On-demand programme services ("ODPS") guidance

Guidance for ODPS providers on measures to protect users from harmful material.

Publication date: 10 December 2021

Contents

Section

1. Overview

This document sets out Ofcom's guidance on the responsibilities of on-demand service providers with regard to harmful material under section 368E of the Communications Act 2003 ("the Act")[1].

The guidance reflects changes to the regulatory framework which came into force on 1 November 2020 and include a new requirement on ODPS providers to take appropriate and proportionate measures to ensure that any material that might impair the physical, mental or moral development of persons under the age of 18 is not normally seen or heard by them. The guidance should be read alongside Ofcom's Statutory Rules and Non-Binding Guidance for Providers of On-Demand Programme Services (ODPS) which sets out in full the statutory requirements with which providers of ODPS must comply and guidance on the administrative rules and those concerned with sponsorship and product placement.

The guidance in brief

Ofcom has produced this guidance for ODPS providers on the updated regulatory requirements with regard to harmful material. The guidance provides detail about the kinds of material that are prohibited on ODPS (including material likely to incite hatred and material which would be refused a classification by the BBFC). Our guidance also sets out measures which may be appropriate for protecting users from other potentially harmful material, and how these may be best implemented. These include:

- applying robust age verification measures for pornographic material; and
- for other material that might impair the physical, mental or moral development of persons under the age of 18, implementing measures such as age ratings, content warnings and parental controls that are proportionate to the potential harm of the relevant material to under-18s.

[1] As amended by the Audiovisual Media Services Directive Regulations 2009, 2010 and 2020.

2. Background and legislative context

Purpose of the guidance

2.1 This document sets out Ofcom's guidance on the responsibilities of on-demand service providers with regard to harmful material under section 368E of the Communications Act 2003 ("the Act") [2]. It replaces our previous guidance on harmful material for providers of on-demand programme services, which was withdrawn on 1 November 2020.

2.2 The guidance reflects changes to the regulatory framework which came into force on 1 November 2020 and sets out how Ofcom will apply the requirements set out in section 368E of the Act. In drawing up this guidance we have had regard to relevant Articles and Recitals of the Audiovisual Media Services Directive[3]. The guidance relates only to the rules relating to harmful material, a full description of the statutory provisions applicable to ODPS can be found in Ofcom's Statutory Rules and Non-Binding Guidance for Providers of On-Demand Programme Services (ODPS).

2.3 The guidance is designed to help ODPS providers understand the changes to requirements relating to harmful material and their responsibilities with regard to the measures that may be appropriate to ensure specially restricted material is not available to under-18s. In some places it sets out what ODPS providers "should do" or "should consider" when implementing measures. These are not prescriptive requirements but intended as helpful suggestions to aid understanding of how compliance could be achieved. In order to reflect the diversity of the sector and the importance of technological innovation, the guidance affords ODPS providers flexibility in how they protect their users without specifying or endorsing any specific technological standards or procedures.

Legal framework

2.4 On-demand programme services ("ODPS") are a category of video on-demand service regulated under Part 4A of the Communications Act 2003 ("the Act"). Part 4A has been amended to reflect revisions made to the EU framework for on-demand services under the Audiovisual Media Services Directive 2018 (the "AVMSD")[4]. The AVMSD governs EU-wide coordination of national legislation on all audiovisual media, both traditional TV broadcasts and on-demand services, and now also extends to video-sharing platforms ("VSPs")[5].

[2] As amended by the Audiovisual Media Services Directive Regulations 2009, 2010 and 2020.
[3] https://eur-lex.europa.eu/eli/dir/2018/1808/oj
[4] Part 4A was amended by the Audiovisual Media Service Directive Regulations 2020 which came into force on 1 November 2020.
[5] For more information about VSP regulation see: https://www.ofcom.org.uk/tv-radio-and-on-demand/information-for-industry/vsp-regulation

2.5 The AVMSD regulatory framework under Part 4A of the Act has been retained in UK law following the UK's withdrawal from the EU, although the criteria for establishing jurisdiction have been amended to clarify when an ODPS will fall under UK jurisdiction[6].

