# ACCEPTABLE USE POLICY

## 1. Purpose and applicability

This policy defines the acceptable use of School's information assets and those assets provided to the School by partner organisations. It is known as the "Acceptable Use Policy" or "AUP".

This policy applies to School workforce including temporary and agency workers, volunteers, independent consultants and suppliers/contractors who need to use School information assets, as part of/to carry out their duties. These people are referred to as "users" in the rest of this document. Acceptable use means that access to information is legitimate, it is used only for the intended purpose(s), the required standards of practice are in place to protect the confidentiality, integrity and availability of information and the use complies with relevant legislation and regulation. The School aims at all times to conduct its business in a professional manner and to provide the highest possible level of service, both internally and to its customers. Any loss, compromise, or misuse of School information and associated assets, however caused, could have potentially devastating consequences for the School and may result in financial loss and legal action.

## 2. Definitions

An **information asset** is any data, device, or other component of the environment that supports information-related activities. Assets include hardware (e.g. laptops), software and confidential information (e.g. a person's record).

Inappropriate use of information assets exposes the School and the service users who entrust us with their data to risks.

A **data subject** is a person or organisation to whom data relates. A **data controller** is a person or organisation who is legally in charge of a data asset. The School is the data controller for many of the assets it holds. A **data processor** is a person or organisation who is tasked by a data controller with using a data asset. The School is a data processor for some organisations such as the NHS, Local Authority and Police. A **user** is any person or organisation accessing information assets. **Personal data** is data that relate to an individual. For example, your name, address and date of birth are examples of your personal data. **Sensitive personal data** is data revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of

genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"[1] **"PC"** means any computer device such as a tablet, laptop or desktop. **"mobile"** means any portable device with a mobile network connecting including smart phones, standard phones, Personal Digital Assistants. Note that some tablet devices (e.g. a tablet with a mobile network connection) fall into both the PC and mobile category and rules for both must be followed.

## 3. Policy Statements

It is the responsibility of all users to know this policy and to conduct their activities accordingly. Breach by any user could result in disciplinary action or other appropriate action being taken.

School information facilities are provided for business purposes only, with limited personal use permitted as defined elsewhere in this document.

Use of information facilities must be authorised by line managers. Any use of School facilities for unauthorised purposes may be regarded as improper use of facilities. School IT systems must display an appropriate warning notice to this effect when users log on.

Users should be aware that any data they create on School systems (including anything pertaining to themselves) is deemed to be the property of School. Users are responsible for exercising good judgment regarding the reasonableness of personal use and to be compliant with the Employee Code of Conduct.

For security and network maintenance purposes, authorised users may monitor equipment, systems and network traffic at any time. The School reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

The policy is not designed to be obstructive. If you believe that any element of this policy hinders or prevents you from carrying out your duties, please contact the School Data Manager.

## 4. Use of Personal Data

The School has access to a wide range of personal data entrusted to us by our citizens and others. This data must be used and access in accordance with law.

Users must only use personal data in accordance with the agreed and published purposes for the collection of data. Using personal data in any manner requires a clear legal basis or consent from the data subject.

---

[1] General Data Protection Regulation EU679/2018 Article 9.

Merging personal data with other sources, for example, is not permitted unless a legal basis or consent is present, and the use of the data correctly authorised.

## 5. Information System Security

Security of the School's information assets is paramount. Information assets must be treated as confidential unless marked as public. The School is the data controller for most information assets held, however users must be aware that the School acts as a data processor for other organisations. Users with access to such information assets must maintain awareness and compliance with the data owner's policies.

### a. Security Controls and Reporting

The School has implemented security systems to safeguard information assets. These include controls over viruses, offensive and illegal material, disruption to our systems, and unauthorised access. Bypassing or attempting to bypass these security systems is a breach of policy. To be effective, all users must support and use these systems and must assist in identifying and eliminating threats to information security. Any breach or suspected breach of this policy must be regarded as a security incident. Users must report security incidents to the Data Manager immediately.

### b. Use of Downloaded Programmes

Under no circumstances may users use any programme that is not already installed on a School PC or laptop or download programmes from the Internet for use on School ICT systems. For mobile devices, only applications from approved app stores should be installed.

