



**COMMUNICATION  
POLICY FOR STAFF  
(2025-26)**

## **Effective online communication for staff**

Employee safety should be a priority in every workplace, and a subject that all workers should be well educated on. Creating a safe workplace is the responsibility of both employer and employee, and the best way to achieve this is to ensure that your workplace safety procedures and protocols are communicated effectively throughout the entire company.

### **Purpose**

The purpose of the school's online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that International Indian School is a safe and secure environment.
- Safeguard and protect all the members of the International Indian School community.
- Raise awareness to all members of the International Indian School community regarding the potential risks as well as benefits of technology.
- Enable all staff to work safely and responsibly, to role model online positive behavior and to be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all staff including the governing body, teachers, support staff, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents

## **Guidelines for Effective Email Communication**

- If sender has CC'ed other people in the mail, use REPLY ALL to not lose them in the replies.
  - In case of replying to a broadcast mail addressed to a mail group for bulk communication, do not reply to all, but only to the sender of the mail.
  - Include only the relevant people in each thread.
- If it's a routine task, higher officials need not be CC'ed unless asked for.
  - Know the organization structure to understand who all are relevant
- Don't let your emotions reflect in an email.
  - It's a formal and permanent record.
  - Can be misinterpreted by whosoever is reading it.
  - Avoid replying to/sending emails when you are in a bad mood.
- Reply to email threads/conversations pertaining to the same topic.
  - Don't compose fresh mail as a reply every time.
  - Helps in maintaining context of the discussion.
- Start using/considering emails as primary mode of communication.
  - When a person sends an email, he/she expects a reply/acknowledgement.
  - Don't expect follow-up/additional calls.
  - Reply at the earliest.
- Avoid using SMS language, shortened forms, and different colour/font/styles unnecessarily.
  - Standard abbreviations are acceptable
- Arrange and organize your inbox.
  - Create & use labels effectively.
  - Keep unread mails to the minimum.
- Always read through your mail one last time before sending.
  - This will minimize typos and miscommunication
  - Will aid in including any points that have been missed initially.

- Always send emails with a relevant & precise subject line, do not send emails without a subject line, ineffective subject lines such as Hi, questions, please note and so on.

## UAE NATIONAL GUIDELINE FOR ONLINE COMMUNICATION

Telecommunications and Digital Government Regulatory Authority (TDRA) implements the Internet Access Management Regulatory Policy (PDF, 500 KB) in the UAE, in coordination with Media Regulatory Office (MRO) and Etisalat and Du, the licensed internet service providers in the UAE.

TDRA monitors online content available to users in the UAE and will notify website operators based in the UAE of any potential breaches of the IAM policy. TDRA, in its enforcement of IAM, also monitors online advertising, including the advertising of medical and other specialised products and services.

Etisalat and Du are required to block online content if so is requested by TDRA. Categories under which content is restricted by virtue of the IAM policy are:

- bypassing blocked content
- pornography, nudity and vice
- impersonation, fraud and phishing
- insult, slander and defamation
- invasion of privacy
- offences against the UAE and the public order
- supporting criminal acts and skills
- drugs
- medical and pharmaceutical practices in violation of the laws
- infringement of intellectual property rights
- discrimination, racism and contempt of religion
- viruses and malicious programs
- promotion of or trading in prohibited commodities and services
- illegal communication services
- gambling
- terrorism

- prohibited top level domains
- illegal activities
- any content prohibited upon order from judicial authorities, or in accordance with the law.

#### Prohibited media content in the UAE

The UAE sets national standards for media content and requires all local mass media institutions operating in the UAE to abide by them. These include:

- to respect the regime of the United Arab Emirates, its symbols and the political system
- not to offend the divine and Islamic beliefs, and show respect to other religions
- to respect the culture and heritage of the UAE
- not to offend national unity nor social cohesion and/or incite up sectarian, regional and tribal conflict
- to respect directions and policies of the UAE at the domestic and international levels
- not to harm the economic system of the country, nor spread rumours, misleading and biased news
- to respect the government policies to promote national identity and the integration of citizens in the media labour market
- to respect the principles and codes of ethics of media work
- not to publish or broadcast information harmful to children, women and other social groups, or that would incite others toward hatred and violence
- to respect the copyright rules and regulations
- not to disclose official confidential contacts, military matters or conventions or treaties concluded by the government without proper authorisations

- not to report distorted proceedings and deliberations of courts or other regulatory bodies
- not to disclose information on a criminal investigation, which has not been concluded and/or ordered to be confidential
- not to publish news, photographs, comments which invade privacy of individuals and families or destroy reputation
- forging, fabricating documents or presenting incorrect news with bad intent
- material which harms the national currency or causes a confusion over the economic situation in a country
- newsletters or advertisements, which include expressions, photographs, or drawings that are in violation of public morals or may confuse the public
- defaming public officials
- investigations which deal with more than one party, without giving an account of the views of all parties directly concerned.

