decide upon in conjunction with the Principal and other members of the SLT. This will be documented on the Academy’s retention policy.

**Email**

Staff are provided with an email address by Welland Park Academy. 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 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 School network.
* Staff should not send personally identifiable information by email, as it is not a secure medium.

# E-mail policy and code of practice

**Introduction**

The Welland Park Academy’s computer system enables members of the Academyto communicate by e-mail with any individual or organisation with e-mail facilities throughout the world.

For the reason outlined above, it is essential that an acceptable use exists, which sets out the rules and principles for use of e-mail by all. Consideration of the WPA wellbeing policy also needs to be applied.

Any breach of this policy will be treated seriously and it may result in disciplinary or legal action or expulsion. The Academymay take steps, including legal action where appropriate, to recover from an individual any expense or liabilities the Academy incurs as a result of the breach of this policy and code of practice by you.

**Purpose**

You should only use theAcademy’s e-mail system for Academy related emails. You are permitted only to send a reasonable number of e-mails.

**Trust's disclaimer**

The Academy’s e-mail disclaimer is automatically attached to all outgoing e-mails and you must not cancel or disapply it.

**Monitoring**

Copies of all incoming and outgoing e-mails, together with details of their duration and destinations are stored centrally (in electronic form). The frequency and content of incoming and outgoing external e-mails are checked from time to timeto determine whether the e-mail system is being used in accordance with this policy and code of practice.

The Principal, Finance Director and Operations Manager are entitled to have read-only access to your e-mails.

**Security**

As with anything else sent over the internet, e-mail is not completely secure. There is no proof of receipt, e-mails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents.

As with other methods of written communication, you have to make a judgment about the potential damage if the communication is lost or intercepted. Never send bank account information, including passwords, by e-mail.

**Program files and non-business documents**

You must not introduce program files or non-business documents from outside onto the Academies network. This might happen by opening an e-mail attachment or by downloading a file from a web site. Although virus detection software is installed, it can never be guaranteed 100% successful, so introducing nonessential software is an unacceptable risk for theAcademy. If you have any reason for suspecting that a virus may have entered the Academies system, you must contact the IT Services staff immediately.

**Quality**

E-mails constitute records of the Academy and are subject to the same rules, care and checks as other written communications sent by the Academy so, for example:

* You should always consider whether it is appropriate for material to be sent to third parties;
* they may have to be disclosed in legal proceedings;
* they may have to be disclosed to a person if he makes a request to see information held about him under data protection law;
* they require the same level of authorisation before being sent;
* printed copies of e-mails need to be retained in the same way as other correspondence;
* they are confidential to the sender and recipient, unless you have been given permission to read them;
* transmitting the works of others, without their permission, may infringe copyright;
* sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libelous, malicious, threatening or contravening discrimination legislation or detrimental to the is a disciplinary offence and may also be a legal offence.

**Inappropriate e-mails or attachments**

You must not use e-mail to access or send offensive material, chain messages or list-servers or for the purposes of bullying or plagiarising work.

You must not send personal or inappropriate information by e-mail about yourself, other members of staff, students or other members of the Academy community.

If you receive any inappropriate e-mails or attachments you must report them to IT Services.

**Viruses**

If you suspect that an e-mail has a virus attached to it, you must inform the technical staff immediately.

**Spam**

You must not send spam (sending the same message to multiple e-mail addresses) without the permission of senior staff.

**Storage**

Old e-mails may be deleted from the Academy’s server after 12 months. **You are advised to regularly delete material you no longer require and to archive material that you wish to keep.**

**Message size**

Staff are limited to sending messages with attachments which are up to 3Mb in size. If you wish to distribute files within the Academy, you can do so by using shared areas.

**Confidential Emails**

You must ensure that confidential emails are suitably protected at all times. If working at home or remotely, you should be aware of the potential for an unauthorised third party to be privy to the content of the email. Confidential emails should be deleted when no longer required.

