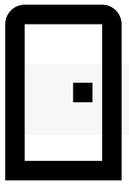
The Interactive Services Model (ISM)

PUBLIC

This Interactive Services Model (ISM) breaks down the user journey and platform workflows across interactive services, including social gaming experiences. It covers the sign on process, participation, additional functionalities that support the game experience, and moderation workflows.



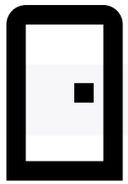
Sign On

Participate

Enable

Moderate

For each phase, from Sign On to Moderate, there are a set of functional models which show the functional and architectural processes that platforms take to achieve the objectives of each phase. The models are representative of four gaming genres, which are explained on the following page.



Sign On

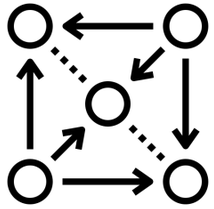
Participate

Enable

Moderate

Game Distributor	Game Provider	Set Up	Compete/Build	Create	Monetise	Analyse	Respond	Comply
Choose access medium	Download and install	Open game session	Begin game session	Launch studio, mode or server	Provide payment details	Decide Trust and Safety Approach	Remove content	Set objectives
Choose distribution point	Launch client	Sign Code of Conduct	Progress	Create experience	Set up wallet	Collect and sift content	Sanction user	Collect data
Make account	Make profile	Enter lobby	Interact with users	Choose settings	Choose membership	Classify and prioritise content	Alert law enforcement	Monitor data
Find game	Choose or accept default account settings	Join queue	Report inappropriate behaviour	Publish experience	Build or buy currency	Improve approach		Redetermine objectives
Purchase game (if relevant)	Create or customise avatar	Be matched	Exit session		Exchange or spend currency			

Given the breadth of gaming experiences, PUBLIC decided to focus on certain game genres for the purpose of the ISM. We prioritised four genres, namely, Battle Arena, Battle Royale, Shooter, and Sandbox games. These genres were prioritised based on their popularity in UK, user demographics and interactive functionality. By interactive functionality we mean the level of user-to-user and user-to-user-generated content, interactions capable within a given game in these genres.

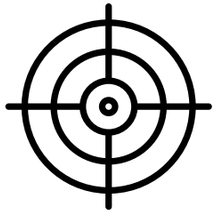


Battle Arena

Games where users control a character that has set abilities in a team of characters, usually controlled by other users. These games are played in symmetric maps that have a set base, often opposite the other team's base. The objective of the game is usually to destroy the other team's base.

Battle Royale

Games where users start from scratch every game and have to survive to be the last person or team standing to win the game. A significant share of gameplay revolves around scavenging random loot. The game forces users into confrontation (e.g., by a shrinking safe zone).



Shooter

Games in which the user controls a character which shoots enemies to defeat them.

Sandbox

Games that give the user a large amount of creativity and freedom on how to play the game, what to do, or to create the game's content themselves with little to no predetermined objectives.

These definitions have been sourced from Newzoo's Internal Research

Sign On | Game Distribution Platforms

Game Distribution Platforms are digital platforms that distribute games to users.

The Sign On process for game distribution platforms covers choosing the access medium and distribution point by which the user will find and access the game. The user must then make an account with the game distributor, verifying any relevant details, choose their game, and make a purchase, if necessary. In addition, some game distribution platforms will provide their own user-to-user communication features or overlay with in-game accounts and communication features.

User Journey

The steps and choices users make moving through an interactive service experience.

User Journey

Platform Architecture

The platform workflows and backend processes that support the user journey and safety policies.

Platform Architecture

Search · Server · Customisation · Security · Profile · Community · Comms Feature · Monetisation · Game Client · Trust and Safety · Database · Cloud · External Service · Search Database · Automation

Ofcom PUBLIC

Journey Phase

Choose Access Medium | Choose Distribution Point | Create Account | Find Game | Purchase (optional)

Cross-play

Previously, users on different distribution platforms couldn't play or communicate with one another, and if a user played a game on different types of hardware, they couldn't share progress. This has now become feasible for many games.

This is managed via users being assigned a developer ID, which can prevent conflicting usernames when cross-platform play is active on a game. For example a user with the username Ofcom123 on a console could be assigned a developer ID as Ofcom#123#1 and a user on a PC with the same username could be assigned a developer ID as Ofcom#123#2 when playing the same game.

Cross-play: Play with other users despite using different hardware

Cross-progression: Carry game progress and purchases across different devices

Cross-communication: Add and communicate with users on another device

Game Distribution Platform Apps

Users can also now download and access companion apps from game distribution platforms, for their PC or mobile device. These can provide: communication features; account management; purchases and download to console; remote play and streaming.

Direct Sign Up

Direct relationship with the gaming distributor where the user adds the required data themselves.

Federated Sign On

User chooses from third-parties supported by the game distribution platform, consenting to share details to complete sign up for a service.

User passes through authentication, according to sign on process

User signs Terms of Service

Dictates users' rights and responsibilities whilst using the service.

Parental Controls

Parental controls can be applied in one of two ways:
On device: Where settings are applied to all users and guests on the device, covering age levels, hardware, and website browsing settings; controlled by pin or password.
Account based: If a user self attests that they are under 13, a different creation process begins. This will usually involve sending an email to a parent or guardian, who will then set up a young person or child account. Parents can control account settings for these users via their family groups. Parents are able to view purchases, games played and screentime on their child's account.

Account Settings

Game distribution platforms may provide account safety and privacy settings.
These usually cover user profile privacy, communication, and content settings. Communication settings usually include:
Private
Friends only
Friends of friends
Open to all

User creates account

Communication Features

Some game distributors provide out-of-game communication features where different media types can be shared. Their Trust and Safety measures will usually be applied to their communication features, but may not apply to communication features within third party games accessed via their distribution platform.
Direct messages: Between two individual users, often restricted to friends or friend of friend interactions.
Party chat: These can be open or closed, where open means that a user can join, or request to join, a friend's or friend of friend's party, and closed means that users can only discover or join the party if they have been invited to do so.
Communities and clubs: Online meeting places created by users. These can be visible, accepting requests to join, or private, only accepting invited users.