2.6 Section 368E of the Act sets out the responsibilities of on-demand service providers with regard to harmful material.

2.7 The structure of the guidance presented in this document is as follows:

- Section Three – guidance around subsection 1 of section 368E of the Act, regarding material likely to incite violence or hatred.
- Section Four - guidance around subsections 2 and 3 of section 368E of the Act, regarding prohibited material.
- Section Five - guidance around subsections 4 to 7 of section 368E of the Act, regarding the protection of under-18s from specially restricted material.

2.8 This document is only intended to provide guidance on the interpretation and application of Rules 10, 11 and 12 of the ODPS rules. A list of all statutory requirements applicable to ODPS can be found here alongside our guidance on the editorial rules relating to sponsorship (Rule 13) and product placement (Rule 14) as set out in sections 368G and 368H of the Act, and the administrative rules (Rules 1 to 9) set out in sections 368BA and 368D of the Act. Our guidance in these areas has not been updated as the legislative revisions have not substantively altered the relevant requirements.

[6] See: The Broadcasting (Amendment) (EU Exit) Regulations 2019

3. Harmful Material: Material likely to incite violence or hatred

3.1 Section 368E(1) of the Act requires that an ODPS must not contain any material likely to incite violence or hatred against a group of persons or a member of a group of persons based on any of the grounds referred to in Article 21 of the Charter of Fundamental Rights of the European Union of 7 December 2000, as adopted at Strasbourg on 12 December 2007.

Guidance

3.2 The grounds referred to in Article 21 of the Charter of Fundamental Rights of the European Union of 7 December 2000, as adopted at Strasbourg on 12 December 2007 are: sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

3.3 ODPS providers will need to ensure their policies take into account both "incitement to violence" and "incitement to hatred". With respect to the latter, "hatred" should be understood as referring to a feeling of animosity or rejection with regard to a person or a group of persons targeting one or more of the protected characteristics listed above. ODPS providers should ensure that any compliance approach relating to incitement policy is not limited to encompass only examples of incitement to violence.

3.4 When determining the appropriateness of the measures taken by ODPS providers, Ofcom will have regard to relevant case law on freedom of expression, which includes the case law of the European Court of Human Rights (ECHR)[7]. In September 2020, the ECHR published a factsheet summarising some of its cases on incitement to hatred, which may be helpful to providers.

3.5 ODPS providers need to be aware that whether content is likely to incite violence or hatred will vary depending on the nature of the protected characteristic, the negative stereotypes that exist and the social context. In assessing whether content is "likely" to incite violence or hatred amongst general users and against the targeted group or person with particular protected characteristics, providers should pay attention to the potential effect of such content.

[7] ECHR cases can be found here.

4. Harmful Material: Prohibited Material

4.1 Section 368E(2) of the Act requires that an ODPS must not contain any prohibited material.

4.2 "Prohibited material" is defined in Section 368E(3) of the Act as:

a) material the inclusion of which in an on-demand programme service would be conduct required by any of the following to be punishable as a criminal offence—

i) Article 5 of Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism[8],

ii) Article 5(4) of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography[9], or

iii) Article 1 of Council Framework Decision (2008/913/JHA) of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law[10]";

b) a video work which the video works authority[11] has determined for the purposes of the 1984 Act[12] not to be suitable for a classification certificate to be issued in respect of it; or

c) material whose nature is such that it is reasonable to expect that, if the material were contained in a video work submitted to the video works authority for a classification certificate, the video works authority would determine for those purposes that the video work was not suitable for a classification certificate to be issued in respect of it.

4.3 In determining whether any material falls within (c), the Act requires that regard must be had to any guidelines issued by the video works authority (the British Board of Film Classification) as to its policy in relation to the issue of classification certificates.