### c. Passwords

Users are responsible for the security of their passwords and accounts.
Passwords must be kept confidential and not shared with others.
Passwords should be changed at regular intervals or based on the number of accesses. The reuse of old passwords is not permitted.
Temporary passwords must be changed at the first log on. Passwords must be changed whenever there is any indication of possible system or password compromise.
If legitimate access to an absent person's system or data is required, then written or e-mail authority must be provided by a senior manager of the users and approved by Data Manager.

## 6. Internet Usage

The School provides access to the information resources on the Internet to help users carry out their functions. The provision of Internet access is at the School's discretion and users provided with internet access are required to read and adhere to this policy.
Internet access for personal use is at School's discretion and should not be assumed as a given. Any misuse of this facility can result in it being withdrawn. Limited personal use of the Internet is permitted outside of normal working hours.

E-mail Usage
The e-mail system is for School business use only. Users should use personal e-mail facilities wherever possible and web mail systems are allowed from School devices for this reason. However, the School understands that users may on occasion need to send or receive personal e-mails using their work address. Users wishing to send personal email must seek the prior permission of their manager.

E-mails that users intend to send should be checked carefully. E-mail should be treated like any other form of communication and, as such, what is normally regarded as unacceptable in, for example, a letter is equally unacceptable in an e-mail communication. The sender of the email is responsible for the safe arrival of information at its intended destination and it is the sender who is usually liable for any breach of security and confidentiality.

Sending e-mails internally is secure. Sending e-mails externally is not generally secure and they can be intercepted and viewed by unauthorised people. Secure e-mail must be used when e-mailing information to external agencies or individuals when the content of the e-mail includes:

- Personal, identifiable client or third party information
- Financial, sensitive or other information that could cause detriment to the School or to an individual

Personal or sensitive business information must not be sent to an email address outside of School, unless it is absolutely necessary, and the transmission is secure.

Staff must be vigilant with attachments to e-mails and links to documents downloaded from other locations as they may contain viruses. Users who

suspect a possible virus attack must report it to the Data Manager. immediately.

Staff must be aware that e-mail is easy to forge and that attacks based on this are common. Always treat e-mails asking for unusual actions with suspicion. For example:

- Any e-mail asking to move money should be confirmed in person or by telephone.
- Any email asking for a password or to click on a link which then asks for username, password or bank details even if it appears to be from IT may be fake – IT will never ask for these details.
- E-mails containing urgent invoices are likely to be fake – invoices should go via our scanning facility

**7. Responding to Security Incidents & Malfunctions**

Any perceived or actual information security weakness or incident must be reported to the Data Manager immediately. Examples of a security incident include unauthorised access to information assets, misuse of information assets, loss/theft of information assets, virus attacks, denial of service attacks, suspicious activity.

**8. Computer Viruses & Other Harmful Code**

All PCs and servers directly connected to resources, whether owned by the School or not, must be continually executing approved virus scanning software with a current virus signature file except where this is not technically possible.

It is a crime under the Computer Misuse Act 1990 to deliberately introduce malicious programmes into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc). Users must not use School facilities for intentionally accessing or transmitting computer viruses or other damaging software or software designed for creating computer viruses.

When the PC is not connected directly to the School network, users should scan any material received/downloaded from the Internet to make sure it is virus free using the approved anti-virus protection system and should not distribute any material that has not been scanned using the approved system.

If you are in doubt about any data received or suspect a virus has entered your PC, log out of the network immediately, stop using the PC and inform the IT Manager. You should always follow the instructions that the IT Manager issues about virus attacks.

**9. Hacking and Associated Activities or Breaches of Policy**

It is a crime under the Computer Misuse Act 1990 to enter into another computer system without authorisation.

School IT facilities must not be used in any way that breaks the law or breaches standards. Such actions could result in disciplinary action being taken.