Laws for using social media

**Federal Decree Law No. 34 of 2021 on Combatting Rumors and Cybercrimes**

**Regulation of Using Social Media by the Employees of Federal Entities as Approved by the Cabinet Resolution No. 73/3/ & 1 of 2014**

**Federal Decree Law No. 2 of 2015 on Combating Discrimination and Hatred**

## ONLINE SAFETY INCIDENT/ BEHAVIORAL REPORTING MECHANISM

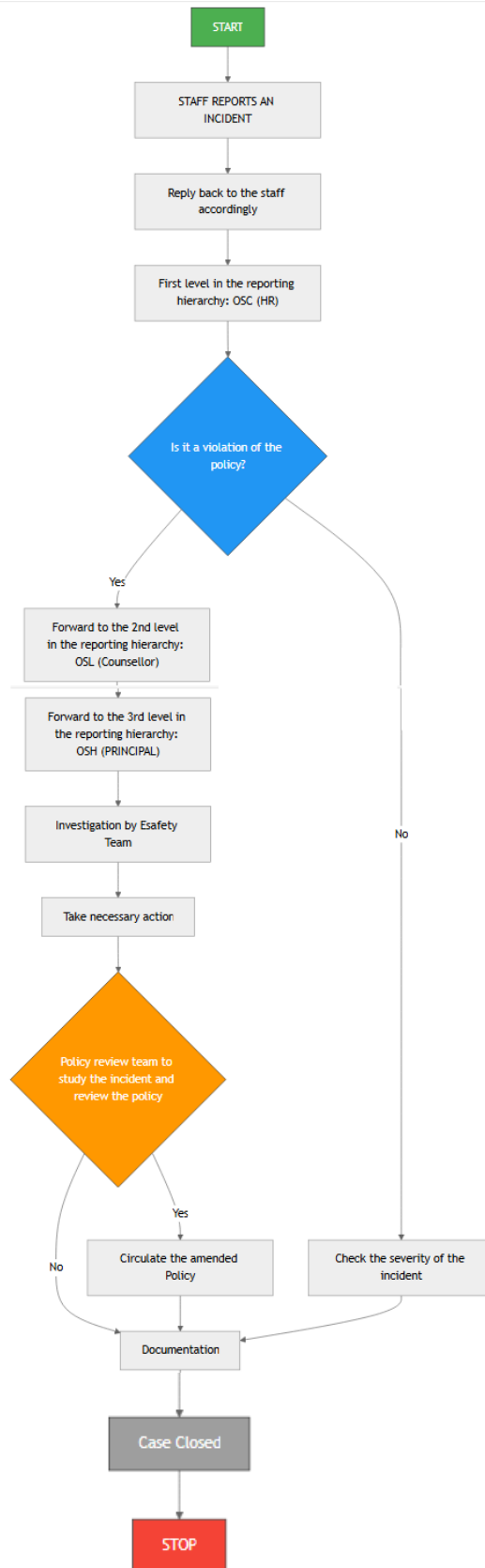
An incident regarding online safety and/or behavioral/bullying can be reported to the concerned through the Employee Service Portal of all staff.

This should be dealt with high confidentiality involving only the concerned and the required actions shall be taken keeping all the matters and staff involved professional and cordial. Before closing the case, the policy review team should study the incident and see if any amendments need to be made in the related policy. In case the same is done, the amended policy should be circulated to all staff with a brief training on the same.

The Employee Service Portal (ESS) where staff can report their incidents:

The screenshot displays the 'Employee Self Service' portal for 'HABITAT SCHOOL AL TALLAH'. The page title is 'Employee Self Service' and it includes a 'Welcome' message and a 'Logout' link. The main navigation menu on the left includes: Home, My Request, Leave, Purchase, IT Help Desk, Photocopying, Incident Reporting, Suggestions, Other Request, End of Service Request, My Profile, Reports, and Tools. The 'Incident Reporting' form is active, showing the following fields: RefNo: 1004, Date: 10/11/2025, Status: New, Requested By: [Redacted], Incident: Online Safety (selected from a dropdown), and Incident Details: [Redacted] (maximum 500 chars). A 'Submit' button is located at the bottom of the form.

# The Reporting Mechanism flowchart will be a



## **Impact of Online safety policy and practices.**

The impact of the online Safety policy and practices will be evaluated and reviewed by the Online Safety Group (OSG) along with the Online Safety Leader (OSL). This will be reviewed yearly through surveys of staff and also regularly audited based on online safety incident logs, behavior/bullying log's as and when report

