

*Children's Charities' Coalition for Internet Safety*



Hamish MacLeod  
Consultant to Mobile Network Operators  
PO Box 34586  
London SE15 5YA

5<sup>th</sup> September, 2003

Draft Code of Practice for the Self-Regulation of New  
Forms of Content and Experiences on Mobiles

Response to consultation by  
02, Orange, T-Mobile, Virgin Mobile, Vodafone and 3

Dear Hamish,

Here are the comments we are making on the above draft. I begin with a short explanation of the origins of CHIS.

Yours sincerely,

A handwritten signature in black ink, appearing to read "John Carr".

## Children's Charities' Coalition for Internet Safety



What is CHIS?



The Children's Charities' Coalition on Internet Safety (CHIS) consists of seven of the UK's largest, professional child welfare charities: Barnardo's, ChildLine, Children's Society, National Children's Bureau, NCH, NCVCCO and NSPCC. Several of our members are represented on the Home Secretary's Internet Task Force and also on the DfES Internet Safety Strategy Group.



CHIS grew out of the joint work of the charities on a range of social policy issues connected with children's welfare. Increasingly, questions about children's safe use of the new technologies in general, and the internet in particular, were becoming more and more common so CHIS was formed in late 1999 to give our work in this area a specific focus.



In 2000 CHIS launched its *Agenda for Action* which set out a range of measures which we asked Government, ISPs, retailers and hardware manufacturers to take to make the Internet a safer place for children. These measures then included :



- Internet Service Providers should not facilitate access to Newsgroups containing child pornography on a regular basis, or to Newsgroups or chat rooms that suggest or encourage paedophile behaviour.
- Internet Service Providers should be required to ensure that any staff employed to moderate children's chat or other child orientated Internet services have been properly trained and police checked.
- A new and wholly independent body should be established which draws together representatives of children's organizations, consumer groups and other categories of Internet users, together with representatives of all parts of the Internet industry, MPs and the Government, to lead an informed debate on public policy towards the Internet.
- More research and development is needed to provide better, more robust and easier to use labeling, filtering and blocking software and other programmes to allow parents and others with responsibility for children to provide a safe Internet environment .
- Government should ensure that clear, mandatory and comprehensive guidelines are issued governing the safe use of the Internet in schools<sup>1</sup>

Happily many of the items on our agenda have now been met or are on course to be so.

<sup>1</sup> For a full version of the CHIS *Agenda for Action* see [www.nch.org.uk/chis](http://www.nch.org.uk/chis)

## Summary

1. We welcome the opportunity to comment on the draft code and applaud the efforts being made by the Mobile Network Operators (MNOs) to address issues of child safety, both generally and specifically in relation to the new mobile technologies which are destined for or have already arrived in the mass market in the UK.
2. We are on the cusp of a huge revolution in the way we will think about and use the Internet. The arrival of mass market mobile Internet access, linked to new online services provided by the MNOs and provided by or through versatile new handsets, promises an explosion of new opportunities. We can expect children and young people to adopt and use the new mobile technologies every bit as fully and enthusiastically as they have the existing mobile technologies.
3. Mobile phones have become a very important, highly personal possession for many millions of children and young people in the UK. In the busy modern world, the existing mobile technologies have been shown to play a very valuable part in family and school life and in establishing or maintaining communications between children and their friends. However, we have also noted various drawbacks e.g. bullying via SMS.
4. The new mobile technologies are likely to maintain all of the advantages, and disadvantages, of the existing mobile technologies but they also have the potential to introduce many enhanced features. In some respects these could contribute significantly to improving aspects of personal safety. However, they also bring new risks.
5. The industry should establish and maintain a mechanism to monitor and research how the new mobile technologies impact on child safety across the board.
6. In the draft code the MNOs seek to make a distinction between what they call *commercial* content, services and experiences and, as it were, “everything else” that will be available via their networks and devices.
7. What the MNOs call *commercial* in fact refers only to content, services and experiences available over their own networks which they supply themselves or through their business partners. The implication of this is that “everything else” that is available over the same networks is not commercial. This is a distinction which will not be easily understood by the wider public. It is also potentially misleading as it implies that the non-MNO provided services, contents or experiences which may be accessed via the MNOs’ devices and networks, are not somehow not connected with commercial activity and provide no financial benefit of any kind to the MNO. That is not the case.
8. We welcome the MNOs’ proposal to establish a rating system for their own content and then restrict access according to the proven age of the user, but we think the same logic should be extended to all services which may be accessible via the handset and the MNOs’ networks.
9. In the fixed Internet world it has been our longstanding view that every new PC sold into the family environment should come with safety software preinstalled and set to a high level of security. It is even more important that this policy is adopted in the mobile

world. Moreover ways should be found to make the protective software operative both at the network level and at the level of the individual handset.