Users must not use School facilities for:

- Sending threatening, offensive or harassing messages
- Creating or sending obscene material
- Accessing or transmitting information about, or software designed for, breaking through security controls on any system.
- Effecting security breaches or disruptions of network communication. These include, but are not limited to:
  - Accessing data to which the user is not an intended recipient without permission, even if it is not protected by security controls
  - Logging into a server or account that the user is not expressly authorised to access
  - Network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes
  - Port scanning or security scanning (unless prior authorisation has been granted)
  - Executing any form of network monitoring which will intercept data not intended for the user (unless prior authorisation has been granted)
  - Circumventing user authentication or security of any host, network or account
  - Interfering with or denying service to any user (for example, denial of service attack)
  - Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's communication session, via any means, locally or via the Internet / Intranet / Extranet

Users may be exempted from the some of the above restrictions during the course of their legitimate job responsibilities (e.g. systems administration

employees may have a need to disable the network access of a host if that host is disrupting production services).

**10. Copyright & Encryption**

It is illegal to break copyright protection. Users could break copyright if they download, transmit or copy protected material.

Users must not:

- Transmit copyright software from their PC or allow any other person to access it from their PC unless the controls/licence so permits
- Knowingly download or transmit any protected information/material (including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources and copyrighted music) that was written by another person or organisation without getting permission
- Copy/install copyright software from/to their PC for any purpose not approved by the licence and for which the School or the user does not have an active licence
- Transmit software, technical information, encryption software or technology, in violation of international or regional export control laws.

The Data Manager should be consulted prior to export of any material that is in question and all information in this respect should be documented accordingly.

**11. Unattended User Equipment**

Users must not leave their workstation unattended without ensuring that sensitive information is not visible on their screen or left on their desks and/or access to any open sessions are closed.

Users accessing sensitive information must position their workstation in such a way that the information is not visible to unauthorised users.

To protect against unauthorised access, equipment must be locked (generally, this can be achieved via holding the Windows key and pressing L) when not attended.

No paper copies of data, memory sticks or other portable media may be left on desks when unattended.

Lockable cabinets need to be available to store sensitive documentation whilst when a desk is unattended.

## 12. Hardware Usage

All School owned computer equipment and software remain the property of the School. Any user who leaves School employment / engagement is required to return all hardware and software that has been provided to them.

Only hardware provided by the School is authorised for use for School business, except as specified in the separate Bring Your Own Device Policy. Users must not attempt to attach any other equipment to School hardware or to network or telephone sockets.

## 13. Software Usage

School is committed to the use of authorised software within its computer systems. It is expressly forbidden for users to load or operate software gained from the Internet, magazines or other sources. The School is also committed to using software for which it has current licences. It is the responsibility of all users to ensure that they do not introduce viruses into computer systems. Users should take care when receiving electronic information from unknown sources, including attachments within E-mail. Where there are reasons to access information from questionable source(s), active virus checking must be performed, preferably on a standalone computer and/or test server, thus having no communication links to other systems.

The following provisions, which apply to the use of all computers, govern all users: -

- Only software purchased by School and approved by the IT Manager may reside on School computer equipment including PCs and mobiles.
- The IT Manager will undertake to purchase licences for all products used by School and will control the allocation of licences for products that are distributed as single media items and licences for multiple instances of that one distribution.
- Only the IT Manager authorised technical staff may install or remove software on School computer equipment.
- Software includes source code, object code and intermediate code that can be firmware as well as software.
- Downloading of “shareware” and/or “freeware” is prohibited irrespective of the fact that a licence may or may not be needed unless the IT Manager has approved the product to be downloaded and installed.
- The installation of personal software including screen savers is prohibited.

- Upgrades to software products will be treated as new products.
- All software media is to be held and securely stored by the IT Manager. Staff may copy software media only if they are legally allowed to do so. This is in accordance with Copyright laws and the terms and conditions of the relevant software license. Software media may not be copied under any other circumstances.

**14. Mobile Computing**

When using computing and communication facilities outside of the secure office environment, special care should be taken to ensure that information is not compromised. Protection must be in place to avoid unauthorised access to or disclosure of information including ensuring your screen cannot be seen by others and that equipment is not left unattended. If a device is lost or stolen, the Data Manager must be contacted as soon as possible.

**15. Access from overseas**

Access to the School's network from overseas is subject to additional controls to ensure compliance with relevant legislation and this may place additional personal liability on users.