Guidance

4.4 Material prohibited on ODPS includes:

- material which would be a criminal offence to publish, distribute or disseminate under laws relating to terrorism; child sexual abuse material ("CSAM"); and racism and xenophobia; and
- video works which have been refused a classification by the BBFC, and material which if included in a video work would be refused a classification by the BBFC.

[8] OJ No. L 88, 31.3.2017, p. 6.
[9] OJ No. L 335, 17.12.2011, p. 1.
[10] OJ No. L 328, 6.12.2008, p. 55.
[11] The British Board of Film Classification ("BBFC") is currently designated as 'the video works authority'.
[12] The Video Recordings Act 1984

Terrorism

4.5 The ODPS rules refer to Article 5 of Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism, which requires prohibition of any statement directly or indirectly encouraging terrorism or that is likely to be understood as such. It is irrelevant whether any person is in fact encouraged or induced by the statement to commit, prepare or instigate a terrorist act.

4.6 Statements that are likely to be understood as indirectly encouraging the commissioning or preparation of acts of terrorism include every statement which glorifies the commission or preparation (whether in the past, in the future or generally) of such acts or offences.

Child Sexual Abuse Material

4.7 The ODPS rules refer to Article 5(4) of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography ("the CSEA Directive").

4.8 We consider the offences under the CSEA Directive most relevant for ODPS providers to be related to the distribution, dissemination or transmission of child pornography. The definition of child pornography is set out in Article 2 of the CSEA Directive and extends to the depiction of any person appearing to be a child as well as realistic images. It also includes simulated activity. Ofcom will generally refer to this as child sexual abuse material ("CSAM")[13].

Racism and Xenophobia

4.9 The ODPS rules refer to Article 1 of Council Framework Decision (2008/913/JHA) of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.

4.10 The offences relating to racism and xenophobia here include publicly inciting violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin, and the committing of such an offence by public dissemination or distribution of tracts, pictures or other material.

4.11 Also included are offences related to publicly condoning, denying or grossly trivializing crimes of genocide, crimes against humanity, war crimes and other specified crimes[14], directed against a group or group of persons defined by the characteristics in 4.10 above, where the conduct is carried out in a manner likely to incite violence or hatred against such a group or a member of such a group.

---

[13] 'Child pornography' reflects the language used within the legal framework for this regime, but this is no longer commonly used in the UK. Children's advocates tend to use the term child sexual abuse material.
[14] These other specified crimes are crimes defined in Article 6 of the Charter of the International Military Tribunal appended to the London Agreement of 8 August 1945.

Material which has been, or would be, refused a classification by the BBFC

4.12 Content which complies with the Ofcom Broadcasting Code, or that has been classified by the British Board of Film Classification (BBFC) in any category, including R18, would not be considered 'prohibited material'.

4.13 Video works which have been refused a classification by the BBFC, and material which if included in a video work would be refused a classification by the BBFC, is 'prohibited material' and cannot be included in an ODPS in any circumstances. All 'material' on the service, including still images and other non-video content is subject to this requirement.

4.14 There is no requirement for material being provided on an ODPS to be classified by the BBFC, but where material has not been classified, Ofcom is required to have regard to the BBFC Classification Guidelines when determining whether it is reasonable to expect that such material when included in an ODPS is material which, if contained in a video work submitted to the BBFC, would be refused a classification.

4.15 For further information on the guidelines issued by the video works authority see the BBFC's website at https://www.bbfc.co.uk/about-classification/classification-guidelines . Providers may also contact the BBFC directly via their website for additional guidance.

