**Protecting children**

Take particular care in the design of games that are likely to appeal to, or be accessed by, children and provide the necessary tools and information about gaming content for parents, guardians and children to enable them to manage all aspects of their children's enjoyment of games. Take extra steps to understand the age of players and ensure age appropriate protections are in place in addition to complying with online safety laws such as the UK's Online Safety Act and the EU's Digital Services Act.

**Treating consumers fairly**

Deal with players as consumers in a fair and transparent manner at all times and never mislead consumers or use aggressive sales practices. Provide players with clear, relevant information so they can make informed decisions, in addition to complying with all relevant marketing, advertising and consumer protection law.

**Safeguarding online communities**

Manage gaming platforms in a responsible manner *by prioritising player wellbeing*. Make every effort to ensure that online communities and interactions are safe and do not expose players to harm, in addition to complying with online safety laws such as the UK's Online Safety Act and the EU's Digital Services Act.

**Respecting personal data**

Take appropriate and proportionate measures to fulfil the seven data protection principles under the General Data Protection Regulation (GDPR) and comply with all other relevant data protection laws and associated codes of practice to ensure that players' rights to personal data privacy are respected. Go beyond complying with basic data protection principles, where games are aimed at children.

**Spending and time management**

Enable players to manage the amount of time and money spent on games through appropriate design and proportionate measures.

**Positive Practices for Games Companies**

The five TIGA Principles embody the spirit of the approach that games companies should adopt in operating their businesses within the UK.

The TIGA Principles are broad and high-level in scope and targeted towards positive outcomes. The Principles are designed to be proportionate: they take into account the fact that a specific action may be appropriate for one business, but it may not be appropriate for another. For example, what may be expected of a large games delivery platform may be different from that expected of a small indie developer.

In order to assist games companies to comply with the TIGA Principles, TIGA has created the following set of 'Positive Practices' for each Principle. The Positive Practices draw upon multiple sources, including legislation, codes of conduct issued by regulators and feedback from TIGA members. The Positive Practices specify a number of behaviours that would tend to suggest compliance with the Principles, but they are not an exhaustive list. While it may be possible to achieve compliance with the Principles without complying with all of the following Positive Practices, this is likely to be difficult. Equally, there may be other actions required to comply with the Principles that are not included in the Positive Practices.

TIGA may update the list of Positive Practices from time to time to take account of new legislation, codes of conduct produced by regulators, experience of TIGA members, developing business practices and technological advancements within the games industry.

TIGA first published its list of Positive Principles in February 2020. We updated them in August 2024 with the assistance of Lewis Silkin LLP

**P.1. Protecting Children**

*Take particular care in the design of games that are likely to appeal to, or be accessed by, children and provide the necessary tools and information about gaming content for parents, guardians and children to enable them to manage all aspects of their children's enjoyment of games. Take extra steps to understand the age of players and ensure age appropriate protections are in place in addition to complying with online safety laws such as the UK's Online Safety Act and the EU's Digital Services Act.*

**Best interests of children.** Games businesses should ensure that games are safe to use for all players. Games businesses should consider that some players, both adults and children of different ages, may be more vulnerable than others. Games businesses should, in particular, ensure that the best interests of the child are a primary consideration whenever designing and developing online services likely to be accessed by a child.

**Choice and support for children.** Ensuring clear and accessible information is available to children with easy-to-use reporting and complaints processes, and giving children tools and support to help them stay safe. For example, children should not be added to group chats without their consent.

**Prevent online harms to children.** Take steps to understand and assess the risks of potential online harms child players might be subjected to and take additional measures to prevent access to harmful content, for example, pornographic or other harmful content.

**Parental controls.** In the case of providers of game platforms, provide a robust and accessible set of parental controls that enable a parent or guardian to manage all aspects of their child's enjoyment of games and provide more choice and support for children. Parental controls allow parents or guardians to place limits on children's online activity to mitigate their exposure to risks. However, these can impact a children's right to privacy. Where games businesses provide parental controls, age appropriate information must be provided about this. If games allow parents to monitor their child's online activity or track their location, the games business must provide an obvious sign to children when they are being monitored. Parental controls may include:

- Screen time and spending for a particular game or all games (see Principle 5).
- Controlling which games can be accessed by reference to their PEGI ratings and complying with the PEGI Code of Conduct.
- Restricting online communications from strangers who have not been added as 'friends'.