User opens communication features

User sets up wallet

Find more information on payments in the 'Monetise' stage

User adds friends

Adding Friends

Users can find friends by:
Name, Username, Gamertag or ID search: Users can find friends by using a search bar; this will not show private profiles.
Suggested friends and 'Players Met': Game providers and distributors may cultivate lists of suggested friends for users. This can include 'Players met' from in-game experiences. Users can 'quick add' from this list.
Linking social media accounts: To share updates, users can add friends who play the same games or belong to a common game distribution platform.
Transference from existing networks: Where one network interconnects with another, automatically syncing friends across. For example, a game distribution platform may sync friends from their platform into the individual games a user plays.
Community search: Users can find friends by searching for clubs or communities and adding users from these networks.

Platform calls authentication service

User details verified

Game distributor database updated

Age Assurance Mechanisms

Many services rely upon self declaration where the user must enter date of birth during registration, but no checks are conducted on correctness of data. However, options that are currently in use include:
Parent verification via payment card: Where parents may be asked to verify on behalf of the child using a payment card.
Age gating using government ID: Where users may be asked to verify age via government issued ID (e.g. passport or driving license) to gain access to the service and/or specific features.

User Information

Though granularity varies, most game distributors will collect:
First or Last Name: Full name, not usually verified
Country: To help tailor the experience appropriately
Email: To associate with the account
Date of Birth: Usually self attested
Display Name or Username: Usually pseudonymous

User searches for game

Platform matches user to games

Malware and App Store Protection

Game software can be a target for malware. Distributor platforms will often vet the applications that are listed on their store, and sometimes alongside the game provider will check applications and user devices and their settings for unusual or inappropriate behaviour.
Game providers may also provide guidance to users, such as FAQs and blogs about targeted attacks or use of known modifications.

Game Distributor Safety Requirements

App Stores and Game distributor platforms sometimes require game providers to meet safety requirements in order to appear on their distribution platforms. Such safety requirements can, for example, include the obligation to have:
Community standards: A set of behavioural standards that users are made aware of.
User facing features: Such as reporting, or blocking.
Backend functionality: Such as content moderation mechanisms.
Points of contact: For escalations around serious offences.

User Content Controls

Users can set controls for what games they can see in game and app stores, filtering out for factors such as graphic content, profanity, for certain themes, and for age restrictions.

User finds game

Finding Games

Users find games through a number of avenues:
Staff picks: A set of games recommended by distributor.
Search: By name, genre or other descriptive terms.
Subscriptions: If a user is on a subscription membership, the game distributor may promote games that are part of, or have recently been added to, the subscription catalogue.
Network recommendations: Some game distributors will show users what their friends are playing or, depending on user preferences, may let them view if their friends own a particular game.

Recommender Algorithms

Content based filtering: Uses metadata on the game, such as genre, to make basic recommendations.
Collaborative filtering: Uses data collected from a user's transactions and activity to map user interests. Makes recommendations and predicts user preferences based on the preferences of other users.
Hybrid filtering: Offers suggestions to the user by combining content based and collaborative filtering. Generates complex insights about user preferences and game popularity and trends.

User signs up for subscription

Pay to Play Games

Pay to Play Games require a subscription payment on an ongoing basis in order to use a service.
Online Multiplayer Subscription: Users may be required to pay a recurring fee to access online multiplayer for pay-to-play titles. In addition, users may be able to redeem from a small selection of different games each month.
Catalogue Subscription: User pays on a recurring basis for access to a larger catalogue of games, which can change over time.
Single Game Subscription: User pays on a recurring basis for access to a single online game. Users can sometimes also pay additional fees to receive the most recent game updates.

User makes purchase

Buy to Play Games

Buy to Play Games can be played after a one time purchase. These games may also include expansions and downloadable content that are made available free of charge or for a fee.
One off: User pays once for permanent access to a game.

User downloads game (if free)

Free to Play Games

Though many games are accessible for free they may derive value in other ways:
Microtransactions: Where users can spend money on in-game items, content or in exchange for virtual currency to make purchases.
Premium memberships: Provide monthly benefits such as access, discounts, or perks relating to in-game content, currency, or progression.
Advertising for revenue: Some free to play games, often mobile, rely on rewarded video advertisements, offer walls, and banner ads for revenue.

Sign On | Game Provider

Game Providers may design, publish, and/or support games.

The Sign on process for game providers often represents an optional secondary layer of account creation beginning from the launch of the game. A user may opt to use a supported federated sign on process, use an existing game distribution platform account, or opt to sign up directly with the game provider. In some instances, signing up with the game provider is required before a user can play the game or access certain in-game features. The method in which the game is accessed may have implications on the user registration process.

Search
Server
Customisation
Security
Profile
Community
Comms Feature
Monetisation
Game Client
Trust and Safety
Database
Cloud
External Service
Search Database
Automation

Ofcom PUBLIC

User Journey

The steps and choices users make moving through an interactive service experience.

User Journey

Platform Architecture

The platform workflows and backend processes that support the user journey and safety policies.

Platform Architecture

Journey Phase | Download and Install | Launch Client | Make Profile | Choose or Accept Default Account Settings | Create or Customise Avatar

User installs game and launches client

Direct Sign Up
Direct relationship with the gaming provider who requests and verifies user account details on game launch.

Federated Sign On
User chooses from third-parties supported by the game provider, consenting to share details to complete sign up for a service.

Managed Sign On
The game provider may automatically establish an account and sync friends for their game where data is provided from a user's existing game distribution platform account.

User provides details

Third party sign on provides user details

Game client installed and launched on user device

Game Client

The game client is the game software or application itself that the user is using to be connected to the game experience, usually downloaded and installed on the user device.
The game client provides game graphics, audio and the game simulation. It receives user input through their device and packages this as information to send to the game server; receiving the updated game state from the server, it will process this information and update the client interface to show the user the changed game world.
The game client will also process any changes to layout or settings made by the client.

User verifies

From our research we understand that inappropriate names generally include: implied or blatant hate speech, violence or harassment towards individuals or an identity group; explicitly attacking social causes or political views; sexual content that is violent, obscene, criminal or vulgar; profanity; and references to any adult or illegal content.

Many games advise or try to prevent users from using their full real name as a visible username.