4.16 Having regard to the current BBFC Classification Guidelines, the following comprises a non-exhaustive list of the types of material which **may** constitute prohibited material:

a) Material in breach of the criminal law (including material judged to be obscene under the current interpretation[15] of the Obscene Publications Act 1959) or that has been created through the commission of a criminal offence[16];

b) Material or treatment which risks harm to individuals or, through their behaviour, to society.[17] For example:

i) material which may actively promote illegal behaviour;

ii) detailed portrayals of violent or dangerous acts, or of illegal drug use, which may cause harm to public health or morals;

iii) portrayals of potentially dangerous behaviour (especially relating to suicide, self-harm and asphyxiation) which children and young people may potentially copy;

iv) material which makes sadistic violence, rape or other non-consensual sexually violent behaviour look appealing; or reinforces the suggestion that victims enjoy rape or other non-consensual sexually violent behaviour; or invites viewer complicity in rape, other non-consensual sexually violent behaviour or other harmful violent activities; and

[15] The Crown Prosecution Service publishes guidance on current interpretation of the Obscene Publications Act at http://www.cps.gov.uk/legal/l_to_o/obscene_publications/#a05

[16] BBFC Classification Guidelines 2019, p28

[17] BBFC Classification Guidelines 2019, pp10, 13, 26 and 31

v) material which is so demeaning or degrading to human dignity (for example, it consists of strong abuse, torture or death without any significant mitigating factors) that it may pose a harm risk; or

c) Material in pornographic works[18] which:

i) is likely to encourage an interest in sexually abusive activity, which may include adults role-playing as non-adults and may include dialogue as well as images;
ii) portrays sexual activity which involves real or apparent lack of consent. Any form of physical restraint which prevents participants from indicating a withdrawal of consent;
iii) involves the infliction of pain or acts which are likely to cause serious physical harm, whether real or (in a sexual context) simulated. Some allowance may be made for non-abusive consensual activity;
iv) involves penetration by any object likely to cause physical harm; or
v) involves sexual threats, humiliation or abuse which do not form part of a clearly consenting role-playing game.

[18] BBFC Classification Guidelines 2019, p28

5. Harmful Material: Protection of Under-18s (Specially Restricted Material)

5.1 Section 368E(4) of the Act requires that a person providing an on-demand programme service must take appropriate measures to ensure that any specially restricted material is made available by the service in a manner which secures that persons under the age of 18 will not normally see or hear it.

5.2 Section 368E(4A) of the Act requires that the measures are to be proportionate to the potential of the material to harm the physical, mental or moral development of such persons.

5.3 As the appropriate regulatory authority, Ofcom must draw up, and from time to time review and revise, guidance for providers of on-demand programme services concerning measures that may be appropriate for the purposes of section 368E(4) (ensuring specially restricted material is not available to under-18s).

5.4 "Specially restricted material" is defined in Section 368E(5) as:

a) a video work in respect of which the video works authority[19] has issued an R18 classification certificate;

b) material whose nature is such that it is reasonable to expect that, if the material were contained in a video work submitted to the video works authority for a classification certificate, the video works authority would issue an R18 classification certificate; or

c) other material that might impair the physical, mental or moral development of persons under the age of 18.

5.5 In determining whether any material falls within (b), regard must be had to any guidelines issued by the video works authority as to its policy in relation to the issue of classification certificates.

Statutory definitions relevant to Rule 12 – section 368E(7):

5.6 As follows:

- "the 1984 Act" means the Video Recordings Act 1984;
- "classification certificate" has the same meaning as in the 1984 Act (see section 7 of that Act[20]);
- "R18 classification certificate" means a classification certificate containing the statement mentioned in section 7(2)(c) of the 1984 Act that no video recording containing the video work is to be supplied other than in a licensed sex shop;

[19] The British Board of Film Classification ("BBFC") is currently designated as 'the video works authority'.
[20] https://www.legislation.gov.uk/ukpga/1984/39/section/7

- "the video works authority" means the person or persons designated under section 4(1) of the 1984 Act as the authority responsible for making arrangements in respect of video works other than video games; and
- "video work" has the same meaning as in the 1984 Act (see section 1(2) of that Act).

