Isle of Wight Education Federation

The Governing Board of the Isle of Wight Education Federation

ICT Acceptable Use Policy

Author	Mark Overy Josh Collins
Approved by	Full Governing Board
Approval date	January 2023
Review frequency	Annually
Next review	January 2024

Revision History

Revision	Change	Date
1.0	Initial Document Recovered	11/08/2021
1.1	Amendments based on system changes	13/01/2022
1.2	Minor Amendments	24/11/2022
1.3	Major Review	06/12/2022

1. Introduction

The purpose of this document is to outline the acceptable use of the Federation's Information and Communication Technology platforms, both on and offsite. Guidance for appropriate use and examples of inappropriate use will be referenced but will not be an exhaustive list. This document is intended to protect all parties: students, staff, visitors and anyone given access to the IWEF ICT System.

2. Term Definitions

Throughout this document there will be reference of certain terms, their definitions are below:
Staff - An employee of the Isle of Wight Federation
Student - an individual who attends any one of the three Federation sites for accessing education
Network User - A user with access to the system infrastructure or core services
Personal Device - A mobile device, such as a laptop or mobile phone, that is not owned by the Federation
Company Owned Device - A mobile device, such as a laptop or mobile phone, that is owned by the Federation

3. Roles and Responsibilities

The Federation's ICT provision is used for a wide range of resources, applications and access to third party resources. As a result, responsibilities for the data being accessed are shared between the most appropriate departments and individuals.

The ICT Department will:
Ensure that access to Education based resources is available via a secure and efficient system, whether these resources are held/stored onsite or within cloud based platforms. Changes to the system and wider network access changes require a review of this, and other ICT related Policies, to ensure they are up to date and accurate at the time of review. The ICT Department is responsible for ensuring staff are aware of their roles and responsibilities with regards to Appropriate Use of the ICT Systems and that all users have evidenced a signed version of this policy before granting access to the system and third party services. An accurate and efficient overview of the Federation's web filter is to be maintained and breaches reported to appropriate Faculty members.

Staff will:
Ensure all guidance within this policy, the Cyber Security Policy and E-Safety Policy are being followed at all times when operating within the Federation's ICT System; extended guidance and examples are in the latter part of this document. Staff must ensure students under their supervision are aware of and understand this Policy, have signed this agreement and are familiar with the rules and regulations in place relating to this Acceptable Use Policy, the Cyber Security Policy and E-Safety Policy. It is the responsibility of the Staff to report any potential breaches of this agreement by colleagues or students to the Helpdesk.

Students will:
Adhere to the guidelines specified in this document and understand that breaches of this can result in disciplinary actions and network access being revoked. Ensure that this policy, as part of the New Starter Pack, has been read, understood, signed and returned to their Head of Year before being given access to the network and wider systems in place. Raise concerns regarding potential breaches, either by fellow students, or inappropriate material being accessible to members of the Federation's ICT System.

All users will:
Understand that any breaches to the guidelines or attempts to bypass the school's security systems can result in network access being revoked indefinitely, if proven. Agree to the fact that the Federation reserves the right to examine or delete any files that may be held on its system and related cloud storage platforms, along with monitoring all aspects of live computer use and/or internet sites visited - with or without staff/student permission.

Isle of Wight
Education Federation

Acceptable use of Computers and Internet Guidance for Staff

Desktop computers on site along with Company Owned Devices are provided for the primary purpose of accessing work related data and applications in a secure manner. The use of such devices are to be used for work related purposes only and the storage of work related information only, not personal data. Using the Federation's ICT system for personal and/or private business use is strictly prohibited and the Federation reserves the right to remove files stored within its on-site or cloud storage platforms that are deemed for personal use. A list of additional guidelines around appropriate and inappropriate use of the Federation's system is as follows. Please note, this is not an exhaustive list.