10. It is our view that all un-moderated chat services and all adult content should be barred by default to under-18s both in respect of the MNOs' own provision and on the wider Internet. The MNOs are proposing to introduce an age verification system so the basic infrastructure to allow this to happen is clearly going to be put in place.
11. MNOs appear to have given little detailed consideration to the implications of the existing fixed internet industry's policy on traceability. We believe this is a hugely important oversight which ought to be addressed as a matter of urgency.
12. In the fixed internet world, where someone dials in to a server and the system detects that they have disabled or do not have CLI (Caller Line Identification) the functionality they can then access is severely restricted by default. This is part of the ISP world's contribution toward reducing the potential for users to abuse the cloak of anonymity. It allows the ISP, and if necessary the police, to pin point a physical location and the time at which certain transactions took place. This can be enormously helpful in an investigation and acts as a disincentive to potential criminals. With a pre-paid mobile, whose original owner may never have been authenticated in any way, this possibility simply would not exist. It would be highly regrettable if, through the medium of pre-paid mobiles phones, this important contribution to crime reduction by the fixed Internet world was effectively rendered obsolete (see the ICF's document *ChatWise StreetWise* [www.internetcrimeforum.org.uk](http://www.internetcrimeforum.org.uk)).
13. The MNOs should consider restricting the functionality accessible to pre-paid mobile phones where the owner has not been authenticated in a reliable way.
14. MNOs should accept that they have a direct and on-going responsibility to provide up to date information on child safety to parents and to children.
15. MNOs should take this opportunity to establish an industry-wide policy on dealing with the replacement of Pay as You Go telephone numbers with no loss of credit for children who have been illegally victimized via the MNOs' networks.

## 16. Some General Remarks

17. We are very grateful for the opportunity to comment on the Code of Practice for the Self-Regulation of New Forms of Content and Experiences on Mobiles (the draft code). There is no doubt that mobile telephones are hugely important to children and young people. The current levels of ownership of mobile devices are upwards of 90% in some age categories. Even among children as young as 5 years old, levels of ownership are significant, and still rising.<sup>1</sup>
18. The mobile telephone has become one of the most treasured and most important possessions of very many children and young people. It provides them with a personal connection to the rest of the world. It is a space and a place that they control. Mobile telephones have also proved to be a useful tool in many busy families, helping parents and children to stay in touch and helping children to stay in touch with their friends. They have contributed to helping keep some children safer in certain circumstances.
19. We have no reason to suppose that the next generation of devices and the supporting network services will not, sooner or later, achieve similar or even greater levels of ownership and usage. However the next generation of mobile networks and devices will not only reproduce and add to the existing body of services available through mobiles, they will also graft on hugely improved, always-on access to the Internet.
20. Thus, all of the known child safety concerns that exist in respect of the established, “fixed” Internet world, will soon arise in relation to a mobile device which, almost by definition, is going to be far less susceptible to parental control and supervision. This new configuration lends itself to new forms of impulsive and opportunist behaviours that will put children at risk in ways which are just not possible in the fixed Internet world, or at any rate are far less likely.
21. Indeed, there are potentially yet other services which could also become attached to the new devices and networks e.g. ones which utilise GPS technology, WiFi (802.11b and related), Bluetooth or other “bypass” technologies, and these will expand the potential for children being exposed to risks.
22. There is a sense, therefore, that we are at an important moment when, essentially, the mobile internet and mobile computing are both arriving simultaneously in the mass market. We are on the cusp of a huge revolution in the way we will think about and use the Internet. The wider implications of this development are potentially profound and, if the experience with the fixed Internet is anything to go by, the likelihood is that we have not, and cannot, anticipate all the twists and turns that lie ahead. Yet at the same time we must not make children the canaries in the cage. We should adopt a precautionary approach at least until we are clearer how things will go. We must try to think ahead and seek to develop a capacity to react swiftly as new issues emerge.
23. Thus we believe there is a case for the industry giving urgent consideration to establishing and funding an on-going initiative which monitors and advises on how the various mobile technologies are impacting upon the child safety agenda across the board, or how they are likely to. Such a new body could also become a focal point for