Choosing a Username

User chooses username

Client calls database to check for taken usernames

Username not accepted

Client engages Trust and Safety profanity filter or content moderation system to check name

Username accepted

Username Filtering

Possible options for username filtering might include:
Simple text filtering: Checked against profanity filter and list of banned content.
Safe words: Automated random username generators.
Tiered text filtering: Identifies usernames as 'Low', 'Medium' or 'High' risk. A variety of data points are used to classify names, including user longevity and past violations. Low risk content will be automatically passed through, whereas medium or high risk content will be either passed to a moderator for review, or automatically rejected.
More complex systems will also convert username text into plain text, removing punctuation, Unicode, emojis and other unnatural language characters.

Game providers also allow users to choose settings for their game experience.
These might cover account privacy and communication features, and will be password or PIN controlled for users who self attest to be under 13.

Game Provider Account Controls

User accepts or changes game preferences

Client manages game settings for user

Users have the ability to set communication preferences, at game distribution platform and at game provider level:
Text chat controls: Can be open to everyone or restricted to friends and teammates, friends only, and nobody. Games typically default to open to everyone.
Voice chat controls: Can include muting individual users, or selecting audience categories such as: Everyone, Teammates, Friends, Teammates + Friends, and No One. Additional voice chat controls may be offered depending on functionality.
Party joinability: Parties are groups that can be established prior to searching for and joining games. The ability to join a party will depend upon privacy preferences: anyone, friends only, or invite only.
Content filtering: Some platforms offer filtering for different types of media such as text, web links and text content.

In-Game Communication Preferences

User creates avatar

Client calls customisation service to manage avatar creation

Customisation service updates user database with preferences

Providers' avatar policies usually cover the prevention of nudity and inappropriate coverage of avatars, and preventing offensive clothing or symbols (such as a red armband).

Avatars are usually moderated through a combination of automated filters, live moderation and user reports.

Platform Avatar Policies

Avatar Options

Default or predefined characters: Usually found in Shooter titles.
Selection of predefined characters and outfits: Usually found in Battle Arena and Battle Royale titles.
Granular customisation, such as in changing the facial and body features and wearables: Usually seen in the Sandbox genre.

Physical features

Clothing and wearables

Tools and weapons

Skins

Generic illustration of what the process of choosing clothes, tools or weapons may look like.

Users can customise their avatars and weapons with skins, tools and wearables through progression unlocks, purchases with in-game points or currency, or purchases using real-world currency. In addition to being developed by game providers, some titles allow third parties or users to develop or design customised in-game assets.
However, customised skins can be harder for automated and human moderators to recognise and manage.

Skins and Customisation

Participate | Set Up

The Set Up process covers actions taken just before the launch of a game session. These include lobbies, choosing teams and matchmaking.

User Journey

The steps and choices users make moving through an interactive service experience.

User Journey

Platform Architecture

The platform workflows and backend processes that support the user journey and safety policies.

Platform Architecture

Search · Server · Customisation · Security · Profile · Community · Comms Feature · Monetisation · Game Client · Trust and Safety · Database · Cloud · External Service · Search Database · Automation

Ofcom PUBLIC

Journey Phase | Open Game Session | Sign Code of Conduct | Enter Lobby | Join Queue | Start Game

User launches game

User signs Code of Conduct

Signed the first time they launch the game, covering acceptable behaviour and platform sanctions.

User chooses mode or server

Public matches: Any user on the game can join a lobby for a match.
Private matches: Individual users can set up private lobbies so that they can customise their experience, for example by choosing custom rules, or only playing with chosen users or friends.

Private and Public Matches

Solo: The user will join games by themselves and play against the environment and other users.
Team: Users will join up with other users in advance, sometimes along with a party chat.

Choosing User Modes

Users can sometimes share links to third party websites, streaming services or modification providers in lobbies. Services take different approaches to allowing and preventing this, usually according to the audience of their service and particularly in regards to demographics. Services may opt to:

Allow all URLs;
Have a list of approved list of URLs: such as social media or streaming sites. Non-listed URLs will be blocked;
URL blocks: All URLs are blocked. Users may be able to bypass such blocks.

Off-platform Link Sharing

In some services, in-game communication features are enabled as soon as users enter a party or lobby. A user may choose to make use of dedicated chat functionality provided by a game distribution platform, or third party services to communicate as they play.

Lobby Communication Features

User enters lobby

Lobbies are pre-session waiting rooms. Users can see ongoing and upcoming sessions, accept or create party invitations, communicate with users or request a match from the matchmaking service.

User chooses mode or character

This is optional, usually found in Battle Arena genres. The user can also customise their character or weapons at this point.

Lobby is disbanded

Lobbies can be disbanded if they fail to reach the minimum number of users, or users wanting to play the same mode.

User joins queue

Lobby reaches mass of users

Lobbies will be open until they collect the minimum number of users for a given session; this varies between different games and genres.

User enters session

Client sends request to game server

Client launches lobby service

Client checks database for sanctions or delays

Client launches matchmaking service

Matchmaking service checks database for user progress, skill

Matchmaking service determines session users and teams

Server admits client

Generic illustration of matchmaking process

Game Server

The game server or host is the authoritative source of events in the game, or the 'game state'.

The game state is a record of user positions, object properties, environmental status and the leaderboard at any one point in the game.

Game servers process all inputs sent from the game client, resolve inconsistencies, update the game state and then transmits updates back to clients. The number of times the game server updates the game state and transmits to client per second is known as 'Tickrate'.

Dedicated and Listen Servers

Dedicated game server: These are remotely hosted by the game provider, and are run independently of any clients or users. They do not support direct input or output, except that which is required for their administration. Users on their hardware must connect to the server to interact with other users online in the game.

Listen server: These function like dedicated servers, but are hosted on a single user's game client. This may mean the host user has a faster connection than other users.

Queue Times and Delays

In multi-user online games, users will often queue to enter a session. This happens as the provider matches users into the sessions most appropriate to their skill level.
Users can be given queue delays as a sanction for poor behaviour.

Matchmaking

In online gaming, matchmaking is the process of connecting users together for online play sessions.
Automated: This may be achieved algorithmically to optimise user experience based on factors such as availability of users, network characteristics, and a user's skill.
Manually: Whereby a user creates or opts to join a specific server or online multi-user instance that best fits their interests.