- All computer use and internet activity should be appropriate to the member of staff's employment
- Access can only be made via your authorised account and password, using an authorised computer
- Your login credentials must not be shared with any other individuals
- As per the Cyber Security Policy, passwords must be routinely changed
- Activity that threatens the integrity and security of the Federation's ICT system, or activity that attacks/corrupts our/other systems is forbidden and is a criminal offence
- All communications to parents/students/carers/visitors must be via the Federation's primary systems, such as Google Mail or SchoolComms, social media contact is not permitted
- Users are responsible for all emails sent and accept that these will be open to scrutiny
- Access to sensitive data stored within the Federation's chosen cloud storage platform must only be accessed via desktop PCs on site or a staff issued company-owned device and authenticated with two Factor authentication. Any attempts to access such data outside of these sources is forbidden
- Use of the Federation's system for personal/financial gain is forbidden, as is gambling/betting etc.
- Use of the Federation's computer system to access inappropriate materials such as pornographic, racist or other offensive materials is forbidden
- Staff access to the WiFi is only available using company-owned devices that have been issued to specific staff members and enrolled to a cloud mobile management system, such as InTune or Google's MDM
- Great care should be taken with giving personal details such as addresses, telephone numbers, bank details etc.
- Personal contact details should never be given out in unregulated situation such as chat rooms
- General Data Protection Regulations (GDPR) and the Computer Misuse Act 1990 apply to all uses of the computers
- If staff are are caught misusing the computer network, the Federation is obliged to take action according to the severity of the offence
- Cyberbullying is considered an offence and will result in the same sanctions as other staff bullying incidents
- Any attempts to download, and run, potentially harmful or malicious software will result in action being taken in line with the severity of the attempt
- Programs/software brought in from home and attempting to be installed on the Federation's ICT System is not permitted
- USB mass storage devices are not permitted for staff use, data must only be shared within the Federation's cloud storage platforms and using the chosen services, such as Google Workspace or O365
- Attempting to login with another member of staff's username/password can result in disciplinary action
- Personal devices are not permitted to be joined to the network unless explicitly authorised and vetted in advance, this applies to staff arranging for visitors/speakers to attend the College sites
- Staff must have read and understood both the IWEF Cyber Security Policy and the IWEF E-Safety Policy
- This form and agreement must be signed on an annual basis for all members of staff without exception

Full Name:

Signed:

Date:

Acceptable use of Computers and Internet Guidance for Students

Students have access to a number of desktop computers on site, banks of shared Chromebooks, individually configured Chromebooks (for specific students) and their personal devices at home. All of these can be used for the purpose of accessing education and Federation related data and applications. The use of any company owned device is to be for educational related purposes only and the storage of school/learning related information only, not personal data. Using the Federation's ICT system for personal use is strictly prohibited and the Federation reserves the right to remove files stored within its on-site or cloud storage platforms that are deemed for personal use. The ICT Department will not take part in any troubleshooting or technician support on a personal device outside of the scope of simply enabling access to the school WiFi for students at The Island VI Form and take no responsibility for these devices or potential damage/loss of data that could incur as result of a plethora of reasons, many outside of the Federation's control.

A list of additional guidelines around appropriate and inappropriate use of the Federation's system is as follows. The use of student's own personal devices is not monitored by the Federation. Please note, this is not an exhaustive list.

- All Federation owned computer use and internet activity should be appropriate to the student's educational and learning needs
- Access can only be made via your authorised account and password
- Your login credentials must not be shared with any other individuals
- Activity that threatens the integrity and security of the Federation's ICT system, or activity that attacks/corrupts our/other systems is forbidden and is a criminal offence
- All communications to teachers must be via the Federation's primary systems, such as Google Mail or Google Classroom, social media contact is not permitted
- All users are responsible for all emails sent and accept that these will be open to scrutiny
- Use of the Federation's system for personal/financial gain is forbidden, as is gambling/betting etc.
- Use of the Federation's computer system to access inappropriate materials such as pornographic, racist or other offensive materials is forbidden and will result in appropriate sanctions, including internet access being revoked and, if deemed necessary, complete network access being revoked
- Attempts to bypass the Federation's web filtering system, either successful or unsuccessful, will result in appropriate sanctions
- Student access to the WiFi is only available to those enrolled at The Island VI Form
- General Data Protection Regulations (GDPR) and the Computer Misuse Act 1990 apply to all uses of computers
- If students are are caught misusing the computer network, the Federation is obliged to take action according to the severity of the offence
- Cyberbullying is considered an offence and will result in the same sanctions as other student bullying incidents
- Any attempts to download, and run, potentially harmful or malicious software will result in action being taken in line with the severity of the attempt
- Programs/software brought in from home and attempting to be installed on the Federation's ICT System is not permitted
- USB mass storage devices are permitted for specific student level access, such as exams or Creative Arts coursework. This is only an alternative to the primary source of data within the Federation's cloud storage platforms and using the chosen services, such as Google Workspace or O365
- Attempting to login with another member of student's username/password can result in disciplinary action
- Students must be aware of their role and responsibilities in terms of E-Safety
- This form and agreement must be signed before access will be granted to the ICT system

Full Name: Tutor Group: Year:

Signed [Student]: Date:

Signed [Parent]: Date: