What is Authentic Content?

Being authentic means that you act in ways that show your true self and how you feel. Rather than showing people only a particular side of yourself, you express your whole self genuinely. That means to succeed in being authentic, you first have to know who your true self actually is.

There is difference between **Authentic** and **Original**. Original is termed relating to the origin or beginning, preceding all others.By definition, Authenticity is being real, or genuine. This is definitely what you should be trying for on social. Even though everyone plays the whole keeping-up-appearances game on social media, authenticity comes naturally to a lot of people on their personal profiles—even if they aren't being entirely authentic.

Our belief of self – accountability of Users and Community for their posts and statements or any other aspect which gets posted on our App / Website prescribes Authenticity Standards. As said that Authenticity creates a safe place and inspires loyalty and engagement, we place high emphasis on ensuring compliance by Users and Community to our Authenticity Standards.

We strictly prohibit any content which includes any of the following:

- Fraudulent Content / Unwarranted Content
- Misrepresentation
- False Content
- Manipulated Content
- Unauthorized Content
- Any Content which is Prohibited Content / Restricted Content covered under our "**Prohibited Content Policy**"
- Inauthentic behavioral content

This additionally covers below (Hosting, Display, Upload, Modification, Publish, Transmit, Store, Update and Share information):

- belongs to another person and to which the user does not have any right;
- is defamatory, obscene, pornographic, paedophilic, invasive of another's privacy, including bodily privacy, insulting or harassing on the basis of gender, libelous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force;
- is harmful to child; infringes any patent, trademark, copyright or other proprietary rights;
- violates any law for the time being in force;
- deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact;
- impersonates another person;

- threatens the unity, integrity, defense, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting other nation;
- contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;
- is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person

1. **<u>Fraudulent Content / Unwarranted Content / Misrepresentation</u>**

   With the fast pace of life and advancement in technology, people rely more on social networking sites for the happenings around the globe. The misinformation or rumors spread across especially during emergency situations such as Pulwama Attack 2019 or The Attack of 26/11 or a natural calamity like the Kerala Flood 2018 can have a devastating effect on individuals and society. Spurious news in such a scenario would not only give rise to panic among the individuals but in some cases, it may also target particular community.

   As per legal framework, fraud is intentional deception to secure unfair or unlawful gain, or to deprive a victim of a legal right. Fraud can violate civil law (i.e., a fraud victim may sue the fraud perpetrator to avoid the fraud or recover monetary compensation), a criminal law (i.e., a fraud perpetrator may be prosecuted and imprisoned by governmental authorities), or it may cause no loss of money, property or legal right but still be an element of another civil or criminal wrong.

   The falsification of documents, known as forgery, and counterfeiting are types of fraud involved in physical duplication or fabrication. The "theft" of one's personal information or identity, like one finding out another's KYC and then using it as identification, is a type of fraud. Fraud can be committed through and across many media including mail, wire, phone, and the Internet (computer crime and Internet fraud).

   We prohibit posting of an untrue statement of a material fact made by one party which affects the other party or have an influential impact.

   It includes any of the following:

   - False statement of the fact / content
   - Any statement or view which is Half Truth
   - Any statement or view which becomes false in future course of action

- Any statement or view which is made in fraudulent manner with an intention to deceive the other / viewers
- Any statement or view which is made without fraudulent manner but with negligence of facts
- Any statement or view which is misrepresented with innocence

We (Open IND Networks operating as a brand SUFFRAGE) have adopted zero tolerance policy against any content which is a Fraudulent Content.

We strictly prohibit any content which is posted by any User / Community:

- By creating a Fake ID over our App / Website (Irrespective of malafide / bonafide intention of individual / community)

  This can be in any of the forms:

  - Creation of ID in name of person non – existent
  - Creation of ID in name of person whom you know but you have created and operating his ID without knowing him
  - Creation and Operating ID on behalf of any person who is major
  - Creation of ID by giving false Personal details
  - Creation of ID by giving personal details of any other person (with / without his knowledge)
  - Maintenance of multiple accounts without any authentic reason (This can be justified in exceptional cases)
  - Evading requirements mentioned in Terms of Service

  Personal details can be referred herein as Date of Birth, Email, Phone No, Age, Name or any other personal details required mandatorily for creation of ID on App / Website.

- Any statement / content posted with an intention to pretend which includes:
  - Use of Image / Videos with an intention to deceive other person (Users)
  - Creation of Page / Link informing it is meant for a person who is not in existent
  - Creation of Page / Link informing it is meant for a person who is unaware of such things or not authorized you to do so
  - Creating / Posting anything pretending you are authorized for such thing but actually you are not
  - Creation / Posting of anything which causes harm / risk to viewers / users

The above list is indicative list and the same is case specific which is subject to additions. Our back - end team continuously monitors activity and it also depends upon intent of User for any post.

2. **Spam**

We strive continuously to restrict any content which is unwanted, intrusive, and irrelevant. Any content that is not created with an intention of serving viewers / users.