---

<sup>1</sup> See Sunday Times, 10<sup>th</sup> August, 2003, quoting a survey by youthMobile, suggesting that 11% of 5 year olds own mobiles, up from 2% in 2000. Ownership among 10-14 year olds has now reached 33%, up from 19%.

sharing research-based information and experiences across the networks. It would also become a natural point of contact, and hopefully a better-resourced point of contact, for the industry in future dealings and discussions on child safety. CHIS would be happy to co-operate in such a venture.

24. We welcome the MNOs' proposal to establish a rating system for their own content, services and experiences and then restrict access according to the proven age of the user, but we think the same logic should be extended to all services which may be accessible via the handset and the MNOs' networks.
25. In the fixed Internet world it has been our longstanding view that every new PC sold in to the family environment should come with safety software preinstalled and set to a high level of security. It is even more important that this policy is adopted in the mobile world. All un-moderated chat services and all adult content should be barred by default to under-18s both in respect of the MNOs' own provision and on the wider Internet. How this might be financed is a separate question but we think a way should be found to factor it into the overall cost of the service. Child safety should not be an optional extra.
26. We are aware that some of the MNOs are considering introducing protective software which will run at the network level. This means that anyone could use their handset to dial into another internet server and completely bypass the MNO's security systems. Alternatively, if they have a WiFi or Bluetooth enabled handset they could connect via a third party's internet connection and again bypass the network based security systems. This seems to us to be very unsatisfactory. Ways should be found to make the protective software, or at least key parts of it, work at the level of the individual handset.
27. At an early stage it would also be useful to start getting a clearer idea of how the MNOs intend to deliver the wider media literacy initiatives referred to or implied by different parts of the consultation document and which will give coherence to many of the document's stated aims. We appreciate that, once it is founded and operational, OFCOM will have an interest in this question but this ought not to be a factor which delays matters unduly, as least as far as the MNOs' responsibilities are concerned.
28. We believe that the education part of the code is crucial if parents and the public are going to understand the new services on offer and especially if parents are to be enabled to carry out their responsibilities as best they can in safeguarding their children from unsuitable content and contact. The commitment to provide information and advice is welcomed but we believe it is important that the final version of the code spells out in greater detail how the information and advice will be delivered.
29. Parents have already had to climb a mountain to understand the intricacies and vagaries of the fixed internet world, and not all of them succeeded as well as they would have wanted. Similar, if not greater, complexities now lie ahead with the mobile internet and thus an even greater effort is needed. The unhelpful distinction referred to earlier, between commercial and "non-commercial" implies that MNOs may only provide information and advice where it relates to their own services. Who will inform parents about the non-MNO provided services, content and experiences which their children will nonetheless be able to access through their networks and devices? Surely this should be an industry wide responsibility?

30. It is similarly unclear how, or to what extent, MNOs will carry out the informational role themselves or merely refer parents to other sources of information. We believe it is important that mobile operators offer separate and specific information and advice to parents about safety and their children. This should be separate from their general safety advice to customers. Education should be a continuous responsibility of mobile operators. It should begin at the point of purchase when parents are selecting a mobile phone. As a matter of routine customers should be asked if the mobile phone is intended for a child. Specific sections for parents on safety should be included in mobile phone manuals with easy to understand instructions. There should also be safety messages online and MNOs should accept that they have a continuing responsibility to keep existing customers informed of new services and developments affecting child safety.

### 31. Overview

32. The document repeatedly seeks to make a distinction between what it calls “commercial” services, content and experiences, all of which will be provided by the MNOs or their partners, and other items accessible from other sources e.g. via the Internet.

33. This distinction is one which will not be easily understood by the wider public. It is also potentially misleading as it implies that when the user is not accessing the MNOs’ services, content or experiences, they will be accessing “non-commercial” items, or items which provide no financial benefit to the MNO. That is not the case.

34. There will, of course, be considerable interest in and concern about the services, content and experiences for which the MNOs are directly, or at any rate more directly, responsible, but concern about how the Internet will interface with the networks and devices will be of at least equal, if not greater, interest and importance.

