

## **IWF Funding Council**

### **Code of Practice for Notice and Takedown of UK Hosted Content Within the IWF Remit**

- 1. Introduction**
- 2. Definitions**
- 3. Scope**
- 4. IWF Notice and Takedown Service**
- 5. Member Obligations**
- 6. Amendment process**
- 7. Document history**
- 8. Adjudication Process**
- 9. Sanctions and Remedies**
- 10. Appeal**

#### **1. Introduction**

This Code of Practice (The Code) defines the 'Notice and Takedown' procedure by which service providers remove or disable access to potentially illegal content<sup>1</sup> hosted on their networks or on Usenet Services they provide, following receipt of a Notice from the Internet Watch Foundation (IWF).

The Code expects the IWF to assess content to a rigorous standard, against appropriate legislation and consistent with training received. Notices are only issued where the IWF believes the material would be capable of sustaining a criminal prosecution if it were to be put before a jury.

Breaches of the Code may ultimately lead to suspension of membership of the IWF.

#### **2. Definitions**

**2.1** A breach is defined as a failure to comply with the process for removal of content outlined in this Code of Practice.

---

<sup>1</sup> Content within the IWF's remit.

## 2.2 E-Commerce Directive

Other terms used within the Code are consistent with those in the Electronic Commerce (E-Commerce) Directive 2000/31/EC.

## 3. Scope

The Code governs those Full Members of the IWF that host content in the UK or provide Usenet services for their UK customers, either directly or under contractual arrangements with third parties. Such Full Members<sup>2</sup> are, hereinafter, referred to as Members. Such Members cannot opt-out of the Code.

The types of content covered by this code are those within the remit of the IWF.<sup>3</sup>

## 4. IWF Notice and Takedown Service

The IWF operates a notice and takedown service to issue Notices alerting hosting service providers (or Members – as described above) to content hosted on their servers in the UK that it has assessed as potentially illegal<sup>4</sup>.

## 5. Member Obligations

### *Contact Details*

Members must provide the IWF with a point of contact to which the IWF can send takedown Notices. This may be a nominated member of staff or dedicated mailbox set up to receive such Notices. In genuine emergency take down situations every effort should be made to establish person to person contact, by telephone for example, to back up the take down notice. It is the responsibility of each Member to notify the IWF of any change to its point of contact<sup>5</sup>.

### *Notice and Takedown*

Upon receipt of a Notice from the IWF, a Member must either

- act expeditiously to remove or disable access to the notified content, or

---

<sup>2</sup> This is defined in the Funding Council Constitution which can be found at: <http://www.iwf.org.uk/funding>

<sup>3</sup> This can be found at <http://www.iwf.org.uk/public/page.35.htm> and/or Appendix 1

<sup>4</sup> See earlier definition of Potentially illegal, P1

<sup>5</sup> The individual or mailbox nominated by the Member to receive notices from the IWF

- notify the IWF if the Notice appears to be improperly issued, incomplete or not applicable to the Member

Members who disregard a notice from the IWF do so at their own risk and will be in breach of this Code.

### *Newsgroups*

Members who provide a Usenet service to their customers will ensure those services are cleaned and updated on a periodic basis in accordance with IWF recommendations<sup>6</sup>. This includes Usenet services delivered under contractual arrangements with third parties.

## **6. Amendment process**

The Code may be amended only by agreement of the Full Members of the Funding Council in accordance with the Funding Council Constitution and with the agreement of the IWF Board.<sup>7</sup>

## **7. Document History**

Version	Date Published	Summary of Changes	Made by

## **8. Adjudication Process<sup>8</sup>**

### **8.1 Notification**

8.1.1 All notifications of a breach should be made to the IWF's Director of Policy and Performance or, in their absence, the Chief Executive of the IWF.

8.1.2 Such notifications will typically be referred internally by an IWF hotline analyst who becomes aware of a suspected breach through the operation of the notice and take down process. Notifications may also be flagged by a member company or a third party.

<sup>6</sup> IWF Newsgroup Policy can be found at Appendix 2

<sup>7</sup> See footnote 3, P2

<sup>8</sup> A flowchart depicting this process can be found at Appendix 3

8.1.3 The IWF will notify the Member company concerned of the suspected breach within 2 working days of the IWF becoming aware of the breach.

8.1.4 The IWF will maintain a confidential log of all suspected breaches that come to its attention.

## 8.2 Initial Inquiry

8.2.1 The Chief Executive of the IWF<sup>9</sup> will investigate a suspected breach and compile a report of initial findings. This report will outline the nature of the suspected breach, the salient facts and any mitigating circumstances.