Matchmaking Considerations

Providers may use any of the following in their matchmaking systems:
Geography: Geographic location by regional servers.
ELO: A user skill score, which calculates the chance of x user beating y user over x% of engagements. In teams based games, every team has a 50% +/- 1% chance of winning, which is made by pairing off teams of roughly the same average matchmaking rating. Users (and therefore teams) win more points if they beat the system.
Connectivity: Matching users based on factors such as latency to reduce lag and hence improve the game experience.
Hardware: Where users within the same ecosystem and/or with the same peripherals are matched in order to maintain a fair experience.
Position preference: In games where a character can only be selected by one user (mainly team based, such as Battle Arena), lobbies will be made up of a sufficient diversity of users so that users have a reasonable chance of attaining the user they want.
Queue time: How long a user has been waiting in the queue, minimising wait times.
Group size: Making groups up to different sizes in order to displace any advantage gained by being in a premade team.

Participate | Compete

Compete covers competitive user versus user games. This stage describes the basic actions of a game session, and the process a user might follow if they experience inappropriate behaviour.

Journey Phase

Open Game Session | Progress | Experience inappropriate behaviour | Report inappropriate behaviour | End Session

Enter Session | Interact With Users

User Journey

The steps and choices users make moving through an interactive service experience.

User Journey

Platform Architecture

The platform workflows and backend processes that support the user journey and safety policies.

Platform Architecture

Generic illustration of Battle Royale map

Generic illustration of Battle Arena map

User begins session

Gain XP, Gold

Defeat enemy users or environment

Progress through environment

User interacts with other users

In contrast to using third party communication services or a game distribution platform party chat, a user might use communication features provided in-game. These may comprise of:
Voice and text chat: That can be exchanged between all users (in a server or lobby) or selectively filtered by the:
Game: Where chat may only be available in certain scenarios due to design decisions. For example, only allowing users with in-game characters in close proximity to communicate or restricting features or setting defaults for younger or non-verified users.
User: Filtering chat from everyone to teammates, friends only, parties, or selectively between individual users.
Signs, emotes, pings: on some platforms, users can make signs or emotes to communicate with other users. These are a specific vector for harm as secondary malicious meetings can become associated with specific signs.

In-Game Communication Features

User experiences inappropriate behaviour

If a user experiences inappropriate behaviour from another user in-game , they might have access to the following user controls to respond:
Muting: Muting another user's text, voice and pings for the duration of the session. Either individual users, a team, or the entire session group.
Blocking: Blocking individual users in session; this mutes all communications from a user for the duration of the session and future sessions. This also prevents the blocked user from adding the target user as a friend, and can hide the profile of the target user to the blocked user.
Reporting: Users can also choose to file a report on an individual user or piece of content in session.

User Response Options

User mutes or blocks offender

User leaves session

User is eliminated

User respawns

In competitive games, services want to encourage competitiveness without promoting inappropriate behaviour. Services aim to achieve this by utilising mechanisms such as:
Honour points or ratings: Points or specialised XP systems whereby good behaviour gains points; Conversely, bad behaviour can mean users lose honour points.
Community based justice: Leagues whereby sanctions for users can be decided by community voting. This showcases negative behaviours and their sanctions, as well as boosting community involvement.
Reputation scores: Services are beginning to explore assigning users reputation scores for positive and negative in-game behaviours.
Education: Services are providing quizzes, interviews and tips on Fair Play to help build healthier gaming communities.

Prosocial Play

Generic illustration of reporting screen

Generic illustration of post-game lobby

In the post-game lobby, users can identify and report another user's content or conduct, by:
1. Choosing a category or reason under which the report falls.
2. Optionally filling out a brief description of the offending behaviour.
Some services place restrictions on reporting, such as: limiting reporting to 20 minutes after gameplay has finished, or to users from the last 5 to 10 games.
If a service suspects a user of maliciously reporting others, they can temporarily or permanently ban them in response to their report.
Some services allow users to 'collect evidence' for their report(s), by going back into voice chat logs which are held under a recording buffer. (See 'Analyse' stage for more detail on this).

Reporting

User completes session

User enters post-session lobby

User files report

User adds friends

User joins community

User queued for next match

Post-Session Lobbies

After a game session closes, the lobby may persist for an amount of time before being disbanded or queueing up the next game session so that users can communicate. In these lobbies or via the main menu users may be able to look up user and match statistics, as well as players met during the session to communicate, add or report other users.

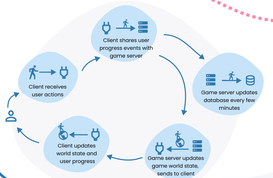
Players Met

When a game concludes, the game may provide a list of 'Players met' during the session to the user, from which they can add new friends, in addition to the feature of adding someone from typical suggestions or adding them from social media.

Client joins server game session

Database provides user progress

Client and game server run the game session



Game Client

The game client represents the software the user is using to connect to the game experience, usually downloaded and installed on the user device.
The game client provides game graphics, audio and the game simulation. It receives user input through their device and packages this as information to send to the game server; receiving the updated game state from the server, it will process this information and update the client interface to show the user the changed game world.
The game client will also process any changes to layout or settings made by the client.

Game Database

The game database holds all data collected and used to operate the game, including but not limited to:
User skill level and progress: For example, experience points (XP), achievements, unlocked skills, wins and losses.
Personalisation: For example, character or avatar personalisation, appearance customisation, skins.
Personal identification: For example, age, IP address, email address, Local Area Network.
Item inventories: For example, gold, weapons, collected or found items and potions that can be used in-game.

Game Server

The game server or host is the authoritative source of events in the game, or the 'game state'.

The game state is a record of user positions, object properties, environmental status and the leaderboard at any one point in the game.

Game servers process all inputs sent from the game client, resolve inconsistencies, update the game state and then transmits updates back to clients. The number of times the game server updates the game state and transmits to client per second is known as 'Tickrate'.

Game services (chat, moderation) communicate with client and server

Game Services

Game services provide non-gameplay, auxiliary functions such as chat, anti-cheat, or user authentication services. These are usually implemented as API or SDK services, technical layers which plug in to the client, server and database to provide their features.

Anti-cheat software

Services build user behaviour algorithms, based on custom heuristics, to assess if user behaviour is human or driven by a mod or cheat software. In addition, server-side software can detect if clients are associated with human users.
Cheating and hacking is usually met with zero tolerance by services.