As per CISCO Systems, % analysis of Spam was as below (Source: Wikipedia - https://en.wikipedia.org/wiki/Spamming)

Rank	Country	Spam (Volume) (in %)
1	India	13.7
2	Russia	9
3	Vietnam	7.9
4	South Korea	6
	Indonesia	6
6	China	4.7
7	Brazil	4.5
8	USA	3.2

With such volume, we have certain guidelines to be followed by Users and expect strict adherence by Users for the same. The list mentioned below is inclusive list and not exhaustive list.

- **Bulk submissions** are a set of comments repeated multiple times with the same or similar text. These messages, also called as spam-bombs, can come in the form of one spammer sending out duplicate messages to a group of people in a short period of time, or many active spam accounts simultaneously posting duplicate messages. Bulk messages can cause certain topics or hashtags to trend highly. For example, in 2009, large number of spam accounts began simultaneously posting links to a website, causing 'ajobwithgoogle' to trend.
- **Profanity** User-submitted comments that contain swear words or slurs are classified as profanity. Common techniques to circumvent censorship include "cloaking", which works by using symbols and numbers in place of letters or inserting punctuation inside the word (for example, "w.o.r.d.s" instead of "words"). The words are still recognizable by the human eye, though are often missed by website monitors due to the misspelling.
- User-submitted **insults** are comments that contain mildly or strongly insulting language against a specific person or persons. These comments range from mild

name-calling to severe bullying. Online bullies often use insults in their interactions, referred to as cyber bullying. Hiding behind a screen name allows users to say mean, insulting comments with anonymity; these bullies rarely take responsibility for their comments and actions.

- User-submitted **threats** of violence are comments that contain mild or strong threats of physical violence against a person or group.
- User-submitted comments can include **malicious links** that will inappropriately harm, mislead, or otherwise damage a user or computer. These links are commonly found on video entertainment sites. When a user clicks on a malicious link, the result can include downloading malware to the user's device, directing the user to sites designed to steal personal information, drawing unaware users into participating in concealed advertising campaigns, and other harmful consequences. Malware can be dangerous to the user, and can manifest in several forms: viruses, worms, spyware, Trojan horses, or adware.
- **Fake Connects** occurs when several fake accounts connect or become “friends”. These users or spam bots often try to gain credibility by following verified accounts, such as those for popular celebrities and public figures. If that account owner follows the spammer back, it legitimizes the spam account, enabling it to do more damage.
- User-submitted comments that inappropriately display full names, physical addresses, email addresses, phone numbers, or credit card numbers are considered leaks of **personally identifiable information**
- Any content which mandatorily require reply to post in form of like / share etc.
- **Impersonation** is when someone pretends to be another person. E.g. You post any content as you are Police Officer (in reality you are employee in private sector). The website pretends to be a reputable brand or service by using a name, domain or content featuring typos, misspellings or other means to impersonate well-known brands E.g. RBLbank.com is replaced with name as rblbnak.com
- **Misleading User interface which results in accidental traffic generation**
- Any post which has impact / relevance to **Branded content** i.e. It may only be posted by accounts and Pages, groups and profiles with access to the branded content tool. We define branded content as a creator or publisher's content that features or is influenced by a business partner for an exchange of value.

3. Imitative / Inauthentic behavior

With reference to our Authenticity Standards, we do not permit Users for any misrepresentation. The standards are created for ensuring trust of our Users.

This includes any of the below categories:

- Use of multiple accounts for sharing of accounts
- Incorrect use of our reporting mechanism w.r.t. to Prohibited Content, Restricted Content
- Concealment of any information about post / page with a malafide intention
- Any act which represents fraudulent activity / mis-representation mentioned above
- Misleading people about identity of User / self
- Misleading people about ownership of account / page
- Misleading people about purpose of account / page
- Misleading people about origination of post / content
- Any behavior which is done with an intention of evasion of guidelines, policy and standards

The above list is indicative list and the same is case specific which is subject to additions. It also depends upon intent of User for any post.

4. Media manipulation

It includes image, video, audio or any combination (such as audio and video OR image and audio etc.)

Media Manipulation tactics may include the use of logical fallacies, psychological manipulations, outright deception (disinformation), rhetorical and propaganda techniques, and often involve the suppression of information or points of view by crowding them out, by inducing other people or groups of people to stop listening to certain arguments, or by simply diverting attention elsewhere.

We remove any content brought to our notice which includes media manipulation through multiple ways. The below is inclusive list for understanding of Users.

- **Astroturfing**
  Astroturfing is when there is an intent and attempt to create the illusion of support for a cause, person, or stance. While this is mainly connected to and seen on the internet, it has also happened in newspapers during times of political elections. Corporations and political parties try to imitate grassroots movements in order to sway the public to believing something that isn't true.

- **Clickbait**
  Clickbait refers to headlines of online news articles that are sensationalized or sometimes completely fake. It uses people's natural curiosity to get people to click. In some case clickbait is simply used to generate income, more clicks means more money made with advertisers.