Guidance

5.7 In considering any particular case, Ofcom's approach in the first instance will be to determine whether the content in question falls within the definition of "specially restricted material".

5.8 R18 and R18-equivalent material and any other material which might impair the development of under-18s is subject to the requirements of this section. All 'material' on an ODPS, including still images and other non-video content is subject to this requirement.

R18 and R18-equivalent material and other sex works

5.9 The R18 category is a special and legally-restricted classification issued by the British Board of Film Classification ("BBFC") primarily for explicit videos of consenting sex or strong fetish material involving adults, and where the primary purpose of the material is sexual arousal or stimulation.

5.10 There is no requirement for material being provided on an ODPS to be classified by the BBFC, but Ofcom is required to have regard to the BBFC Classification Guidelines when determining whether material on an ODPS is R18-equivalent. R18-equivalent material is material whose nature is such that it is reasonable to expect that if it was submitted to the BBFC for a classification certificate, the BBFC would issue an R18 classification certificate.

5.11 Other material that has either been issued, or would be likely to be issued, an 18 classification certificate as a "sex work" by the BBFC will also be regarded by Ofcom as restricted material of a pornographic nature and should be subject to the same restrictions as R18 or R18-equivalent material.

5.12 When an ODPS provider is considering whether its service contains specially restricted material which would be likely to be issued an 18 classification certificate by the BBFC or not, it should have regard to the BBFC's definition of such material as works whose primary purpose is sexual arousal or stimulation.

5.13 For more information on the R18 certificate, sex works issued with an 18 classification certificate and the type of content likely to be awarded these certificates, see pages 26 and 28 of the British Board of Film Classification's Guidelines on their website: https://www.bbfc.co.uk/about-classification/classification-guidelines. It is the responsibility of ODPS providers to ensure that they are aware of any changes to the BBFC's guidelines.

Other "specially restricted material"

5.14 In assessing the broad range of material that might impair the physical, mental or moral development of under-18s, ODPS providers should also consider whether the material is age-appropriate for its users. To support this approach, it may be useful to understand the strength and types of material that the BBFC regards as appropriate for different age groups in its classification guidelines.[21]

5.15 Material which might impair the physical, mental or moral development of under-18s is likely to evolve over time and ODPS providers should ensure they remain informed about changing attitudes.

5.16 This guidance notes a non-exhaustive range of other material that might impair the physical, mental or moral development of under-18s. ODPS providers should consider, for example, if any of the following could be relevant to the material available on their service:

- Sexual material
- Violence
- Depictions of dangerous behaviour (including the use of illegal drugs and the misuse of alcohol)
- Material portraying eating disorders, self-harm or suicide[22]
- Abusive and offensive language
- Exorcism, the occult or the paranormal

Appropriate measures

5.17 Provided the material is not illegal or otherwise prohibited (see Section 3), content which is likely to fall under this section (i.e. 'specially restricted material') may be made available by an ODPS provided access is controlled by appropriate measures to secure that people aged under 18 'will not normally see or hear' such material. The principle applies that specially restricted material that has the most potential to harm must be subject to the strictest access control measures.

5.18 An ODPS is defined by reference to it being a service provided by a person with 'editorial responsibility'. A person has editorial responsibility if they have general control over what programmes are included in the service and the manner in which those programmes are organised.

5.19 Having general control over the selection of material available on their service means that ODPS providers are in a position to review all their content and identify any content which may meet the definition of specially restricted material ahead of it being made available to

[21] See age ratings issues in BBFC Classification Guidelines. Providers may also contact the BBFC directly for additional guidance.

[22] As set out in the BBFC Classification Guidelines, material promoting dangerous behaviour (especially suicide, self-harm and asphyxiation) which children or young people may potentially copy may be refused a classification. Such content would therefore be considered 'prohibited material'. See paragraph 4.16

users. Accordingly, we expect ODPS providers to consider implementing measures that have a particular focus on preventing under-18s from accessing the strongest specially restricted material and providing parents and carers with the tools to make informed decisions about the content their children are able to access.