Leaver Buster Software

Services may use automated systems to discourage users from repeatedly leaving matches or idling during gameplay. Users might be warned, placed in a low priority queue or have their XP increases from the session prevented. However, these systems may have implications for users leaving games for other reasons such as experiencing inappropriate behaviour.

Game session is closed for server and client

Game Session Duration

The duration of the game session is dependent on the type of game genre:
Battle Arena: The user's character can regenerate multiple times in one game session, meaning that when they 'die' the client does not leave the game session. Rather, the session will end when one of the teams is defeated.
Battle Royale: In some Battle Royale titles, the user's character can also regenerate multiple times until the session ends. The session ends when a final user or team is alive with all other users or teams having exhausted respawn capabilities. In other titles, the user's character cannot respawn and may only exit the game session, or choose to watch other users continue, once they die.
Shooter: Depending on the mode and objective of the game, once a user's character dies they may respawn until a score or time limit is reached, or where an objective is met by a user or team.

Search | Server | Customisation
Security | Profile | Community
Comms Feature | Monetisation | Game Client
Trust and Safety | Database | Cloud
External Service | Search Database | Automation

Ofcom PUBLIC

Participate | Build

Build covers Sandbox genre games, whereby the gameplay is much less structured, prescriptive, and linear. This stage covers some of the basic activities a user can explore, as well as the process they might follow if they experience inappropriate behaviour.

User Journey

The steps and choices users make moving through an interactive service experience.

User Journey

Platform Architecture

The platform workflows and backend processes that support the user journey and safety policies.

Platform Architecture

Search
Server
Customisation
Security
Profile
Community
Comms Feature
Monetisation
Game Client
Trust and Safety
Database
Cloud
External Service
Search Database
Automation

Ofcom
PUBLIC

Journey Phase

Open Game Session
Enter Session
Progress
Interact With Users
Experience inappropriate behaviour
Report inappropriate behaviour
End Session

Generic illustration of Sandbox game screen

User enters server

Client and server run game session

Server Types

Servers are user or provider owned multi-user game servers. Users can set up a server using software from the game provider or by using a third party service.
Public servers: Provider hosted servers open to all players.
Private servers: Owned and managed by groups, organisations or individuals not affiliated with the game provider. Private server owners control the settings and users allowed in their servers, and can even charge for users to access their server. These servers can have either particularly strong or weak Trust & Safety measures, depending on the approach of the server owner.

Sandbox Game Session

Where in competitive genres, the session is defined by a match or discrete action loop which can last for varying amounts of time, in Sandbox genres the session length is not linked to any discrete loop. Rather the user may join or be assigned to a game session via manual server selection, matchmaking or invitation. The session then persists for as long as the game session is populated by the minimal required number of users.

Build and destroy content

Explore

Fight enemies

Sustain character

Play minigames

Users who act disruptively may be labelled or given visual labels to allow other users to identify them as disruptive users, and may be placed into spheres of influence where they can only interact with other users labelled as disruptive. On the other hand, users who are cooperative can be given benefits such as payouts and discounts.

Safety by Design in Sandbox Games

Users interacts with other users

Users may encounter other users through public servers, where a public session is available, or private servers, whereby a user may invite other users. This might also be impacted by:
Privacy preferences: The constraints the host has set on access to the game or server, such as requiring requests, or placing limits on the type of user who might join, for example covering age or skill level.
Discoverability: Whether the game can be searched for or listed on a public page.

User Interactions in Sandbox Games

Experience inappropriate behaviour

in contrast to using third party communication services or a game distribution platform party chat, a user might use communication features provided in-game. These may comprise of:
Voice and text chat: That can be exchanged between all users (in a server or lobby) or selectively filtered by the:
Game: Where chat may only be available in certain scenarios due to design decisions. For example, only allowing users with in-game characters in close proximity to communicate or restricting features or setting defaults for younger or non-verified users.
User: Filtering chat from everyone to teammates, friends only, parties, or selectively between individual users.
Signs, emotes, pings: On some services, users can make signs or emotes to communicate with other users. These are a specific vector for harm as secondary malicious meetings can become associated with specific signs.

In-Game Communication Features

User mutes or blocks offender

If a user experiences inappropriate behaviour from another user in-game, they might have access to the following user controls to respond:
Muting: Muting another user's text, voice and pings for the duration of the session. Either individual users, a team, or the entire session group.
Blocking: Blocking individual users in session; this mutes all communications from a user for the duration of the session and future sessions. This also prevents the blocked user from adding the target user as a friend, and can hide the profile of the target user to the blocked user.
Reporting: Users can also choose to file a report on an individual user or piece of content in session.

User Response Options

User files user report

Discover inappropriate content

User completes session

Game Session Ends

In contrast to competitive genres, in Sandbox genres the 'game state' persists, meaning that the session does not loop and close in the same way as, for example, a Battle Arena game. This means that the environment and context for the game world will remain stable between times that the client can access the game world.

User files content report

In public servers, moderators and administrators may be employed by the game provider. They will work across all users, according to the game provider's Code of Conduct. Moderators generally manage server communities, supervising user activity and content. Administrators usually have additional controls over content, permissions, and settings. In private servers or user-generated experiences, the server owner might designate themselves, employ moderators and admins, or organise volunteers to moderate the experience. The community guidelines will vary depending on the specific server or experience.

Moderators and Administrators

Generic illustration of chatroom screen

Enable | Create

Create covers functionality wherein interactive services provide users with the ability to create their own experiences, which other users can then take part in.

User Journey

The steps and choices users make moving through an interactive service experience.

