WESTFIELD COMMUNITY SCHOOL

ACCEPTABLE USE OF ICT EQUIPMENT POLICY COMPLIANT WITH GDPR

UPDATED SEPTEMBER 2022

TO BE REVEIWED SEPTEMBER 2024

Westfield Community School
Montrose Avenue
Wigan
WN5 9XN
www.westfield.wigan.sch.uk

ACCEPTABLE USE OF ICT EQUIPMENT

Introduction

Westfield Community School has provided computers for use by staff as an important tool for teaching, learning, and administration of the School. Use of school computers, by both members of staff and pupils, is governed at all times by the following policy. Please ensure you understand your responsibilities under this policy and direct any questions or concerns to the Headteacher in the first instance.

All members of staff have a responsibility to use the Westfield Community School computer system in a professional, lawful, and ethical manner. Deliberate abuse of the computer system may result in disciplinary action.

Please note that use of the network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to subjectively limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the School and staff, to safeguard the reputation of the School and business delivery, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

Computer / Network Security and General Data Protection Regulation (GDPR)

The school will provide staff with a user account for accessing the computer system both internally and externally. This account will be tailored to the level of access you require, and is for intended user only and in line with the requirements of the General Data Protection Regulation. As such, you must not disclose your password to anyone. Password complexity requirements have been put in place to help secure user accounts.

- You must **never** allow a pupil/student to have individual use of a staff account under any circumstances
- When leaving a computer unattended, you must ensure you have either logged off your account, or locked the computer to prevent anyone using your account in your absence.
- You must not transmit any sensitive or personal information about staff or students via email without the data being encrypted by a method approved by the school.
- When publishing or transmitting non-sensitive material outside of the school, you must take steps to protect the identity of any pupil whose parents have requested this.
- If you use a personal computer at home for work purposes, you must ensure that any school – related sensitive or personal information is secured to prohibit access by any non-member of staff, and encrypted to protect against theft/loss.
- You must ensure that all portable computer equipment (such as laptops, ipads, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when not in use.

User Registration / Account Creation

Users account creation and removal procedures are enforced in line with contractual start and end dates. System access will be automatically denied as soon as contractual end dates are triggered. This may include:

- Access to internal systems
- Access to remote systems
- Access to Office 365 systems
- Access to MIS systems
- MIS services such as Arbor or SIMS

We endeavour to keep a copy of all data / email for up to 6 Months in line with the school retention / backup procedures. Under no circumstances will you backup / transfer any personal data for use in any other organisation.

Access Right Management

The school carefully controls access rights for all system users. Access rights are allocated based on group memberships and roles within the school and in line with the requirements of the General Data Protection Regulation. No attempt should be made to circumvent systems in an effort to gain access to resources / documents.

The school will regularly review access rights to ensure system/data security and to ensure users have the required access rights.

If a user has access to his/her email account or work document via a personal device the school reserves the right to secure/safeguard its data via any means it feels appropriate.

Backup / Restore Procedures

The school has a robust backup procedure. This includes:

- Scheduled backup plan
- Multiple onsite backup repositories / hardware
- Restricted access to all backup infrastructure systems / locations
- Cloud backups of all core systems / data
- Extensive backup retention periods

It is the user's responsibility to ensure their data is consistent and available. In the event that data is accidently overwritten and/or deleted this must be reported to a member of ICT Support staff as soon as possible. Failure to do so may result in data permanently being lost, subject to backup retention policies and availability.

Staff Password Policy

When you log on for the first time, the system will ask you to change your password.

- Your password must be at least 8 characters and meet the following criteria:
  - Must NOT contain the user's account name or parts of the user's full name that exceed two consecutive characters. o Be at least six characters in length.
  - Contain characters from three of the following four categories:
- English uppercase characters (A through Z).
- English lowercase characters (a through z).
- Base 10 digits (0 through 9).
- Non-alphabetic characters (for example, !, $, #, %).

o Password History enforced – A setting of '32 password remembered' has been configured

An example of the above would be… JysbnKKk15!

- You MUST NOT tell anyone your password or write down your password.
- To ensure system security we will not reset your password before verifying your identity.

Pupil / Student Password Policy

Pupil and student password polices will be robust yet specific to their relevant key stage group. Regardless all password policies will with operate in line with the requirements of the General Data Protection Regulation,

Expected Conduct

You **must** at all times conduct your computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. The following uses are considered unacceptable:

- Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
- Making ethnic, sexual-preference, or gender-related slurs or jokes.
- You **must** respect, and not attempt to bypass, security or access restrictions in place on the computer system.
- You **must** not intentionally damage, disable, or otherwise harm the operation of the computer network and/or resources.
- You **must** make efforts not to intentionally waste resources. Examples of resource wastage include:
- Excessive storage of unnecessary files on the network storage areas; Storage quotas have been implemented to prevent this.
- Excessive use of department/office printers to produce materials, instead of using reprographics resources.
- You should avoid eating or drinking around computer equipment.

