



# Acceptable Use Policy

<b>Last reviewed on:</b>	May 2024
--------------------------	----------

<b>Next review due:</b>	May 2025
-------------------------	----------

<b>Source</b>	Judicium
---------------	----------

<b>Owner</b>	Director of Operations
--------------	------------------------

### **Document Owner and Approval**

The Director of Operations the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the Trust's policy review schedule.

A current version of this document is available to all members of staff on the Trust website.

Signature:

Date:

### **Version History Log**

<b>Version</b>	<b>Description of Change</b>	<b>Date of Policy Release by Judicium</b>
1	Initial issue	06.05.18
2	Corrected spelling of iPads. Added bullet point about emails not containing personal opinions about other individuals and descriptions must be kept in a professional and factual manner.	23.08.19
3	Formatting amendments	03.08.22

## **Acceptable Use Policy and Agreement**

This policy is designed to enable acceptable use for staff, trustees and governors.

The Trust provides a range of ICT resources which are available to staff members, trustees and governors. In order to ensure the safety of staff, governors and pupils it is important that all staff members and governors follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the Trust's ICT systems and infrastructure;
- Define and identify unacceptable use of the Trust's ICT systems and external systems;
- Educate users about their data security responsibilities;
- Describe why monitoring of the ICT systems may take place;
- Define and identify unacceptable use of social networking sites and Trust devices; and
- Specify the consequences of non-compliance.

This policy applies to staff members, trustees, governors and all users of the Trust's ICT systems who are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by staff and monitoring by the Trust of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the Trust's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to the Director of Operations.

### **Provision of ICT Systems**

All equipment that constitutes the Trust's ICT systems is the sole property of the Trust.

No personal equipment should be connected to or used with the Trust's ICT systems. Users must not try to install any software on the ICT systems without permission from the Trust's IT Support Provider.

If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

The Headteacher, Director of Operations and the Director of Finance are responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptops/desktop computers or ICT equipment may be removed at any time and without prior warning for regular maintenance, reallocation or any other operational reason. Maintenance includes but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

### **Network Access and Security**

Users are not permitted to make any physical alteration either internally or externally, to the Trust's computer and network hardware.

All users of the ICT systems at the Trust must first be registered. Following registration, a network user account will be created consisting of a username, password and an e-mail address. All passwords should be of a complex nature to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them with any other person, except to designated members of the Trust IT Support Provider for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the Trust IT Support Provider as soon as possible.

Users should only access areas of the Trusts computer systems to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the Trust ICT systems or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the Trust ICT systems or cause difficulties for any other users.

### **Trust Email**

Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner.

Where email is provided, it is for academic and professional use [with reasonable personal use being permitted. Personal use should be limited to short periods during recognised break times and comply with this Acceptable Use policy.] The Trust's email system can be accessed from both the Trust computers and via the internet from any computer. Wherever possible, all Trust related communication must be via the Trust email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the Trust does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official Trust business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g., sensitive or personal information) will only be sent using a secure method including:
  - Email encryption;

- A secure upload portal (where by the recipient will be required to log in to retrieve the email/documentation sent);
- Password protection on sensitive documents. The sender must ensure that the password is sent separately to the intended recipient (i.e., in a separate email or over the phone).
- Emails should not contain children's full names in the subject line and preferably, not in the main body of the text either. Initials should be used wherever possible.
- Access to Trust/setting email systems will always take place in accordance to data protection legislation and in line with other appropriate Trust/setting policies e.g., confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).
- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on Trust headed paper would be.
- Trust email addresses and other official contact details will not be used for setting up personal social media accounts.
- Where possible, emails must not contain personal opinions about other individuals e.g., other staff members, children or parents. Descriptions of individuals must be kept in a professional and factual manner.

### **Internet Access**

Internet access is provided for academic and professional use [with reasonable personal use being permitted. Priority must always be given to academic and professional use.]

The Trust's internet connection is filtered meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a Trust. In this case, the website must be reported immediately to the Trust's IT Support Provider.

Therefore, staff must not access from the Trust's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material or using any of the following facilities will amount to gross misconduct (this list is not exhaustive):

- accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the Trust and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil and whether for the employee or for the Trust);
- downloading or disseminating material in breach of copyright;

- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found, the Trust may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.