Access from the countries of the EEA is generally permitted for school information assets, but not for those owned by others – please seek advice from the Data Manager before taking devices with access to non-data overseas.

The facility to remotely access the network from other countries will only be permitted in exceptional circumstances and should not be assumed. A written request including a business case must be submitted to the Data Manager for considerations at least a month in advance of any planned travel.

The user should seek advice from the It manager before taking any School supplied ICT equipment outside the United Kingdom. The equipment may not be covered by the School's normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel.

**16. Fax**

All faxes must include a non-disclosure statement and security classification.

All users must ensure that confidential faxes are protected during transmission and only sent when the recipient is aware of the transmission and is instructed to protect its content.

Confidential faxes must be removed as soon as the transmission has ended.

**17. Telephones**

Personal calls should be kept to a minimum and not interfere with performance of duties. The School reserves the right to check, review and monitor telephone calls made using any School telephone or telephone system.

Where the School provides a user with a mobile phone, it is to ensure that the user is contactable when away from the office. Therefore, School mobile phones should be switched on or directed to voicemail or an alternative phone at all times during working hours. Voicemail should be checked regularly, and greetings updated as necessary. Voicemail users should secure their messages with a minimum four-digit pin code and clear down messages on a frequent basis.

**18. Legislative Requirements**

Under no circumstances are users allowed to engage in any activity that is illegal under local, national or international law while utilising School resources.

**19. Monitoring Use**

The School reserves the right to monitor, review and record the use of all information and telephone systems and all documents stored on information systems, including documents profiled as private and confidential.

The School reserves the right to monitor e-mail traffic within the school email system and to access mailboxes and private directories without notification to the individual concerned that the right is being exercised. The School may exercise this right in order to establish facts relevant to School business and to comply with:

- Regulatory practices and procedures
- To prevent or detect crime
- To ensure compliance with School policies
- To investigate or detect unauthorised uses of the system or to ensure the effective operation of the system (e.g. to check if viruses are being transmitted)

Therefore, users do not have the right to privacy when using School information systems or in relation to any communications generated, received or stored on School information systems.

**20. Policy Compliance**

The School expects that all users will achieve compliance to the directives presented within this policy. This policy will be included within the School's Policy & Procedure folder and compliance checks will take place to review the effectiveness of its implementation.

**21. Exceptions**

In the following exceptional cases compliance with some parts of the policy may be relaxed. The parts that may be relaxed will depend on the particular circumstances of the incident in question.

- If complying with the policy would lead to physical harm or injury to any person
- If complying with the policy would cause significant damage to the company's reputation or ability to operate
- If an emergency arises

In such cases, the user concerned must take the following action:

- Ensure that their manager is aware of the situation and the action to be taken
- Ensure that the situation and the actions taken are recorded in as much detail as possible on a non-conformance report
- Ensure that the situation is reported to the Data Manager.

Failure to take these steps may result in disciplinary action.
In addition, maintains a list of known exceptions and non-conformities to the policy. This list contains:

- Known breaches that are in the process of being rectified
- Minor breaches that are not considered to be worth rectifying
- Any situations to which the policy is not considered applicable.

The School will not take disciplinary action in relation to known, authorised exceptions to the information security management system.

**22. Penalties**

Non-compliance is defined as any one or more of the following:

- Any breach of policy statements or controls listed in this policy

- Unauthorised disclosure or viewing of confidential data or information belonging to the School or partner organisation
- Unauthorised changes to information, software or operating systems
- The use of hardware, software, communication networks and equipment, data or information for illicit purposes which may include violations of any law, regulation or reporting requirements of any law enforcement agency or government body
- The exposure of the School or partner organisation to actual or potential monetary loss through any compromise of security
- Any person who knows of or suspects a breach of this policy must report the facts immediately to the School Business Manager.

Any violation or non-compliance with this policy may be treated as serious misconduct.
Penalties may include termination of employment or contractual arrangements, civil or criminal prosecution.

Policy Declaration

**I confirm that I have read, understood and will adhere to School's Acceptable Use Policy.**

Signature: ……

Name: ……..

Department: ……

Team: …… Date:

……

**To be retained by your Personnel Admin Team**