- **Propoganda Laundering**

  Propaganda laundering is a method of using a less trusted or less popular platform to publish a story of dubious origin or veracity for the purposes of reporting on that report, rather than the story itself. This technique serves to insulate the secondary more established media from having to issue a retraction if the report is false. Generally secondary reports will report that the original report is reporting without verifying or making the report themselves.

- **Search Engine Marketing**

  In search engine marketing websites use market research, from past searches and other sources, to increase their visibility in search engine results pages. This allows them to guide search results along the lines they desire, and thereby influence searchers.

  Business have many tactics to lure customers into their websites and to generate revenue such as banner ads, search engine optimization and pay-per-click marketing tools. They all serve a different purpose and use different tools that appeal to multiple types of users. Banner ads appear on sites that then redirect to other sites that are similar. Search engine optimization is changing a page to seem more reliable or applicable than other similar pages. Pay-per-click involves certain words being highlighted because they were bought by advertisers to then redirect to a page containing information or selling whatever that word pertained to. By using the internet, users are susceptible to these type of advertisements without a clear advertising campaign being viewed.

- **Distraction by major events**

  Commonly known as "smoke screen", this technique consists of making the public focus its attention on a topic that is more convenient for the propagandist. This media manipulation has been referenced many times in popular culture.

- **Distracting the Public**

  This a mere variation of the traditional arguments known, in logic, as ad hominem and ad populum but applied to countries instead of individuals. This technique consists on refuting arguments by appealing to nationalism or by inspiring fear and hate towards a foreign country or to all the foreigners. It has the potential of being important since it gives the propagandists the power to discredit any information coming from other countries.

- **Image Manipulation**

Visual media can be transformed through photo manipulation, commonly called "photoshopping." This can make a product, person, or idea seem more appealing. This is done by highlighting certain features on the product and using certain editing tools to enlarge the photo, to attract and persuade the public.

- **Video Manipulation**

  Video manipulation is a new variant of media manipulation that targets digital video using a combination of traditional video processing and video editing techniques and auxiliary methods from artificial intelligence like face recognition. In typical video manipulation, the facial structure, body movements, and voice of the subject are replicated in order to create a fabricated recording of the subject. The applications of these methods range from educational videos to videos aimed at (mass) manipulation and propaganda, a straightforward extension of the long-standing possibilities of photo manipulation. This form of computer-generated misinformation has contributed to fake news, and there have been instances when this technology was used during political campaigns.

The above list is indicative list and the same is case specific which is subject to additions.

5. **Memorialization**

   Memorialization generally refers to the process of preserving memories of people or events. In case of demise of person, we receive requests from relatives or friends for memorialization of account.

   Once the memorialization is tagged against account, the word “XXXXX” appears to clarify viewers and users which also prevents from unauthorized logins and fraudulent activities.

   For further clarity, please refer **Account Management Policy**.

6. **Falsification of news**

   Declining the spread of news which are inaccurate is our responsibility and we take it seriously. We understand that this being a sensitive issue and factor determining action of Users / Viewers, we prefer to keep people informed with news which are accurate enough and not false.
   There is also a thin line between false news and satire or opinion. And because of this, there may one find news which are not accurate present on our App / Website.

   We are building a platform for publishing accurate news and keeping viewers and users informed by means of following:

- Channel Partner Authenticity
- Ensuring compliance to SUFRAGE Policy guidelines in publishing of news

7. **Cyber Security**

In general, Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as information technology security or electronic information security.

Cybersecurity is important because it encompasses everything that pertains to protecting our sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems from theft and damage attempted by criminals and hackers.

Cybersecurity risk is increasing, driven by global connectivity and usage of cloud services, to store sensitive data and personal information. Widespread poor configuration of cloud services paired with increasingly sophisticated cyber criminals means the risk that your organization suffers from a successful cyber - attack or data breach is on the rise.

Gone are the days of simple firewalls and antivirus software being your sole security measures. Business leaders can no longer leave information security to cybersecurity professionals.

Therefore, we are concerned and this being our utmost priority to ensure cybersecurity.

We have narrated below is a list of few indicators which are harmful and against cybersecurity:

- Access to User account without consent or knowledge of User irrespective of intention
- Extracting Personal Sensitive Information as per GDPR and Date Protection Act of India without consent or knowledge of User
- Depicting User for downloading of unauthorized content
- Accessing the emails / accounts of Users and posting of contents or extracting information of other users through said list
- Any phishing attack
- Any compromise to gain full access to software license which can be sold over dark web
- Any attempt of identity theft
- Public sharing of login credentials of self or third party

- It also includes any act of User towards Denial of Service Attack, Eavesdropping Attack, URL Interpretation, File Inclusion attacks, Session Hijacking, Brute force & Dictionary attack, Domain Name System (DNS) Spoofing, Injection attacks etc. (or any other wherein intention to gain access to Personal Sensitive Data by any means of Users for unauthorized intentions)

In case of any further clarifications, you may refer **Limited Liability Policy Guidelines**.

Changes in Authentication Standards

Date of Change	**Nature of Change**	**Effective Date and Version**