UWC IT POLICY

QUALITY POLICIES

KORAMBAYIL AHAMED HAJI MEMORIAL UNITY WOMEN'S COLLEGE

MANJERI, MALAPPURAM, KERALA, INDIA.

INTERNAL QUALITY ASSURANCE CELL

UWC IT Policy

The IT policy ensures the efficient and secure use of technology resources on campus. This policy applies to all students, faculty, staff and any other individuals or entities granted access to IT resources. It addresses various aspects of IT, including hardware and software usage, network security, data protection and acceptable use.

General Responsibilities

- **Responsible Use**: All users must use IT resources in a responsible and ethical manner.
- **Minimal Personal Use**: Personal use of college IT resources should be minimal and must not interfere with academic or work-related activities.

Access and Security

- **Wi-Fi Usage**: Students may use the student Wi-Fi access points on campus solely for academic purposes.
- **Unauthorized Access**: Access to computer labs, the Network Research Centre and other resources without permission is strictly prohibited.
- **Account Security**: Users are responsible for maintaining the security of their accounts, passwords, and devices. Passwords should be complex and updated regularly.
- **Reporting Incidents**: Users should report any suspected security breaches, lost or stolen devices, or other security incidents to the relevant office or administrators immediately.

Software and Hardware Usage

- **Authorized Use**: Software and hardware must be used for their intended purposes. Installation of unauthorized software or hardware is not allowed.
- **Integrity of Resources**: Users should not engage in activities that may harm the integrity, security, or performance of the college network, website, or other applications.

Social Media Guidelines

- **Official Communications**: Social media accounts created on behalf of the college should be registered using official college email addresses and contact information.

- **Account Administration**: Account administrators should be designated and approved by college administration or relevant department heads. Administrators must ensure that login credentials are securely stored and accessible only to authorized personnel.
- **Content Sharing**: Content shared on college-affiliated social media accounts should align with the college's mission, values and strategic objectives. Confidential or sensitive information, including financial data and personally identifiable information, should not be shared on social media.
- **Monitoring**: Social media accounts should be regularly monitored for inappropriate or offensive comments, which should be removed or hidden as necessary.

Compliance and Review

- **Policy Violations**: Violations of this IT policy may result in disciplinary actions, including but not limited to loss of access privileges, suspension, or legal action as appropriate.
- **Policy Review**: This IT policy will be reviewed regularly to ensure its relevance and effectiveness. Any proposed changes to the policy will be subject to approval by the relevant college authorities.