Grimsdyke School
Acceptable Use of ICT Policy and Agreement

(Adopted model template from Judicium Ltd)

Written by:	Iain Sutherland	**Date:**	02.06.2020
Approved by:	Governing Body	**Date:**	29.11.2022
Last reviewed on:	05.07.2021		
Next review due by:	September 2023		

Introduction

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

The School provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of both 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 School's ICT systems and infrastructure.

- Define and identify unacceptable use of the school'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 school devices.
- Specify the consequences of non-compliance.

This policy applies to staff members and governors, and all users of the School's ICT systems 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 School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the UK General Data Protection Regulation (UK GDPR) and all data protection laws and guidance in force.

Staff are referred to the School's Data Protection Policy for further information. The School is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of staff are required to comply with the provisions set out in this policy at all times to protect the School's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the School's disciplinary procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

The School has the right to monitor all aspects of its systems, including data which is stored under the School's computer systems in compliance with the UK GDPR.

This policy mainly deals with the use (or misuse) of computer equipment, e-mail, internet connection, telephones, iPads (and other mobile device tablets), Blackberries, personal digital assistants (PDAs) and voicemail, but it applies equally to the use of fax machines, copiers, scanners, and the like.

The use by staff and monitoring by the School 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 School'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 Headteacher.

Provision of ICT Systems

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

No personal equipment should be connected to or used with the School's ICT systems. Users must not try to install any software on the ICT systems without permission from the Headteacher. 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 is responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptop/desktop computers or ICT equipment may be removed at any time, 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.

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

Network access and security

All users of the ICT systems at the School 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 complex 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.

Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

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 to any other person, except to designated members of the [Finance Team or Wibird (ICT support company)] 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 Headteacher or Mrs the School Business Manager] as soon as possible.

Users should only access areas of the schools 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 school 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 school ICT systems or cause difficulties for any other users.

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

School Email

E-mail is a vital business tool, but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline.

Where email is provided, it is for academic and professional use. Personal use is allowed but should be limited to short periods during recognised break times and locations across the school to fully comply with this acceptable use policy.

The School's email system can be accessed from both the school computers, and via the internet from any computer. Wherever possible, all school related communication must be via the school email address. Staff are advised to not link their emails to their personal mobiles in order to manage workloads, if this is done then it is seen as a personal choice by the member of staff.

E-mails should never be sent in the heat of the moment or without first checking the content and language and considering how the message is likely to be received. Staff are encouraged wherever practicable to write a draft e-mail first, print it out and review it carefully before finalising and sending. As a rule of thumb if a member of staff would not be happy for the e-mail to be read out in public or subjected to scrutiny then it should not be sent. Hard copies of e-mails should be retained on the appropriate file.

All members of staff should remember that e-mails can be the subject of legal action for example in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of staff who sent them and the School. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the School in the same way as the contents of letters or faxes.

Members of staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages. If such messages are received, they should not be forwarded and should be reported to a member of the Senior Leadership Group immediately. If a recipient asks you to stop sending them personal messages then always stop immediately. Where appropriate, the sender of the e-mail should be referred to this policy and asked to stop sending such material.

All staff must consider the following when sending emails:

- Language must not include swear words, or 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 School does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school 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 secure and encrypted email or password protection.
- Emails should never contain children's full names either in the subject line or preferably not in the main body of the text. Initials should be used wherever possible.

- Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/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 school headed paper would be.
- School 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 use being permitted. Priority must always be given to academic and professional use.]

The School'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 school. In this case the website must be reported immediately to the Headteacher or the School Business Manager.

Staff must not therefore access from the School'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 School 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 School);
- 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 School 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.

Additional Equipment and School Systems

Digital cameras

The school encourages the use of digital cameras and video equipment; however staff should be aware of the following guidelines:

Photos should only be named with the pupil's name if they are to be accessible in school only. Photos for the website or press must only include the child's first name.

The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones, iPads or similar.

All photos should be downloaded to the school 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 school 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. Any files stored on removable media must be stored in accordance with the information access and security policy, summarised as follows:

If information/data has to be transferred it must be saved on an encrypted, password protected, storage device

No school data is to be stored on a home computer, or un-encrypted storage device.

No confidential, or school 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 for staff are permitted in school, 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 school provides digital cameras for this purpose. In the unforeseen circumstance that images need to be taken as a record of the event

then permission must be sort from the Headteacher or Deputy Headteachers who have had DSL training.

All images must not leave school site and therefore must be securely stored on the school system and removed from any personal device.

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

Social networking

The School 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 school, staff and students at all times and that they treat colleagues, students and associates of the school 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 school's reputation, nor the reputation of individuals within the school are compromised by inappropriate postings.

Use of social networking sites for school business is not permitted, unless via an officially recognised school site and with the permission of the Headteacher.

Members of staff will notify the Headteacher, 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 school/setting.

- No 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 school who are not directly related to the person posting them, should be uploaded to any site other than the school's Website or designated school social media accounts. In doing so express permission from the parents must be sort.
- No comment, images or other material may be posted anywhere, by any method that may bring the school 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.

Additional Electronic Resources and Subscriptions

Annually the school subscribes to educational resources in order to support the teaching and learning of the curriculum. Depending on the resource and the access required, staff members are presented with usernames and passwords. These should be treated in in the same respect as the usernames and

passwords in school and should not be shared for any reason. Sharing of these could result in a breech in our GDPR procedures and the part or full removal of the resource through cancelling the subscription.

Monitoring of the ICT Systems

The school 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 school'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 Headteacher 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 school policy;
- investigate a suspected breach of the law, this policy, or any other school policy.

Failure to Comply with the 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.

Any unauthorised use of the school's ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the Headteacher 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 school 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.

Related Policies:
Social Media Policy

ACCEPTABLE USE AGREEMENT

To be completed by all staff

As a school 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 school 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 school acceptable use policy. If I am in any doubt I will consult the Headteacher; Mr Iain Sutherland.

I agree to report any misuse of the network to the Headteacher; Mr Iain Sutherland. Moreover, I agree to report any websites that are available on the school internet that contain inappropriate material to the Headteacher; Mr Iain Sutherland. I finally 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 Headteacher; Mr Iain Sutherland.

Specifically when using school devices: -

- I must not use these devices for inappropriate purposes
- I must only access those services I have been given permission to use
- I will not download, use or upload any material which is unsuitable within a School setting or that may cause disruption to the School 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 School will monitor communications in order to uphold this policy and to maintain the School's network (as set out within this policy).

Signed ……. Date ……..

Print name ……