Preventing access to specially restricted material of a pornographic nature for under-18s

5.20 The Act requires that the measures implemented by ODPS providers to ensure that under 18s will not normally see or hear specially restricted material are proportionate to the potential of the material to harm the physical, mental or moral development of under-18s. Ofcom's interpretation of this requirement is that for pornographic material (including R18 and R18-equivalent material and 18-level "sex works"), there should be in place robust age verification measures that either operate as an age-gate to block users from the entire platform or to filter material in a way that can protect under-18s. This should be an age verification system which verifies that the user is aged 18 or over and prevents under-18s from accessing the pornographic service.

5.21 Traditional examples of age verification include solutions such as matching a user to their official age on their passport, driving licence or credit card. However, we do not currently recommend or endorse any specific technological tools or methods that an ODPS provider could use to restrict access to pornographic material, though the chosen access control measure(s) should be effective in preventing access to that material for under-18s. We expect providers to stay informed of emerging technological developments and solutions for online safety and to consider these as part of their ongoing assessment of the measures that are appropriate for their service[23].

5.22 ODPS providers should seek to provide users with a clear understanding of the age verification method(s) that they are being asked to use on the service and, if more than one method is available, accurate information on the choice of those methods.

5.23 Ofcom would not consider the following forms of age verification to be appropriate protection measures for the strongest specially restricted material:

- Self-declaration of date of birth or a 'tick box' system to confirm that the user is over the age of 18;
- General disclaimers asserting that all users should be deemed to be over the age of 18;
- Relying on age verification through online payment methods which may not require a person to be over the age of 18, e.g. Debit, Solo or Electron cards or any other card where the card holder is not required to be over the age of 18;
- Relying on publicly available sources or otherwise easily known information such as name, address and date of birth to verify the age of a user. This does not include electoral roll information, which is a valid data source for age verification.

[23] Age Verification Providers Association is the industry trade body for UK age verification providers. Its members are developing a range of solutions that an ODPS provider might consider implementing.

5.24 Responsibility for ensuring that any required age verification system is in place and is operating effectively rests at all times with the person with editorial responsibility for the ODPS. The 'Guidance on who needs to notify' document provides further detail on how to determine the person with editorial responsibility for the ODPS.

Other specially restricted material

5.25 When considering appropriate measures to ensure that other specially restricted material (ie. material which is not pornographic in nature but which may still impair the physical, mental or moral development of under-18s) will not normally be seen or heard by under-18s, ODPS providers should take into account the following:

- The potential of the material to harm under-18s
- The likely degree of harm caused
- The likelihood of under-18s accessing the material
- The nature of the ODPS and its likely audience
- The age of any under-18s likely to access the material.

5.26 What measures are appropriate and proportionate will vary in each case. However, such measures may include the use of:

- Age ratings or other classification systems
- Content warnings and information
- Parental controls, including restricted mode settings and PIN protection
- Age assurance, including age verification.

5.27 It is important to note that where a measure is taken, it must be implemented in such a way as to carry out the requirement to protect under-18s from specially restricted material.

5.28 Ofcom recognises that there is a broad range of services operating as ODPS and the nature of the content they provide is equally diverse. The systems and processes listed above are included by way of indicating the type of measures that may be used in ensuring that under-18s are suitably protected but not all measures will be appropriate for all ODPS. It is a matter for individual providers to determine which measures, or combination of measures, are appropriate in protecting under-18s, taking account of all the relevant factors.

Considerations for effective use of age ratings

5.29 The most basic way in which ODPS can use ratings systems to aid the protection of under-18s is to have a binary rating system, where content is tagged by the platform as, for example, "Mature" or "Caution". Some platforms may consider having more sophisticated ratings systems, where content is labelled with age-appropriate ratings.

