# ICT Acceptable Use Policy

**How this policy fits in with other policies:**

| E safety policy | Staff Code of Conduct | Safeguarding & Child Protection policy | Adab & Behaviour policy |
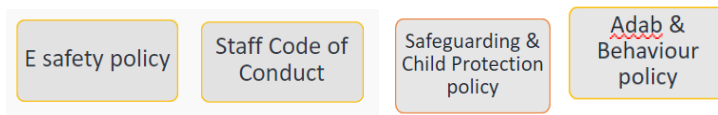
**Log of updates**

| 09/2015 | Adopted |
|---------|---------|
| 09/2017 | Reviewed |
| 09/2021 | Amended |

## Introduction

This Policy provides the guidelines of acceptable use of Information Communications Technology (ICT) equipment and facilities within Lady Nafisa School. ICT is seen as beneficial to all members of the School in supporting learning, teaching, research, administration and approved business activities of the School. The School's ICT Facilities provide a number of integral services and, therefore, any attempt to misuse a computer system could cause significant disruption to other users at the School. This could also lead to a breach of the data protection rights of individuals, resulting in harm to that individual and the School.

The purpose of the Acceptable Use Policy is not to impose restrictions that are contrary to established culture of openness, trust and integrity within the School. This policy is designed to protect all authorised users from illegal or damaging actions by individuals, either knowingly or unknowingly.

All Users, including but not limited to governors and staff using the School's Information Technology and Systems must ensure that they have read this Policy

before commencing to use its information and communication technology. All students will need to read and sign the User agreement included in this policy.

## Definitions

*"ICT Device"* means any laptops, tablets, telephones, smartphones, desktop computer, console, printer, speaker, camera or other electronic equipment that could be used for the carrying out of School business or the processing or storing of information.

*"ICT Facilities"* means all devices, facilities, systems and services including, but not limited to, network infrastructure, ICT Devices, software, websites, web applications or services and any device, system or service which may become available in the future which is provided as part of the ICT service.

*"Users"* means Governing Body, staff, students, volunteers, temporary guests, and all other persons authorised by the School to use the ICT Facilities.

*"Personal use"* means any use or activity not directly related to the users' employment, study or purpose.

*"Authorised Personnel"* means employee(s) authorised by the School to perform systems administration and/or monitoring of the ICT Facilities.

*"Materials"* means files and data created using the ICT Facilities including but not limited to documents, photographs, audio, video, printed output, web pages, social networking sites, bulletin boards, newsgroups forums and blogs.

## Policy Statement

The School's ICT Facilities should only be used to support learning, teaching, research, administration and approved business activities of the School. The ICT Facilities must not be used for personal commercial, political, charitable, and other such activities unless expressly authorised by the School.

The School employs various measures to protect the security of its computing resources and of its user accounts. Users should be aware that the School cannot guarantee such security. Users should therefore engage in safe computing practices at all times, backing up files, and promptly reporting any misuse or violations of this policy.

All devices that use the ICT Facilities, and that are capable of supporting software updates, security updates and automatically updating anti-virus products, must be configured to perform such updates.

Users' accounts and passwords must not be shared with anyone. Users are responsible for the security of their passwords, accounts and setting account and file permissions. Disclosure of account or password information may result is disciplinary action.

Occasionally the School may need to access information held by a User of the School within ICT Facilities, including, but not limited to, email, files stored on a personal computer or file storage or on other file store or backup media. This will usually occur when a User is absent, either ill or on leave, and a situation

arises which requires a rapid response. Users must be made aware that the School reserves the right to obtain access to files stored upon systems and services owned by the School, and that the privacy of personal material stored upon such systems and services in the event of authorised access cannot be guaranteed.

In exceptional circumstances, Authorised Personnel may need to make changes to user data or storage for the purposes of operating and providing a system or service. Where reasonable, Authorised Personnel should request permission of the data owner unless the situation is of such urgency as to make this impracticable. However, after such a change the file owner should be informed of the change and the purpose as soon as possible.

The Authorised Personnel may not, without specific authorisation from the Data Protection Officer, modify the contents of any file in such a way as to damage or destroy information.

Users must abide by all applicable laws and School policies to protect the copyrights and intellectual property rights of others. Copyrighted works may include texts, cartoons, articles, photographs, songs, videos, software, graphics, and other materials. This includes the use of the internet, as many of the materials available through the internet are protected by copyright. It is the responsibility of the user to assume that materials found upon the internet are copyrighted unless the materials contain an express disclaimer to the contrary. Users must obtain permission of the creator or publisher to copy or use software or other copyrighted materials written or created by others and must abide by contracts and agreements controlling installation and use of such software and other materials.

Users' use of the ICT Facilities must be in an ethical and legal manner and in accordance with School policies and procedures. Usage of the system to harass, defame, or invade the privacy of others, or to send or receive obscene materials, is not allowed and may result in disciplinary action under policies controlled by the School or prosecution under applicable laws.

## Unacceptable Use

The School reserves the right to block, disconnect or otherwise prevent what it considers to be unacceptable use of its ICT Facilities. Unacceptable use includes, but is not limited to:

All actions or activities that are illegal or in conflict with the School's policies, procedures, processes and regulations or which breach contracts or policies applied to the School by third party through a valid service contract or agreement.

Using the ICT Facilities for access, creation, modification, storage, download, hosting or transmission of material that could be considered pornographic, offensive, obscene, or otherwise inappropriate, or for placing direct or indirect links to websites which publish or host pornographic, offensive or inappropriate material.

