User
Protection
Commitment

1. Moderation

Content Moderation

Ti strives to be a safe space for expression, sharing, and learning. We do not have strict guidelines as to what is *acceptable* to post, that is determined by the community. However, we have a strict and adhered to policy when it comes to what is not allowed.

We recognise that as a social network, we are exposed to the platform being misused, which can come in many forms. The types of content that we actively remove from Ti is anything that contains hate speech, racism, or violence. We also monitor for and manage bullying on the platform, and discrimination against a person's physical, mental, and emotional well-being. Any false or misleading information is removed, as are links leading to scams or malware threats.

Social media companies have inherited a similar role to broadcast news in serving as information gatekeepers; they have not however, taken on the responsibilities associated with the role, leading to the spread of misinformation on platforms that do not effectively moderate content, which can ultimately threaten people's safety.

We recognise the role of Ti as essentially a publication, and that through moderation, what is acceptable and what is not acceptable is determined. We strive to have as diverse a team of moderators as possible, representative of everyone on the LGBTQIA+ spectrum. They will determine what is unsuitable and harmful, collectively but each with the influence of their own queer background.

Moderation Methods

Reactive moderation on Ti means all users can participate in flagging down content that they believe is harmful or incorrect, allowing the moderators to review it and stop its spread.

All new users will be subject to a *post-moderation* process - posts and comments will be published automatically and are subject to moderation in a 24-hour window. If a user doesn't raise any flags, their posts will no longer be subject to post-moderation, but remain subject to routine sweeps and the reactive moderation done on the platform. If a user is flagged by post-moderation as violating Ti's rules and policies, they will be subject to *pre-moderation* - posts and comments will undergo review before appearing on the platform.

Groups are subject to an additional layer of moderation in the form of *self-moderation* - group admins are required to review posts made within the group before they appear. Finally, certain automated methods of moderation exist on the platform to catch certain links and types of imagery and videos that are recognised as harmful.

Our Moderators

At Ti, we recognise that attention and regular mental health check-ins are needed for the people tasked with routinely handling negativity and conflict. The care we have for our users is shared with our staff, and the side-effect of moderating for the safety of our users is the toll it can take on our own.

We have an open conversation culture amongst the moderators and managers, allowing for discussion about what is being seen and digested on a daily basis, support for those having difficulty, and generally for managing this task together. If any of the content our staff are moderating is upsetting to them, and it relates to them personally, they pass the responsibility on to another moderator who will be better able to manage it. We also limit moderation shifts to no more than four consecutive hours and have schedule flexibility for those who need to take time to recover after a particularly affecting incident.

2. Data

Ti upholds itself to a commitment of data protection for all users and imposes strict data protection policies. Privacy controls on the platform itself are clearly signposted and easy to use, and the only user data required to use the platform is a username.

Data Usage and Access

No personal, behavioural, demographic, post, or any manipulation of them is shared outside of the Ti company with third parties or otherwise. Your behavioural data is collected to supply the

suggested function on Ti's Home Feed; this can be deactivated in privacy settings.

Access to personal data is limited to staff that are modifying or deleting it. Access to behavioural and demographic data is limited to staff modifying the *suggested* function. Access to post data is limited to moderators. All access is granted on a temporary basis for the duration of performing the necessary task. All user data is monitored and protected using Data Loss Prevention (DLP) to ensure it does not leave the secure server through accidental or deliberate action of Ti staff.

Data Storage

All data is encrypted upon creation using a decentralised database with SHA 256-bit encryption - one of the safest encryption methods available. User data is stored on secure and regularly maintained private local servers. All post data is stored on secure and regularly maintained private cloud servers.

Data Protection

Ti uses full-spectrum antivirus protection on its network to ensure real-time, dynamic web defence against malware and related issues, as well as a strong firewall and regular security updates and patches. All links are validated before bing accepted on posts.

Data Breach Response

In the event of a data breach, we have a reactionary system in place to minimise harm. Ti's high degree of safeguarding means

that this shouldn’t be needed, but we are prepared for all eventualities.

If any of the data stored on Ti’s servers is compromised, all staff will be locked out immediately and the servers affected will be disconnected and shut down moving outwards from the source of the breach to prevent spread. If any user data is found to have been compromised, the persons affected will be notified immediately with instructions as to how best to remedy it. An investigation will begin immediately and our security team will address the issue to ensure a swift resumption of service and protection of Ti’s users.

Our Employees

At Ti, staff are regularly trained in the protocol around the handling of data and network security practices, and clear guidelines are set for everyone coming into contact with sensitive information.