# E-MAIL POLICY – advice to all users

* All users should remind themselves of the AUP which relates to the monitoring, security and quality of e-mails. In addition staff should be guided by the following good practice:
* All users should check their e-mails on a daily basis and respond, as appropriate, within a reasonable period if the e-mail is directly addressed to them
* All users should avoid Spam, as outlined in the AUP.
* All users should avoid using the e-mail system as a message board and thus avoid sending trivial global messages. Whilst accepting the convenience of the Distribution lists, all users should try to restrict its use to important or urgent matters.
* All users should send e-mails to the minimum number of recipients
* All users are advised to create their own Distribution lists, as convenient and appropriate
* All users should always include a Subject line
* All users are advised to keep old e-mails for the minimum time necessary

# Further guidelines:

* **Remember**: E-mails remain a written record and can be forwarded to others or printed for formal use
* As a rule of thumb staff should be well advised to only write what they would say face to face, and should avoid the temptation to respond to an incident or message by e-mail in an uncharacteristic and potentially aggressive fashion. Remember “Tone” can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression.
* Remember that sending email from your Academyaccount is similar to sending a letter on Academy letterhead, so don't say anything that might bring discredit or embarrassment to yourself or the Academy.
* Linked with this, and given the popularity and simplicity for recording both visual and audio material, staff are advised to remember the possibility of being recorded in all that they say or do.

### **External services**

Welland Park Academy 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

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.

**Office365 and 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 School retains the right to monitor email communications at any time if this is deemed necessary.

* Web-email is provided for use of Welland Park Academy Staff and students only. Access by any other party is strictly prohibited.
* By using Web-Email, you signify that you are an employee of Welland Park Academy, and that you have been authorised to use the system by the relevant School 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. Welland Park Academy accepts no responsibility for damage caused to any external equipment or software as a result of using the web-email service.
* The rules that apply to Email are also to Web-Email.

### **Privacy & data protection**

**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 IT Services.
* If you believe that a student or other staff may have discovered your password, then change it **immediately**.

**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 to The Principal, Operations Manager or Finance Director.
* Any user identified as a security risk will be denied access to the system and subject to disciplinary action in accordance with WPA Disciplinary Procedures.

**Management and Information Systems**

Access to MIS software [SIMS.net] is available only from designated locations and only to those staff who require it. Access is subject to agreement with Principal, Operations Manager & Finance Director. 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, **change it immediately**.
* 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.
* Joining administration and curriculum networks raises issues regarding who within the school organisation has access to data. Within Welland Park Academy it is understood that the Principal & Senior Leadership team have a clear duty of care to protect the access to confidential data.
* 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.

### **Mobile technologies**

For reasons of safety and security staff, governors and volunteers 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 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, it is advisable that staff, governors and volunteers working with children and young people within the school setting, limit their use of mobile technologies to necessary communication during specified breaks during the school day.

If you are sent inappropriate material e.g. images or videos **report it immediately**.

### **Support services**

All ICT hardware and software maintenance and support requests should be submitted to IT Services using one of the following methods:

* Email helpdesk@wellandparkacademy.com
* In person at the IT Services.

Welland Park Academy will make every effort to ensure that all technical or operational problems are resolved within a reasonable time.

### **Software installation**

The IT Services Team 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 5 working days 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 School network. If you are unsure, please ask IT Services for assistance. 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 School 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 School network, please check its suitability, compatibility and licensing terms with the Operations Manager. Purchase orders for new software will normally be authorised only with the agreement of Finance Director/Operations Manager.

### **Service availability**

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 ICT system is at your own risk. Welland Park Academy specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

### **Social media**

Staff should not use social networking sites such as Facebook, Instagram, snapchat etc at school. Any activity should be avoided which puts staff at risk of breaches of privacy – staff should be careful when joining authorised social network groups such as sports clubs which current or recent students are members of and should not accept any links with current or recent students of Welland Park Academy. Staff are advised to ensure that any personal information released on such sites is not available to students at the Academy.

### **Useful Information:**

* This policy has been written with the following legislation taken into consideration:
	+ Computer Misuse Act
	+ Data Protection Act 1998
	+ RIPA – Regulation of Investigatory Powers Act 2002
	+ GDPR – General Data Protection Regulations - 2018