Publishing materials or making statements which the School may deem to be advocating illegal activity, or threatening, or harassing, or defamatory, or bullying

or disparaging of others, or abusive, or libellous, or slanderous, or indecent, or obscene,  or offensive or promotes unlawful discrimination, breaches copyright or otherwise causing annoyance, or inconvenience.

Unauthorised production, distribution, copying, selling, hiring, performing of copyrighted material including, but not limited to, digitisation and distribution of computer software, television, radio, streaming services, websites, photographs, magazines, books, music or any  copyrighted  sources  and  installation  of  any copyrighted  software  for  which  the School does not have an active licence or explicit permission of the copyright owner, is strictly prohibited.

Authoring or sending any form of electronic communications or messages, including, but not limited to, videos, chats, messages and/or emails that were unsolicited and may be considered inappropriate, junk, "chain letters", "Ponzi", hoax warnings or advertising, and that do not correctly identify you as the sender, or messages which appear to originate from another person.

Unauthorised transmission, distribution,  discussion or disclosure of  information gained through a user's presence within the School or through the use of ICT Facilities.

Connecting any non-approved ICT  device, system or service (including  wireless access points) to School networks or setting up any network services, without the explicit or delegated permission from Authorised Personnel.

Unauthorised access (or attempted unauthorised access) to any ICT Facilities provided by the Academy.

Allowing, inciting, encouraging or enabling others to gain or attempt to gain unauthorised access to the ICT Facilities.

Causing any damage to ICT Facilities, including through the consumption of food or drink, or moving or removing such facilities without authorisation. The School reserves the right to charge for any damage caused.

Attempting  to  modify,  alter or in  any way interfere with  ICT facility security controls, hardware or software, configurations, settings, equipment, data files or websites  without  the  written  authorisation  or  delegated  permission  from Authorised Personnel.

Introduction of unauthorised and/or malicious software or programs into the  ICT Facilities, including, but not limited to: unlicensed software, viruses, worms, Trojan horses or logic bombs; by downloading, creating or using any program, tool or item of software designed to monitor damage, disrupt or interfere with the functioning of ICT Facilities, user accounts or data.

Effecting security breaches or disruptions of network communication, including, but not limited to, accessing or modifying data (or data headers) of which the  user  is  not  an intended recipient or logging into an ICT system or service, or account, that the user is not expressly authorised to access.  Disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.

Acting in any way that directly or indirectly causes disruption to others' use of School ICT Facilities or using ICT Facilities to disrupt or deny the use of ICT Facilities of third parties at any time.

**This is not an exhaustive list but merely an indication of the types of conduct that could come under the heading of inappropriate. Failure to follow this policy may result in disciplinary action up to and including dismissal. It may also lead to criminal or civil action.**

## ICT Monitoring

The School may monitor the usage of any or all ICT Facilitates and has access to reports on any internet sites that have been visited.

# Learner Acceptable Use Policy Agreement (KS3-KS4)

ICT is seen as beneficial to all members of the School in supporting learning, teaching, research, administration and approved business activities of the School. The School's ICT Facilities provide a number of integral services and, therefore, any attempt to misuse a computer system could cause significant disruption to other users at the academy.

This Acceptable Use Agreement is intended
to ensure:

- that all users, will be responsible and stay safe while using ICT devices, systems and services.

- that School devices, systems, services and users are protected from accidental or deliberate misuse that could put the security of these systems and users at risk.

**AGREEMENT**

I understand that I must use School systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

When using the School's ICT
Facilities:

- I understand that the School systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have prior permission;

- I understand that the School may monitor my use of the devices, systems, services and communications at any time, and that I am not provided with personal private data storage;

- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it;

- I will not disclose or share personal information about others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.…);

- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online;

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes);

- I will respect others' work and property and will not access, copy, remove or otherwise use or alter any other user's files, without the owner's knowledge and permission, and I will ensure that any use is in accordance with the School's policies;

- I understand there are risks when using the systems and services, and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials;

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions;

- I will respect copyright of materials and intellectual property rights and not take or distribute text, images or other materials without permission;

- I will not record, photograph, or otherwise capture the content of a computer in any way, without permission;

- I will not use or modify any of the School devices, systems and services in any way that will disrupt their use for others in any way;

- I will not install or attempt to install or store programmes of any type on any School device, nor will I try to alter computer settings;

- I understand that I am not permitted to attempt to connect any devices or systems (e.g. laptops, mobile phones, USB devices, etc.…) to any School devices, systems or services without prior permission from an Authorised Person within the School. I understand that, if I am permitted to use my own devices in the School I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

I understand that I am responsible for my actions, both inside and outside of the School:

- I understand that the School also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the School and where they involve my membership of the School community (for example, cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action.  This may include loss of access to the

School ICT systems and services, disciplinary action as set out in the codes of conduct and in the event of illegal activities involvement of the police.

I agree to follow these guidelines at all times when:

- using or connected to the School's devices, systems and services;

- using my own equipment inside or outside of the School in a way that is related to me being a member of this School (for example, communicating with other members of the School, accessing School email, websites and services, etc.…).

**I have read and understand that use of the School IT systems and devices is governed by the full Acceptable Use Policy and all of the policies available from the School's website [www.ladynafisa.org.](www.ladynafisa.org)**

**Print Name** ................................................................

**Signed** ...............................................................

**Date:** ...............................................................

Parents and Carers should sign below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to the School's ICT Facilities.

**Print Name (parent):** ...............................................................

**Signed (parent):** ...............................................................

**Date (parent):** ...............................................................