8.2.2 On the basis of these initial findings the Member may agree with the Chief Executive that the matter can be fully and satisfactorily resolved without further action.

8.2.3 If the matter cannot be fully and satisfactorily resolved with the Member or requires further investigation and/or input from other parties, the Chief Executive may initiate a full inquiry.

8.2.4 The IWF will notify the Member concerned if a full inquiry is initiated about them.

## 8.3 Full Inquiry

8.3.1 The full inquiry will normally be completed within 15 working days from the date of notification to the Member (referred to in 8.2.4). In exceptional circumstances (eg if the matter being investigated is complex) the duration of the inquiry may be extended. A further period of a maximum of 7 working days may elapse between the completion of the full inquiry and the notification of any sanction to be applied.

8.3.2 The inquiry aims to determine whether a breach has occurred and, if it has occurred, the reasons for that breach. The inquiry will also seek to ascertain any mitigating actions taken by the Member in relation to the breach and reasons why the Member did not act on the notice in question. The inquiry will verify that the IWF has acted correctly and consistent with its agreed procedures.

8.3.3 All evidence collected as part of the inquiry will be recorded, auditable and disclosable to the Member subject to the inquiry.

---

<sup>9</sup> For the purposes of this document the Chief Executive could be a delegated member of the IWF Executive team

8.3.4 A representative(s) of the Member company and employees of the IWF will be invited to co-operate fully with the inquiry and provide written evidence and/or attend meetings in person.

8.3.5 If during the course of the inquiry, a dispute arises over the assessment of whether content is potentially illegal<sup>10</sup>, external professional advice, including reference to law enforcement agencies, may be sought.

8.3.6 The IWF will produce a report on the suspected breach. The Chief Executive is responsible for ensuring that the inquiry has been conducted appropriately and that the conclusions reached in the report are consistent with the evidence considered in the full inquiry. The Chief Executive will approve the final report and send a copy to the Member.

8.3.7 The Chief Executive may:

- a) Agree with the Member that the original notice was inaccurate or inappropriate or contained manifest errors, and that the matter is closed without the Member having to act on the notice;
- b) Agree with the Member that the matter is closed and that the Member will act on the original notice;
- c) Agree with the Member to refer the matter to the relevant law enforcement agency;
- d) Refer the matter to the Breach Sub-Committee of the Board if the Member will not comply with the original notice.

#### 8.4. Referral to IWF Breach Sub Committee

8.4.1 It is anticipated that most failures of the process can be remedied quickly without the need for formal proceedings (outlined above). However, if a Member is found to be in breach after a full inquiry, the Board (or relevant Sub- Committee) may decide to impose proportionate sanctions on a Member in order to secure their compliance.

8.4.2 Referrals received by the IWF Board pursuant to 8.3.7 (d) will be delegated for consideration to a Breach Sub-Committee of the Board which will be an ad hoc committee rather than a standing committee.

---

<sup>10</sup> See earlier definition of potentially illegal, P1

8.4.3 Any Breach Sub-Committee of the Board will comprise at least three people, with a ratio of 2:1 being maintained in relation to non-industry/industry membership. The Chair will be a non-industry trustee. The industry representative must not be employed by the Member company which is the subject of the case.

8.4.4 The inquiry by the Breach Sub-Committee will normally be completed within 15 working days from the date of notification to the Member (referred to in 8.3.7 (d)).

8.4.5 The Member shall be entitled to meet with the Breach Sub-Committee in person or by teleconference, depending on the Member's preference, and present its response to the final report per 8.3.6. The Member may be assisted by or represented by another person, including a legal advisor. The Member shall also be entitled to submit written evidence.

8.4.6 Members and employees of the IWF are expected to co-operate with any reasonable request from the Breach Sub-Committee to assist in obtaining evidence.

8.4.7 The Breach Sub-Committee will determine the facts and arrive at a decision and will then agree an appropriate sanction. The Breach Sub-Committee will consider the report from the Executive (referred to in 8.3.6) and may, if it considers appropriate, seek independent legal advice in respect of a case brought before it.

8.4.8 The IWF shall inform the Member of the Breach Sub-Committee decision within ten business days of the decision being made and shall provide details of the Breach Sub-Committee reasoning and any proposed sanction. This reasoning can be used as grounds for an appeal.

8.4.9 For the avoidance of doubt, if the Breach Sub-Committee finds that there was no case to answer then no further action shall be taken and the Member will be advised.