5.30 Where ODPS providers are using their own framework for making rating decisions, the overall basis on which these decisions are made should be made clear to viewers.

5.31 An ODPS may rely on an existing age ratings framework such as the BBFC ratings system. We expect providers who choose to use existing, established age ratings frameworks on

their platforms to also ensure that this is done with the knowledge of the relevant ratings body. This is to promote consistency of established ratings standards, as well as to protect users who will rely on the accuracy of ratings information provided to them by the ODPS.

Content warnings and information

5.32 Providing warnings and information to users about the content of programmes is another measure that may be appropriate in helping secure that content that may impair the physical, mental or moral development of under-18s will not normally be seen or heard by under-18s. That is because they allow viewers to make more informed decisions about their viewing and the viewing of any under-18s they are responsible for. However, ODPS providers should bear in mind that such protection measures are most effective when combined with other protection measures that more robustly control the content that is available for access by under-18s. If there is a significant risk to under-18s posed by harmful material on a service, it may not be proportionate to regard content warnings and information as an appropriate measure without other more robust measures in place to protect younger and/or vulnerable under-18s.

Parental controls, including restricted mode settings and PIN protection

5.33 Parental control systems allow an adult responsible for a person under the age of 18 a degree of control over what content the child can see or hear. Providers who offer services to under-18s should strongly consider having some form of parental control feature to support their overall protection measures for under-18s.

5.34 There is a range of parental control features that ODPS are able to design and implement. Some ODPS have systems which allow the parent or carer to create an account for their child giving the parent or carer control over the type of content that their child can see. These systems may be used alongside age ratings information to allow parents and carers to more carefully tailor the content that is available for their children to view.

5.35 Parental control systems can allow guardians to set boundaries for the content that their children access on ODPS. In principle, they can be used as a way for parents to feel comfortable that their child is using an ODPS within safe parameters, rather than being an instrument for monitoring and control. As such, these tools can work most effectively where there is a trust-based dynamic between the parent or carer and the under-18. Where there is less trust in the parent/carer-child relationship and/or if the children have access to tools to circumvent parental checks, parental controls will be less reliable and successful.

5.36 Parents and guardians need to know what parental controls systems ODPS offer and understand how best to use them to support a child's use of ODPS. Providers could use guides and other media literacy tools alongside parental controls to support this awareness and understanding. ODPS may consider best practice from, and partnerships with,

organisations in the provision of media literacy tools. For example, the ICO and Internet Matters both provide guidance to help parents understand Parental Controls[24].

5.37 ODPS providers should be mindful that not all children in the UK have parents or guardians that are able to make use of parental controls to protect their children. For instance, parents with less familiarity with ODPS and the devices these services are made available on may find it difficult to apply parental controls effectively.

5.38 Parental control functions should not be easily circumventable by under-18s and ODPS providers should consider the use of passwords or PINs to ensure that the protection provided by parental control systems is robust.

5.39 Ofcom commissioned research in 2018 on consumers' use of and attitudes towards mandatory and voluntary PIN protection systems. The research found that awareness and usage of PIN systems was high, along with opinions on their effectiveness. The majority (85%) of parents of 11-15 year olds were confident that the PIN protection they had in place provided adequate protected viewing for their children. Most parents also considered mandatory PINs to be safer than voluntary PINs because with mandatory PINs the responsibility is taken away from the parent to set it up in the first place.[25]

Considerations for effective age assurance

5.40 As set out in paragraph 5.20, ODPS providers should have robust age verification measures in place to block under-18s from accessing material of a pornographic nature. For specially restricted material that is non-pornographic in nature, ODPS providers should put in place measures, which may include age assurance methods if appropriate, which are proportionate to the potential of the material to cause harm to under-18s.