Use of Social Networking websites and online forums

Please refer to the trust Social Media Policy a copy is available on the schools / service shared internal directory drives. Details are also referenced in the employee Code of Conduct policy.

Use of the internet

The internet is a valuable resource that is provided for users to conduct research, support teaching and learning and communicate with others. Due to the nature of some material on the Internet and the possible

misuse of the Internet, a number of precautions have to be taken to help ensure that the system is used responsibly. By using the internet, I agree that:

- I will only access the Internet for job related or for school authorised activities.
- I will not take part in Newsgroups, Chat or any instant messaging which have not been approved by the school.
- I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other staff and myself.
- I will not use school resources to subscribe to any goods or services, nor buy or sell using the Internet.
- I will not take part in any activity which goes against school guidelines or relevant legislation.
- I will not use any inappropriate language.
- I must not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- I will not harass, insult or attack others through electronic media.
- I will respect the ownership rights of people outside of the school as well as staff and pupils. This includes abiding by copyright and plagiarism laws.

The school recognises that occasional personal use of the schools computers is beneficial for to the development of your skills. Such use is permitted, with the conditions that such use:

- **must** comply with all other conditions of this AUP as they apply to non-personal use, and all other school policies regarding staff conduct;
- **must not** interfere in any way with your other duties or those of any other member of staff;
- **must not** have any unjustified effect on the performance of the computer system;

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

Use of Email

All members of staff with a computer account are provided with an email address for communication both internally and externally to organisations/individuals. The following considerations must be made when communicating by email:

E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. You **must** be cautious when sending both internal and external mails. The corporate standards used by the school must be practiced for e-mail.

- You **must not** purchase goods or services on behalf of the school via e-mail without proper authorisation.
- All school e-mail you send should have a signature containing your name, job title and the name of the school.
- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless clearly authorised to do so, you **must not** send, transmit, or otherwise distribute exclusive information, copyrighted material or other confidential information belonging to the school to any organisation.
- Sensitive email intended for external recipients must be encrypted using Office 365 Mail encryption technologies.
- All externally set emails are delayed for a period of 15 minutes to enable the sender time to ensure precise recipients.

Use of Remote Services

The school provide users with remote access to email, shares resources, personal data and common programs used by the school. To ensure maximum system security we have operate a two-factor authentication security measures. By using these remote access services, school employees agree that:

- I will not let any other person use my account to gain access to remote systems.
- I will not leave a remote session unattended

- I will not copy / share resources with any other organisation / individual or save to a personal device
- You **must** respect, and not attempt to bypass, security or access restrictions in place on the computer system.

Use of removable Storage Devices

USB memory sticks and other removable storage devices have become increasingly popular because of their small form appearance and large storage capacity. This has made them very convenient devices for carrying files from one place to another.

However, this way of storing data has introduced new security risks:

• Loss of information – a memory stick, like a computer, is susceptible to data loss or failure.
• Potential breach of data confidentiality – if the memory stick is lost or stolen.
• Loss of physical device – being so physically small the memory stick can be easily lost.
• Corruption of data - if the memory stick is not removed from a computer properly.
• Malicious content transmission – memory sticks can introduce viruses onto our internal computer network.

As such, the school have taken the decision to prohibit the use of any storage devices on the internal school network. Instead, Microsoft OneDrive for Business has been issued to all staff for data storage. This eliminates the security risks identified above.

Use of trust Mobile Devices such as ipads, laptops and phone

(not an extensive list) User Responsibilities

- The user is ultimately responsible for the physical state and condition of the mobile device.
- Cases for all mobile devices will be provided and must not be removed.
- The mobile device screen is made of glass and therefore is subject to cracking and breaking if misused: Never drop or place heavy objects (books, laptops, etc.) on top of the device.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the mobile device screen.
- Do not subject the mobile device to extreme heat or cold. Do not store or leave unattended in vehicles.
- Users may not photograph any other person, without that persons' consent.
- The mobile device is subject to routine monitoring by the school. Devices must be surrendered immediately upon request by a member of the school senior leadership team.
- Users must comply with the password policy set by the administrators.
- Due to the financial implications of paid apps from the App Store, we recommend avoiding purchases without first speaking to the Headteacher.

Safeguarding and maintaining as an academic tool

- Mobile device batteries are required to be charged and be ready to use in the school. (Charging Facilities are available in ICT Support however during this period the mobile device will remain in the ICT Support Office). The whereabouts of the mobile device should be known at all times.
- It is a user's responsibility to keep their iPad safe and secure.
- If a mobile device is found unattended, it should be given to a member of the schools Senior Leadership Team Immediately.