## 9 Sanctions and Remedies

9.1 If a Member is found to be in breach after a full inquiry the Breach Sub-Committee may decide to impose sanctions on a Member in order to secure their compliance.

9.2 Remedies and sanctions available to the Breach Sub-Committee for breaches are:

- (a) Request a formal, written undertaking as to future compliance
- (b) Issue of a warning or reprimand
- (c) Report filed with relevant law enforcement authority
- (d) Suspension from membership
- (e) Withdrawal of membership

9.3 If the Breach Sub-Committee levies either 9.2(d) or 9.2(e) in the list of remedies and sanctions then it may publish its adjudication on the IWF website. Other adjudications shall not be published.

9.4 When determining the level of any remedy or sanction the Breach Sub-Committee will consider a number of factors that will determine the most appropriate course of action. Recognising that each case is likely to have its own particular features, the factors which the Breach Sub-Committee may take into account include the following:

- (a) Whether the breach was inadvertent, negligent reckless or knowingly an act of commission or omission
- (b) Seriousness of the breach in terms of detriment to consumers or the wider public interest
- (c) Repetition or regular breaches or flouting of the rules
- (d) Mitigating actions taken by the Member or mitigating circumstances
- (e) Impact of the breach on the integrity of the IWF
- (f) Degree of co-operation with the IWF by the Member in connection with the identification and rectification of the breach
- (g) Relevant precedent, although the IWF Board will not be bound by precedent

9.5 IWF can recover reasonably incurred marginal costs<sup>11</sup> of the process from the Member concerned who is found to be in breach. These costs are limited to those reasonably incurred by third parties involved in the process.

## 10 Appeal

10.1 A Member may appeal against a decision of the Breach sub committee<sup>12</sup> that a breach has occurred and/or the sanction applied (per 8.4.8).

10.2 Notification of the intention to appeal must be made in writing to the Chair of the Breach Sub Committee within 10 working days of receipt of the outcome full inquiry of the Breach Sub-Committee and/or receipt of the notification to impose a sanction as per 8.4.8. If no notification is received the matter will be considered closed.

---

<sup>11</sup> Additional, marginal costs over and above usual staff resources such as Trustee attendance fees, research costs or external expert advice.

<sup>12</sup> As laid out in 8.4.7

10.3 The Board will use its best endeavours to hear an appeal within 15 days of the receipt by the Board of a notification of an intention to appeal. Those Board members who formed the Breach Sub-Committee may not be part of the Board meeting that considers the appeal.

10.4 The following are able to make representation in writing, by teleconference or in person (the Member is entitled to request a face to face meeting). The following are also able to give additional evidence to the Board.

- Chair of the delegated Board Breach Sub-Committee
- Representatives of the Member organisation
- The Chief Executive of the IWF

10.5 The Board can take external professional advice, including legal and law enforcement authority advice.

10.6 The Board is required to report its decision to the Member within 10 working days of the appeal having been determined. The Chief Executive of the IWF and, where relevant, other Board members will be advised of the decision also.

10.7 The Board decision made will be final and there will be no further appeal process.

## Appendices

### Appendix 1

#### IWF Remit

- Images of child sexual abuse hosted anywhere in the World
- Criminally obscene content hosted in the UK
- Incitement to racial hatred content hosted in the UK

### Appendix 2

#### Summary of Newsgroup Policy

##### Regularity and Names Policies

Regularity policy:

- The IWF recommends all ISPs serving UK customers not to host newsgroups which the IWF identifies as regularly containing child sexual abuse content. The agreed description of 'regularly' is "finding an average of at least 1% of images viewed to be potentially illegal and additionally applying a further test whereby in each of six consecutive monitoring rounds finding any potentially illegal content would lead to the immediate listing of the group".
- The IWF publishes monthly to ISPs a list of groups categorised as 'suspect' or under 'close monitoring' in relation to the regularity policy, with the status of those lists being emphasised

Names policy:

- The IWF recommends all ISPs serving UK customers not to host newsgroups which the IWF identifies as having names which are potentially illegal advertisements under Section 1(1) (d) of the Protection of Children Act 1978.
- The IWF Board will not publish the list of group names.

##### Other Policies

Advisory policy:

- The IWF advises all ISPs serving UK customers not to carry newsgroups that are associated with advocating or linking to content of a paedophilic nature.

Individual notices and takedowns:

- Potentially illegal content found in any newsgroups not listed is issued with a notice and takedown in accordance with established practice.

### Appendix 3