**Promotion of parental controls.** Promote the following on your company's website and promotional materials in a clear and prominent manner:

- Applicable age ratings in each territory where the game is sold.
- The availability of parental controls on the devices on which the game is published.
- Safety information relating to the safe operation of any hardware required to play the game.

**Ease of use of parental controls.** Parental controls should be located all in one place on the platform, they should be easy to use, parents should be prompted to set them up and parents should be provided with documentation that is easily understood.

**Age assurance.** Where a game is available for download outside of a platform featuring a robust age verification process, developers should, where appropriate, include their own robust age verification process within the game to understand if players are children and prevent children from encountering harmful content.

**Compliance with data protection legislation and codes relating to children.** Comply with the law, codes and best practices when dealing with children's personal data. For example:

- **Acting in the best interests of children.** Do not process children's data to pursue commercial or other interests that are not in the best interests of children, including serving advertising that can cause harm or encourage addictive behaviour. Avoid taking a one-size-fits-all approach and consider the varying privacy awareness of players of different ages.
- **High privacy by default.** Privacy settings must be 'high privacy' by default and games businesses should not use techniques that lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections. For example, geolocation settings and personalisation or profiling activities should be off by default.
- **Detrimental use of data.** Games businesses should prevent exploitation of children's inexperience or vulnerability and avoid using personal data in ways which can be detrimental to children's wellbeing or that go against industry codes of practice or guidance.
- **Policies and community standards.** Game businesses should uphold any other published terms, policies, and community standards in which they have made commitments around how they use children's data.

**Compliance with online safety laws.** Comply in full with the spirit and letter of online safety laws and codes relating to children such as the UK's Online Safety Act and the EU's Digital Services Act (see also Principle 3).

**Publicise online safety advice.** Publicise the following sources of information:

https://tiga.org/about-tiga-and-our-industry/consumer-advice

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety

http://commonsensemedia.org

**P.2. Treating Consumers Fairly**

*Deal with players as consumers in a fair and transparent manner at all times and never mislead consumers or use aggressive sales practices. Provide players with clear, relevant information so they can make informed decisions, in addition to complying with all relevant marketing, advertising and consumer protection law.*

**Accessible terms.** Ensure that terms and conditions with users contain all information required by law and are clear and accessible, including to children and other vulnerable users, and that they meet standards set by any relevant regulators.

**Not misleading players or using aggressive sales practices.** Ensure that users are not mislead either by act or omission and that you are not using aggressive sales practices or manipulative online practices (known as “online choice architecture” or “dark patterns”).

**Fair enforcement of terms.** Enforce terms and conditions effectively and consistently.

**Refund policy.** Have a fair refund policy that complies with consumer laws and takes into account a player’s individual circumstances, for example, if a child were to enter into unauthorized transactions on a parent’s credit card.

**Complaints process.** Establish and maintain a complaints and appeals process that is in line with consumer law requirements, effective, easy to use, and provides users with timely, clear and transparent responses to complaints.

**Compliance with laws relating to subscriptions.** If games are monetised via paid subscriptions, subscription practices must comply with all applicable consumer laws including as set out in the Digital Markets, Competition and Consumers Act.

**Compliance with OFT principles.** Adhere to the 8 principles relating to online games and in-app purchases published by the Office for Fair Trading (now the Competition and Markets Authority), which can be summarised as follows:

- Costs information about in-game subscriptions and purchases should be provided clearly, accurately and prominently up-front, before the consumer begins to play, download or sign up.
- Game information, including a clear description, game functionality and compatibility with hardware and software, should also be provided clearly, accurately and prominently up-front.
- Information about your game company should additionally be provided clearly, accurately and prominently up-front.
- Commercial intent of any in-game promotion of paid-for content or promotion of any other product or service should be clear and distinguishable from gameplay.
- Companies should not mislead by giving the false impression that payments are required or are an integral part of the game if that is not the case.
- Companies should not include any aggressive practices or exploit a child’s inherent inexperience, vulnerability or credulity or place undue influence or pressure on a child to make a purchase.
- Companies should not include direct exhortations to children to make a purchase or persuade others to make purchases for them.
- Payments should not be taken from the payment account holder unless express, informed consent for that specific payment has been given by the account holder.
- (See: https://www.gov.uk/government/publications/principles-for-online-and-app-based-games).