User Journey

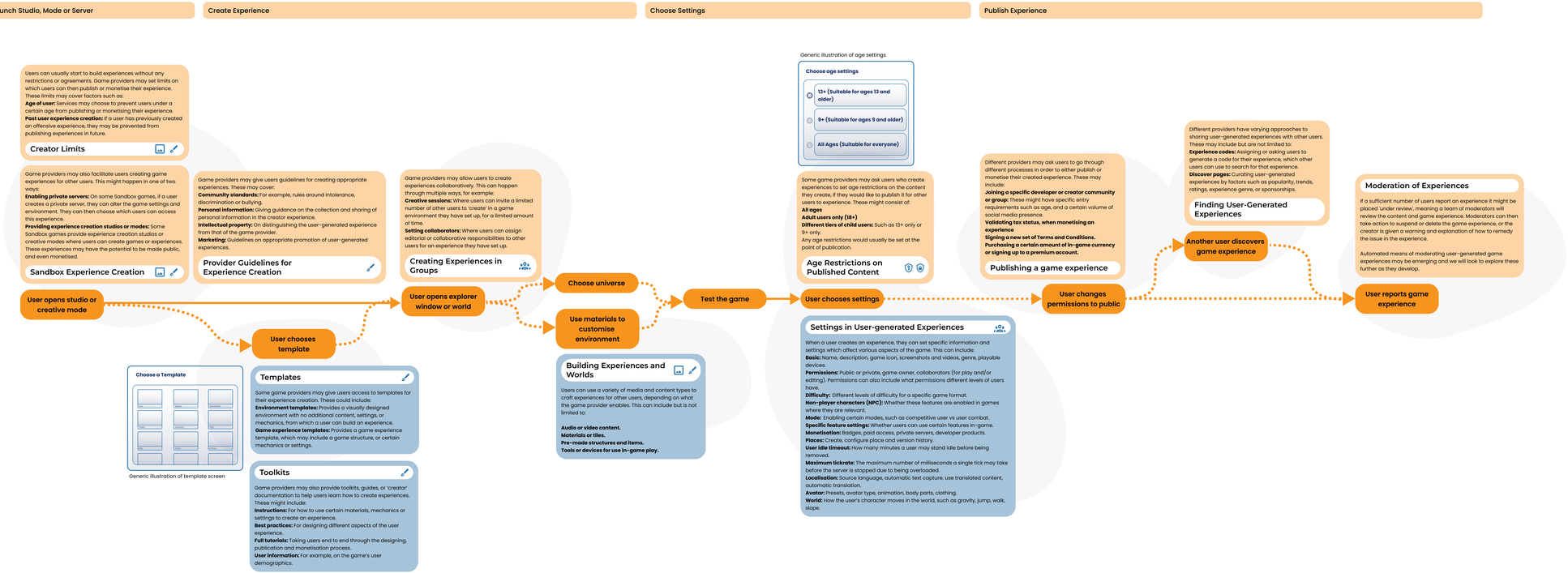
Platform Architecture

The platform workflows and backend processes that support the user journey and safety policies.

Platform Architecture

Search
Server
Customisation
Security
Profile
Community
Comms Feature
Monetisation
Game Client
Trust and Safety
Database
Cloud
External Service
Search Database
Automation

Ofcom
PUBLIC



Enable | Monetise

The Monetise stage represents the possibilities for service monetisation in gaming. This covers users setting up payment details and virtual wallets, and participating in in-game and out-of-game economies, as well as the associated potential inappropriate behaviours that may arise from these activities.

User Journey

The steps and choices users make moving through an interactive service experience.

User Journey

Platform Architecture

The platform workflows and backend processes that support the user journey and safety policies.

Platform Architecture

- Search
- Server
- Customisation
- Security
- Profile
- Community
- Comms Feature
- Monetisation
- Game Client
- Trust and Safety
- Database
- Cloud
- External Service
- Search Database
- Automation

Ofcom PUBLIC

Journey Phase | Provide Payment Details | Set Up Wallet | Choose Membership | Build Currency | Exchange or Spend Currency

Generic illustration of currency purchase screen

Provide direct payment details

Integrate gaming distributor wallet

Integrate gaming distributor purchases

Integrate mobile payment structure

Game distribution platform wallets: Users can make purchases in game distribution platform stores (such as purchasing virtual currency and items) that are redeemable in-game, in many multi-platform titles these purchases can be synced across devices.
Linked wallets: For some games, the game provider and user can choose to allow game distribution platform account and payment details to make in-game purchases.
In-game wallets: Users can set up wallets in individual games, by providing payment details in the game.
Mobile payment: Users can make in-game purchases by integrating existing payment mechanisms from their mobile.
Gift Cards: Users can also use gift cards of set balances in order to make in-game purchases.

In-Game Purchases

Users and services can transact with each other for in-game items and virtual currencies in a variety of ways, for example:
User-to-service transactions: Such as premium membership fees and in-game purchases.
User-to-user transactions facilitated by the service: Through in-game trading hubs, or by providing a sign on mechanism in partnership with a third party site so that users can trade items securely.
User-to-user transactions not facilitated by the service: These can take place on a variety of third party sites.

Transaction Types

User sets up wallet

User chooses membership level

Games often offer 'Premium' memberships to users with benefits such as custom skins, virtual currency and new experiences. This is not for access to the core game, but rather for additional perks.

Secondary Economies

Some game commodities, which can be unlocked through gameplay or purchased by users, have gained value that is additional to or separate from in-game functionality.
For example, rare skins in some games have built high social capital; meaning they may become worth high volumes of in-game and real-world currency. Some games facilitate the trade of these commodities through in-game trading and purchasing hubs. There are also a broad variety of third party buying, selling and exchanging sites that facilitate commodity transactions outside of the game.

Exchange Mechanisms

In-game: Some games provide 'Loot Boxes', which can be purchased through gameplay or in exchange for virtual or real currency, and can contain a set of in-game items of unknown quality and quantity.
Out-of-game: Third party sites provide exchanges using skins or items as currency, where users bet on games, tournament or stream outcomes. Users might link their game account or provide their login details to the site, giving the site access to their item inventory, which they then lose control of for the duration of the bet. If they lose the bet, the item(s) are automatically transferred to the winning user(s).

Generic illustration of Loot Box screen

Secondary economies may emerge around a virtual currency or item, which may lead to practices such as:
Gold Farming: In games where types of currency can be earned through hours played, this has sometimes given rise to users being paid to play the game for another user, in order to earn hours and virtual currency.
Botting: Users may use an automated programme to gain virtual currency through either obtaining a high volume of hours played, or through levelling accounts to maximum level.

Farming and Botting

User earns or finds virtual currency or items

User purchases virtual currency or items

Accounts with high experience or valuable items may face a higher risk of online attacks. Perpetrators might target user IP addresses, or use malware, phishing, fake third party websites in order to obtain account details to gain access to those items.