5.41 **Age assurance** is a broad term that refers to the spectrum of methods that can be used to be informed about a user's age online.[26] Examples of age assurance cover a range of potential methods, from users self-declaring their date of birth to the use of face-recognition biometrics and computational methods. Other forms of age assurance may include trusted sources that point to a child's age, such as parental verification tools.

a) **Age verification** is a form of age assurance where a user's age is established to the greatest degree of certainty practically achievable and is currently therefore considered the strictest form of access control. It is likely to rely on data sources that can secure a high level of confidence in the information provided. Examples of age verification may include:

i) Hard identifiers (passport scans, credit details, driving license, electoral roll information);

[24] ICO Parental Controls Standard; Parental Controls & Privacy Settings Guides – Internet Matters.
[25] See Ofcom's Daytime PIN Research, Kantar Media, 2018.
[26] The development of the concept and definition of age assurance has been supported by the government-led Verification of Children Online research project (VoCO). More information on age assurance can be found in the VoCO Phase 2 report (November 2020)

ii) Third-party attribution, such as digital identity solutions, use of data held by third party organisations (e.g. credit card companies) to validate the claimed age of an individual, or single sign-on schemes that minimise the need for repeat authentication or verification.

b) **Age estimation** refers to methods that can estimate or infer a person's age, usually by algorithmic means. This may include, but is not limited to, the following techniques:

i) Biometric analysis, such as analysis of facial features, fingerprints, and retinal patterns to estimate age;

ii) Behavioural analysis, i.e. behaviour patterns of the user on the platform and their interaction with it (e.g. time, location of use) to determine likely age;

iii) Linguistic analysis, i.e. analysis of written language structure to evaluate age;

iv) Profiling, such as using a user's past activity or history to evaluate certain aspects relating to the user.

c) **Account confirmation** through the use of parental control software and mechanisms allows for existing account holders to confirm the age of a user.

d) **Self-declaration** is where a user states their age or date of birth but offers no further evidence to confirm the information. This is a measure that is easy to bypass by the user, who is able to enter the minimum age that allows access to a service that may carry age-inappropriate or harmful material for the actual age of the user.

5.42 ODPS providers may consider the following factors when establishing and operating age assurance systems:

a) When implementing age assurance, ODPS providers should consider how reliable and accurate any method is and what level of confidence it provides, in relation to the risk.

b) Age assurance measures that are easily integrated into existing platforms and avoid disrupting the user experience are likely to be more widely adopted and sustainable in the long term.

c) Some under-18s can provide false information to easily bypass age assurance measures, e.g. self-declaring to be 18 or over. ODPS providers should aim to have a robust and effective age assurance approach to account for and disincentivise this behaviour. Examples of this can range from neutral design of the date of birth request upon sign-up with no further chance to sign in if an underage declaration is made, to introducing hard identifiers or account verification for users who claim to be over 18.

d) ODPS providers should consider how different tools such as ratings and parental controls might interact with age assurance to provide greater confidence about the age of under-18 users.

5.43 When considering any of the protection measures under the ODPS Framework providers should have regard to privacy issues and GDPR requirements. This is likely to be of greater consideration for age assurance and age verification measures. We encourage providers to

consult the ICO's guidance on UK GDPR requirements and The Age Appropriate Design Code.

5.44 Given the nature of their service, the level of user interaction and the amount of information held about their users, it is likely that age assurance methods may be more commonly used by providers of VSPs rather than ODPS (other than those ODPS required to have age verification systems in place as they provide pornographic material). Given the constantly evolving technology in this area, ODPS providers considering using age assurance methods in order to protect under-18s may wish to refer to Ofcom's guidance to VSP providers.

Combining the use of multiple measures

5.45 The measures set out above may be particularly effective when used in combination with one another. For example, combining parental controls alongside an effective rating system can help ensure that under-18s cannot access restricted material (or parental controls allow the responsible adult to restrict access to the material). More sophisticated ratings systems involving multiple tiers allow the responsible adult to further tailor an appropriate experience on the ODPS.