### **Digital Cameras**

The Trust encourages the use of digital cameras and video equipment. However, staff should be aware of the following guidelines:

- Photos should only have the pupil's name if they are on display in schools only. Photos for the website or press must only include the child's first name.
- The use of personal digital cameras in the Trust is not permitted, including those which are integrated into mobile phones, iPads or similar.
- All photos should be downloaded to the Trust network as soon as possible.
- The use of mobile phones for taking photos of pupils is not permitted.

### **File Storage**

Staff members have their own personal area on the network, as well as access to shared network drives. Any Trust related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area for example, copyright music files.

### **Social Networking**

Any files stored on removable media must be stored in accordance with the Information Security Policy, summarised as follows:

- If information/data is to be transferred, it must be saved on an encrypted, password protected, storage device.
- No Trust data is to be stored on a home computer or un-encrypted storage device.
- No confidential or Trust data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.

### **Mobile Phones**

Mobile phones are permitted in Trust with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard/locker.
- Personal mobile phone cameras are not to be used on school trips. The Trust provides I pads/tablets for this purpose.

- All phone contact with parents regarding Trust/school issues will be through the Trusts/schools phones. Personal mobile numbers should not be given to parents at the schools in the Trust.

### **Messaging Services – e.g. Use of Whatsapp**

The use of messaging services, e.g. SMS, WhatsApp etc for trust or school business must be limited and must never disclose the names of children, parents or carers, or include any other categories of personal data. Staff should be mindful when using their own personal messaging accounts to communicate internally with other staff members for trust or school business that should a Subject Access Request be made, personal phones may be requested as part of the request as the information shared could include categories of personal data.

The Trust has a Social Media Policy which should be read in conjunction with this policy. The key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the Trust, schools, staff and students at all times and must treat colleagues, students and associates of the Trust with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly and users should ensure that neither their personal or professional reputation and/or the Trust's reputation, nor the reputation of individuals within the Trust are compromised by inappropriate postings.
- Use of social networking sites for Trust/school business is not permitted, unless via an officially recognised Trust site and with the permission of the CEO.
- Members of staff will notify the Director of Operations if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the Trust/setting.
- No Trust/school information, communication, documents, videos and/or images should be posted on any personal social networking sites.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos which show pupils of the Trust who are not directly related to the person posting them, should be uploaded to any site other than the Trust's website.
- No comment, images or other material may be posted anywhere, by any method that may bring the Trust or the profession into disrepute.
- Users must not give students access to their area on a social networking site (for example, adding a student as a friend on Facebook). If in exceptional circumstances, users wish to do so, please seek advice from the Headteacher.

The Trust may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the Trust's ICT system is or may be taking place or the system is or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by the Trust IT Support Provider to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy or any other Trust policy;
- investigate a suspected breach of the law, this policy or any other Trust policy.

#### **Failure to Comply with Policy**

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

#### **Monitoring of the ICT Systems**

Any unauthorised use of the Trust's ICT systems, cloud-based ICT systems, the internet, e-mail and/or social networking site accounts which the Trust considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The Trust reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.



**Acceptable Use Agreement**

*To be completed by all staff*

As a Trust user of the network resources/equipment I hereby confirm that I have read and understood the Acceptable Use Policy and that I agree to follow the Trust rules (set out within this policy) on its use. I will use the network/equipment in a responsible way and observe all the restrictions explained in the Trust Acceptable Use Policy. If I am in any doubt, I will consult the Director of Operations.

I agree to report any misuse of the network to the Director of Operations. Moreover, I agree to report any websites that are available on the Trust internet that contain inappropriate material to the Director of Operations. Finally, I agree to ensure that portable equipment such as cameras, iPads or laptops will be kept secured when not in use and to report any lapses in physical security to the Director of Operations.

Specifically, when using Trust devices:

- I must not use these devices for inappropriate purposes;
- I must only access those services for which permission has been granted;
- I will not download, use or upload any material which is unsuitable within a Trust setting or that may cause disruption to the Trust network.

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored. I understand that the Trust will monitor communications in order to uphold this policy and to maintain the Trust's network (as set out within this policy).

Signed ..... Date .....

Print name .....