Online Attacks

Game providers and distributors work to counter fraud through a variety of ways, such as:
Information pages: These can include lists of ongoing or current scams.
Recommended trading practices: Guidance on how to tell if trades or purchases are valid or fraudulent.
Trade bans: These are account bans or suspensions on users taking part in fraud.
Additional account security measures: Some services offer optional higher account security measures, such as two factor authentication.
Fraud protection platforms: Machine learning platforms which provide real-time fraud detection, though analysis of purchase information and user and item tracking.

Protection of Users

User gains virtual currency or items

Virtual Currency Types

Hard currency: Primarily obtained through in-game purchases; grants users a premium gameplay experience.
Soft currency: Low value, general purpose currency primarily obtained for free.
Medium currency: Can be obtained through gameplay, but comes with usage or collection limitations.
Energy currency: In relevant games, the amount of energy a user has, which is spent on performing actions or reduced through other user attacks.
Feature currency: Associated with the use of certain game features.
Social currency: Acquired via social activities, like participating in multi-user events.
Guild currency: Generated by groups of users, can be shared or distributed amongst groups.
Event currency: Layers of game economy or currency which are independent from the main game.
Discard currency: Obtained through the destruction of game items
VIP currency: Generated as a byproduct of performing an in-game purchase.
Informal currency: Elements that users use as a medium of exchange, even though the intended purpose of the game provider for that element was different.

Balancing Currency

Game providers must balance the flows of virtual currency in-game. This is important, as imbalances can lead to user dissatisfaction, and can even encourage fraud, if availability of a certain currency becomes limited and extremely high value. Providers do this by placing limits on currency gain and expenditure, especially for medium or hard currencies, and by controlling what users can take in and out of the game economy.

User spends virtual currency

User withdraws virtual currency

Pay to earn games are games users may be paid for completing certain tasks, where payments may be in the form of crypto currencies or Non-Fungible Tokens (NFTs).

Cryptocurrency

User trades virtual currency or items

There are many third party trading and gambling websites where users can exchange valuable skins and items. such websites are not usually owned by interactive services, and where they are not owned may not be under their purview.

Third-Party Trading Websites

Moderate | Analyse

The Analyse stage details the measures put in place by interactive services to collect and analyse content and user behaviour to determine whether it is inappropriate. This includes deciding Trust and Safety measures, collecting data, classification and prioritisation of content and conduct, and improvement of systems.

User Journey

The steps and choices users make moving through an interactive service experience.

User Journey

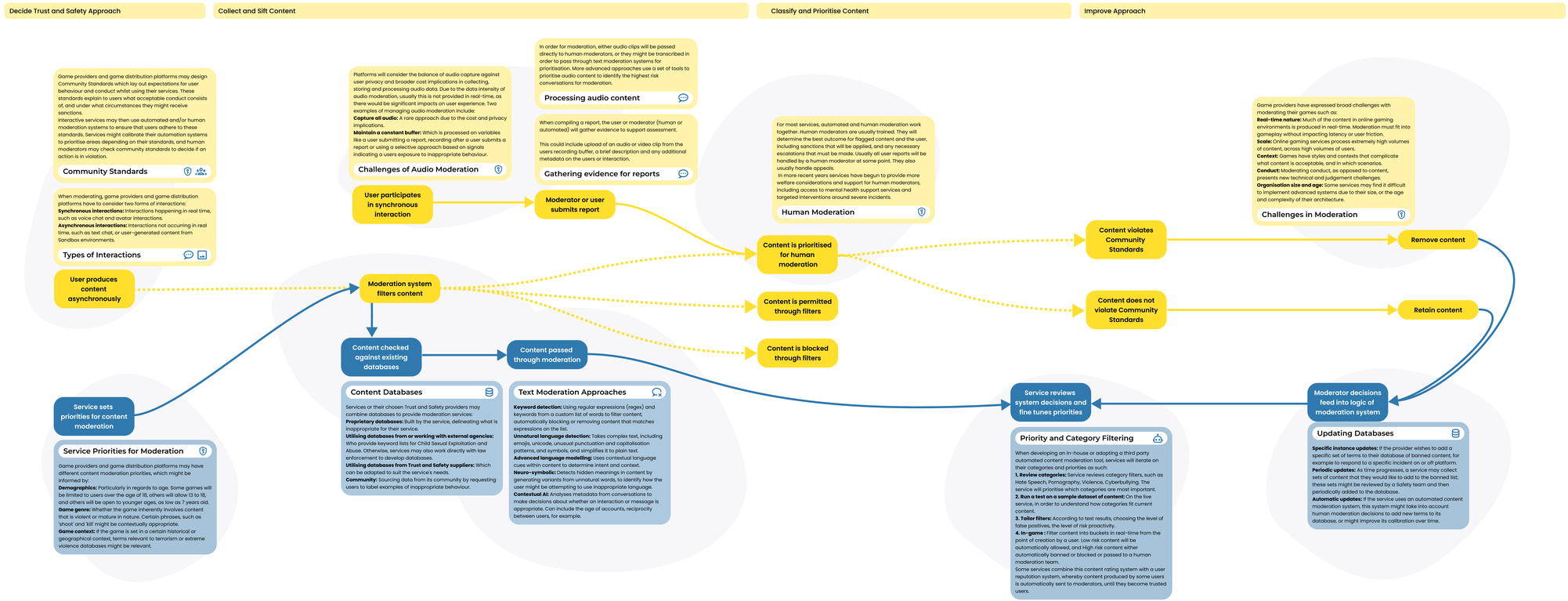
Platform Architecture

The platform workflows and backend processes that support the user journey and safety policies.

Platform Architecture

Search
Server
Customisation
Security
Profile
Community
Comms Feature
Monetisation
Game Client
Trust and Safety
Database
Cloud
External Service
Search Database
Automation

Ofcom PUBLIC



Moderate | Respond

The Respond stage provides details on how interactive services respond to the finding of inappropriate content or user behaviour. These may include the process of removing content, sanctioning users and alerting third-parties, such as law enforcement, where necessary and appropriate.