**Transparent advertising and compliance with the CAP Code.** Ensuring advertising if transparent and complies with the Advertising Standards Agency's CAP Code, for example, making sure influencers that are paid to promote a game disclose the fact they have been paid.

(See: https://www.asa.org.uk/codes-and-rulings/advertising-codes/non-broadcast-code.html)

**Compliance with consumer law.** Comply with all applicable consumer law including the Digital Markets, Competition and Consumers Act.

**Constant review of industry guidance.** Games companies should keep information and guidance published by TIGA under review at https://tiga.org/about-tiga-and-our-industry/consumer-advice.

**P.3. Safeguarding Online Communities**

*Manage gaming platforms in a responsible manner by prioritising player wellbeing. Make every effort to ensure that online communities and interactions are safe and do not expose players to harm, in addition to complying with online safety laws such as the UK's Online Safety Act and the EU's Digital Services Act.*

**Online safety and terms.** Ensure terms and conditions with users contain all information required by online safety laws including how players are protected from online harms.

**Acceptable behaviour standards.** Make explicitly clear the standard of behaviour required and behaviour that will not be accepted and enforce these standards.

**Prevent illegal behaviour.** Take steps to understand and assess the risks of potential illegal behaviour players might be subjected to and take additional measures to prevent and take down illegal content in online communities. These harms include, amongst other things, child sexual exploitation and abuse, terrorist activity, organized immigration crime, extreme and revenge pornography, harassment and cyberstalking, hate crimes, encouraging or assisting suicide, drugs and firearms offences, offences relating to illegal immigration and human trafficking, offences relating to the proceeds of crime and fraud, incitement of violent, sale of illegal goods/services, accessing content illegally uploaded from prisons and the distribution of indecent images by under 18s.

**Prevent online harms.** Take steps to understand and assess the risks of potential online harms players might be subjected to and take additional measures to prevent and take down harmful content. These harms include, amongst other things, cyberbullying and trolling, extremist content and activity, coercive behaviour, intimidation, disinformation, violent content, advocacy of self-harm, the promotion of female genital mutilation and other physical or psychological harms.

**Clear complaints system.** Provide clear, effective, easily accessible complaints and reporting procedures and tools for players to use and protect themselves online. Ensure appropriate and timely action is taken in response to complaints.

**Player management system.** Set up proportionate systems to manage players' behaviour online, including appropriate systems, procedures, technologies and investment, including in staffing, training and support of human moderators.

**Assist law enforcement.** Comply with any requests by law enforcement where doing so is in accordance with legal obligations and duties. For example, assisting law enforcement where a specific threat to the safety of children has been identified and support investigations to bring criminals who break the law in online games to justice.

**Effective user reporting.** Take prompt, transparent and effective action following user reporting, including by imposing proportionate sanctions on players who breach behaviour policies in an appropriate timeframe.

**Effective governance.** Ensure an effective governance regime is in place to ensure online safety duties are complied with. Set standards and expectations for employees around protecting players from risks or harmful or illegal behaviour.

**Safety technology.** Purchase or develop safety technologies to address online safety risks and assist with identifying, flagging, blocking or removing illegal or harmful content.

**Records of harmful content.** Keep appropriate records of risk assessments, reports of illegal and harmful content and behaviour, including the number of reports received, how many of those reports led to action and what the action taken was.

**Support for users.** Provide information to users who have suffered online harm about appropriate sources of support.

**Review efforts to tackle online harms.** Regularly review efforts in tackling online harms and adapt online processes to drive continuous improvement.

**User protection from harm by design.** Include features of game design to mitigate the risks of harmful or illegal online behaviours, for example, by enabling players to mute, make invisible and not be impeded by the avatars of those who are harassing them (while respecting the limitations of a player vs player environment).

**Compliance with online safety laws.** Comply in full with the spirit and letter of online safety laws and codes such as the UK's Online Safety Act and the EU's Digital Services Act.