Prohibited uses (not exclusive)

- Accessing inappropriate materials – All material on the mobile device must adhere to the ICT Acceptable Use Policy. Users are prohibited to send, access, upload, download or distribute offensive, threatening, obscene, or sexually explicit materials.
- Illegal activities – Use of the schools internet/ e-mail accounts for financial or commercial gain or for any illegal activity. Violating copyrights – Users are prohibited from storing Copyright Music/ Videos on their mobile device.

- Cameras – Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos or ensure consent has been provided when using any ipad or portal device camera under the General Data Protection Regulation.
- Jailbreaking – Jailbreaking is the process of which removes any limitations placed on the mobile device by the OS vendor or hardware manufacturer. Jailbreaking results in a less secure device and is strictly prohibited.
- Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school.
- The mobile device must only be used by the individual user; friend's/ family members are strictly prohibited from using the device.

Monitoring/ Configurations

- All mobile devices are configured and monitored by ICT Support 24/7 using mobile device management software. It is possible for ICT to obtain data / usage reports at any time as required by the school.
- ICT Support will regularly check the mobile device for any new updates. During this period ICT will require sole access to the device.
- It is possible for the school to remotely view all mobile and fixed ICT device screens.
- All devices that access / store sensitive information are fully encrypted encryption protection to prevent from online attack or in the event the device is lost or stolen.
- All devices are password protected using Microsoft best practice password policies.
- All devices are configured with a local administrator account in the event of password loss / configuration changes.

Supervision of Pupil Use when using ICT Equipment

The school operates sophisticated classroom monitoring solutions to help staff with the supervision of students when using computer equipment.

- Pupils **must** be supervised at **all** times when using computer equipment.
- Staff are responsible enforcing the pupil Acceptable use policy when using computer equipment.

Confidentiality and Copyright

- Respect the work and ownership rights of people outside the school, as well as other staff or pupils.
- You are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the computer system or the Internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.
- You **must** consult a member of SLT staff before placing any order of computer hardware or software, or obtaining and using any software you believe to be free.

Reporting System Problems

The school is responsibility for the school computer system is working at all times and that any faults/problems are resolved as soon as possible. In support of this:

 You should report any problems that need attention to the ICT Manager or the Business Director as soon as reasonable practical.

Reporting Breaches of this Policy

All members of staff have a responsibility to ensure this policy is adhered to. Employees **must** immediately inform a member of school SLT, of abuse of any part of the computer system. In particular, you should report:

- any websites accessible from within school that you feel are unsuitable for staff or student;
- any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;

- any breaches, or attempted breaches, of computer security; or
- any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school computer system.

Mobile Phones and other Devices

For the purposes of this document, the term 'mobile phone' refers to any electronic device that can be used to take images or record videos, including tablets.

Use of mobile phones by staff members

- Staff members must not use personal mobile phones or cameras when children are present.
- Staff may use mobile phones on school premises outside of working hours when no children are present.
- Staff may use mobile phones in the staffroom during breaks and non-contact time.
- Mobile phones should be safely stored and in silent mode whilst children are present.
- Staff may take mobile phones on trips, but they must only be used in emergencies and should not be used when children are present. Mobile phones must not be used to take images or videos at any time during trips.
- Staff who do not adhere to this policy will face disciplinary action.
- Staff may use their professional judgement in emergency situations.
- Staff must report any concerns about another staff member's use of mobile phones to the DSL, following the procedures outlined in the Child Protection and Safeguarding Policy and the Allegations of Abuse Against Staff Policy.

Use of mobile phones by parents, visitors and contractors

- Parents, visitors and contractors are not permitted to take photographs or record videos without prior permission.
- Parents may take photographs and videos only containing their own child during school events.
- Parents may take group photographs at school events but only with the informed consent of the parents of the children involved.
- The school strongly advises against the publication of any photographs or videos taken at the school or school events on social media

Staff must report all concerns about parents, visitors and contractors to the DSL, following the procedures outlined in the Child Protection and Safeguarding Policy.

Use of the school's mobile phones and cameras

- Staff are provided with a school device to ensure that only school devices are used to take photographs and videos.
- School devices must have passcode protection.
- School devices must only be used for work related matters only.
- School devices must only be used to take photographs in the presence of another staff member and only with the consent of the child's parent.
- Staff must not take photographs of bruising or injuries for child protection reasons. Instead, they should immediately receive support and advice from the DSL.

Where staff members have concerns over material on a school device, they must report all concerns to the DSL, following the procedures outlined in the Child Protection and Safeguarding Policy.

Monitoring

All Westfield Community School resources, including computers, email, internet usage and voicemail are provided solely for educational purposes. At any time and without prior notice, Westfield School maintains the right and ability to examine any systems and inspect/review any data recorded in those systems using advanced auditing systems. This may include remote monitoring of an interactive logon session, any information stored on a computer, whether the information is contained on a hard drive, computer disk or in any other manner may be subject to scrutiny by Westfield Community School. This examination helps