Search
Server
Customisation
Security
Profile
Community
Comms Feature
Monetisation
Game Client
Trust and Safety
Database
Cloud
External Service
Search Database
Automation

Ofcom
PUBLIC

Journey Phase
Remove Content
Sanction User
Alert Law Enforcement
User Appeals

User Journey

The steps and choices users make moving through an interactive service experience.

User Journey

Platform Architecture

The platform workflows and backend processes that support the user journey and safety policies.

Platform Architecture

Increasingly gaming services are making partnerships with suicide prevention charities. If suicidal or self harm content is detected, then users might be sent links to one of these support services.

Escalation for Suicide and Self Harm

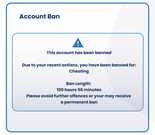
Approaches to counter-terrorism vary across the industry. Some companies partner with organisations to co-ordinate response to extremist content, by operating incident response strategies whereby they share resources that services can plug in to existing content moderation services to continually update their counter-terrorism approach.

Escalation for Extremist Content

Content that is identified as Child Sexual Exploitation and Abuse (CSEA) and Material (CSAM) may be immediately removed, either by automated or human moderators. The service will then compile a report containing any inappropriate content, and any metadata about the user they have. Services may have escalatory routes for CSEA and CSAM, where this report may be shared with appropriate parties.

Escalation for Child Abuse Material

Generic illustration of account ban screen



Frequency: Whether the offence is the first infraction from the user, or whether it is a repeat offence. Typically services will apply escalating sanctions.
Severity: This might include how many users were affected, and what type of users were affected. This could also include whether the offence has legal implications, such as coming under priority categories such as CSEA, Terrorism and Suicide and Self-Harm.

User Sanctions Factors

Warning message: This would be received before any sanction was imposed, usually on first offence, unless the offence was severe enough to warrant immediate account suspension.
Queue sanctions: This applies to Battle Arena, Battle Royale and Shooter genres; the user will receive increased waiting time in the queue before the game, which might increase with additional offences.
Points, XP sanctions: In some games, points and/or XP sanctions are applied to offenders, reducing how many points or XP they can earn from the session.
Temporary account bans: Temporary account bans follow less severe sanctions as mentioned above. These can range from 24 hours, to 72 hours, to 7 days. The user would receive a message in the client notifying them they cannot access or play the game.
Shadow bans: Placing users in special lobbies or games with only other previous offenders, for example if user is suspected or has been confirmed to have cheated.
Global muting: Users might be permanently muted, meaning they cannot communicate within the game at all, if they have offended frequently or severely.

User Sanction Types

Notifying Users

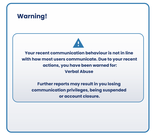
Services may have a variety of approaches to notifying users of their behaviour such as:
Notification: If a user is offending for the first time, or the offence is not severe, they would usually be notified of a sanction, such as a queue ban.
Explanation: Some services also offer explanations as to why a user might be receiving a sanction, or sharing with them their offence.
No notification: Services may opt to not notify users because the service does not have a notification system, or the user offence is so severe that services don't want the user to know they are aware of or have recognised the behaviour because they have reported the activity to third parties for further action.
Notification by the service might be affected by the scale of the service, what it might consider to be offending behaviour, and the design of its case management system.

Appeals Options

Users can apply for an appeal against a moderator action, unless the offence was particularly severe. This would consist of contacting a support desk, and explaining why the sanction has been unfairly applied. Appeals are usually handled by human teams.

Moderator witnesses conduct
Moderator removes content
Moderator checks for previous user offences
Content or conduct shared with external authorities
User is banned
User is sent a warning
User is given a sanction
User is notified of sanction
User appeals decision
Safety team reviews appeal
User sanction removed
User sanction amended
User sanction upheld
User does not have access to appeal

In egregious circumstances the user may not have the ability to appeal a sanction.



Generic illustration of user warning screen

Database adds user information to block list

Permanent Bans

Permanent bans may be given if temporary bans have expired and the user reoffends, or if a serious enough offence has been committed, such as an illegal offence, or cheating. This might take one of four forms:
Permanent IP bans: Targeting the IP address of the access point of the banned user.
Permanent device bans: Targeting an identifier of the access point of the banned user.
Console bans: Targeting the console of the user, meaning they cannot access the network on any account using this console.
Account bans: By game providers and game distribution platforms, preventing the use of online features.

Platform Sanction Workflows

Services set up workflows around user offences, recidivism, and sanctions. This usually would take the form of a matrix, linking offences, instances (i.e. primary offence, secondary) to actions in the platform workflow around sanctions. These can be both positive and negative. There are different routes for managing these workflows:

Human moderation: Some services will only allocate decisions on sanctions to human moderators, who can review a case with all relevant metadata and context.
Human and automated: Some services will use a combined approach, where an automated system will hand out warnings and minor sanctions, such as queue delays, and human moderators will hand out severe sanctions like permanent bans.

Some services will outsource response workflows in line with content moderation systems.

Database provides user information

User De-Identification

De-identification: Games will usually track user offences over time. However in order to ensure anonymity, users are associated with identification numbers which change on a routine basis. If enough offences happen over time, the user might have sanctions placed against them.

User Reputation Systems

An increasing trend in Trust and Safety systems in online gaming is incorporating or prioritising user behaviour into moderation efforts, as a majority of inappropriate content usually originates from a small percentage of users.
Longevity of account: Restricting user permissions based on how long an account has been held for.
Verification: Restricting user permissions based on whether the user has age or identity verified to the service.
Prior behaviour: If a user has been blocked or reported, or has sent a message which has been blocked, this can contribute to poor personal 'trust' scores. These systems are also called 'reputation' ratings, and may be shared with users to encourage positive behaviour.

Moderate | Comply

The Comply stage sets out the processes that interactive services undertake to internally audit and report on Trust and Safety. These may include designing Trust and Safety policies, setting priority objectives, monitoring data, escalation and transparency reporting.

Search
Server
Customisation
Security
Profile
Community
Comms Feature
Monetisation
Game Client
Trust and Safety
Database
Cloud
External Service
Search Database
Automation

Ofcom PUBLIC

Journey Phase | Set objectives for Trust and Safety | Collect Data | Monitor Data | Redetermine Objectives

User Journey

The steps and choices users make moving through an interactive service experience.

User Journey

Platform Architecture

The platform workflows and backend processes that support the user journey and safety policies.

Platform Architecture