**P.4. Data Protection**

*Take appropriate and proportionate measures to fulfil the seven data protection principles under the General Data Protection Regulation (GDPR) and comply with all other relevant data protection laws and associated codes of practice to ensure that players' rights to personal data privacy are respected. Go beyond complying with basic data protection principles, where games are aimed at children.*

**Compliance with GDPR.** Comply in full with the spirit and letter of the data privacy law enshrined in the General Data Protection Regulation (GDPR)'s seven core principles, which can be summarised as follows:

- Lawfulness, fairness and transparency – personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
- Purpose limitation – personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data minimisation – personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accuracy – personal data shall be accurate and, where necessary, kept up to date.
- Storage limitation – personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.
- Integrity and confidentiality (security) – data shall be processed in a manner that ensures appropriate security, including protection against loss or unauthorised use.
- Accountability – the controller shall be responsible for, and be able to demonstrate compliance with, the above principles.

**Data protection at heart of game design.** Be responsible for placing data protection at the centre of the design of online services and games so that the requirements of applicable data protection legislation, codes of practice and guidance are embedded in the design.

**Undertake Data Protection Impact Assessments (DPIAs).** Undertake DPIAs and have them approved by the ICO where high risks persist.

**Data subject rights.** Ensure players can easily exercise their privacy rights including the right to be informed, right to access, right to rectification, right to erasure, right to data portability, right to object and right to not be subject to automated decision-making including profiling) .

**Policies and procedures.** Ensure that policies and procedures are in place that demonstrate how the games business complies with data protection obligations, including data protection and IT security policies and provision of training for relevant staff involved in the design and development of games.

**Transparent use of personal data.** Where players provide games companies with personal data in order to access online games and services, players should be able to understand how their personal data is processed and why, usually via a privacy notice. Where non-essential cookies or similar technologies are used as part of a game (typically a mobile game), then a cookies notice and compliant cookie banner is also required.

**Data security.** Put in place appropriate technical and organisational measures to keep data secure against personal data breaches.

**Accountability with third party providers.** Ensure contractual protection is in place with third-party suppliers who process data on their behalf and carry out due diligence before engaging third parties to ensure they have appropriate security measures in place.

**P.5. Spending and Time Management**

*Enable players to manage the amount of time and money spent on games through appropriate design and proportionate measures.*

**Spending and time controls.** In the case of game companies operating closed game platforms, provide controls to enable players and/or their parents and guardians to monitor and also to restrict the overall amount of money and time spent within each game and on the platform as a whole. In the case of games available on an open platform, consider introducing such controls where proportionate and technically practical. Drive awareness and uptake of such spending and time controls.

**Independent time management**. Where proportionate and technically practical, include game design features that enable and encourage players to be able to manage the time spent within the game, for example:

- enabling players to save a single-player game regularly;
- designing multiplayer games so that they do not require long individual play sessions to avoid being penalised, or provide alternatives, such as the possibility of substituting another player during an extended session; and
- including features such as reminder messages to take breaks; rest systems (where characters continue to progress while the player takes time away from the game); and time limitation structures (e.g. player has a specific time limit to complete a level in order to encourage shorter periods of play).

**Self-exclusion.** Where proportionate and technically practical include the function for players to self-exclude from further spending any more money or time on a game for a set period of time.

**Spending caps.** Where proportionate and technically practical, allow players to set an in-game spending cap for any in-game purchases, whether daily, weekly, monthly or a combination of the foregoing.

**Track spending.** Allow players to track their spending on in-game purchases, including lifetime spending on the game and by providing the option for periodic emails or other communications to remind players what they have spent.

**Analysing spending.** Where proportionate and technically practical, obtain anonymised data relating to spending for use in analysing typical amounts of spending, frequency of spending and patterns of spending, for use in independent research and for assisting players with managing their spending (while protecting any sensitive commercial information at all times).

**Monitoring.** Introduce processes and systems to monitor and protect individual levels of in-game spending (to the extent technologically and legally practical, and where proportionate). Where spending indicates patterns of spending that are not typical for that individual or for players as a whole, consider sending automated reminders to players, having a cooling-off period where no further spending is possible or other appropriate and proportionate measures.

**Disclosure of loot boxes**. Comply with all laws relating to loot boxes. Where legal to offer loot boxes, comply with best industry practice and voluntary industry codes by utilising responsible design to allow players (and guardians) to make informed decisions. Disclose the use of paid or hard currency loot boxes (or other chance systems) up-front before a player purchases, downloads or signs up to a game and describe their potential contents and the chances of that content being received in simple and easy to understand language. Consider approaches which provide a de facto cap on expenditure, for example, through the use of finite loot box collections.