35. In other words how the Internet is going to work with and through the MNOs’ current and future networks and current and future devices will be central to many people’s concerns in this debate.

36. We think the document as a whole would therefore benefit from a clear and simple exposition, right at the very beginning, of the basic fact that the new networks and the new devices will provide access to what are, essentially, two types or classes of content, services and experiences:

- a. those which the MNOs themselves are providing or in which they have a direct commercial interest (Class A) and
- b. those which a handset user may be able to access or use via the MNOs’ devices and networks but which are provided by third parties who have no direct commercial relationship to the MNOs (Class B)

37. The above then sets the context within which the MNOs can proceed to discuss in a focussed and specific way the approach to self-regulating the content, services and “experiences” which the MNOs and their commercial partners are proposing to provide or facilitate, and their attitude towards “everything else”.

38. Thus, for the sake of clarity, the document could usefully divide itself into two distinct sections:

- a. one setting out MNOs' proposals in relation to Class A services, content and experiences and
- b. one setting out MNOs' proposals in relation to Class B services, content and experiences

39. Please also refer to our comments in paragraphs 22-25 (above) and in the Summary where you will see we believe both types of content should, by default, be subject to control for anyone below the age of 18.

40. We now turn to our comments on specific sections of the draft Code.

#### 41. Objectives

42. We are not sure the text is as clear as it could be in respect of paragraph 1 in the text box. We suggest the following instead:

“To make existing customers, and potential new customers, aware of, and provide access to, information intended to help them manage the consumption of services, content and experiences which might be accessed over or through our networks or devices, with particular reference to the usage of such networks or devices by persons under the age of 18.”

#### 43. The Code

44. We can see merit in the proposal to establish an independent body to rate content. We are agnostic as to who provides such a service, save to say that whoever does it ought to be demonstrably free of any significant financial ties to any of the players whose content they might find themselves rating. But see also our comments in paragraphs 22-25 and in the Summary i.e. while the MNOs may want to regulate their own content this should not divert attention away from the importance of having easy to use and effective control over other forms of content and services to which the MNOs’ devices and networks will provide access.

#### 45. Parental Controls - commercial services

- a. See our more general comments on this aspect in paragraphs 22-25 and in the Summary.
- b. See earlier references to the confusing notion of “commercial services” and the Internet.
- c. Could we not use a term other than “gating”? “Age verification” seems to say what is intended a lot more clearly.

#### 46. Parental Controls - Internet access

- a. See earlier comments about the unhelpful way the two are presented or distinguished from each other and also our comments in paragraphs 22-25.

#### 47. Combating new forms of nuisance or malicious communications

- a. As this document addresses concerns about children’s usage, might there be some merit in specifically mentioning the word “bullying”?
- b. Also we believe the industry should take this opportunity to establish an industry-wide policy on replacing telephone numbers for Pay as You Go users in general, or specifically for children who are Pay as You Go users, who can show they have been illegally victimized via the MNOs’ networks. They or their families should not be financially penalized because they have been illegally victimized. Like monthly account holders, they should be able to get a free new number without the loss of any credit they currently hold on their phone.

#### 48. Objectives of Code

- a. Not sure what, exactly, the paragraph on “M-etiquette” is trying to say. On one reading it is being suggested that the MNOs have no interest or concern in how personal communications are conducted, yet obviously they do and say so elsewhere with references, for example, to malicious communications. Also it is possible MNOs could be required to provide information to law enforcement about such communications.
- b. Not sure the references to the status of the code logically follow from the previous paragraph. This is a major policy statement which ought to be given greater prominence. Clearly different MNOs’ performance under the Code will be closely monitored by OFCOM and others, including ourselves, and any significant downward variations from the Code will call into question its usefulness.
- c. See earlier references to the section in the text box.(para 41).

#### 49. Parental controls

- a. See our comments in the Summary and in paragraphs 22-25. Clearly we would hope and expect the protective software to be of the most advanced and robust kinds available and that they can be automatically and remotely updated by the MNOs.
- b. We also believe the cost should be factored in to the overall cost of the service. Child safety should not be an optional extra. Parents or carers should not feel they are unable to make the devices as safe as they would want them to be because they are deterred either by additional costs or by the apparent complexity of implementation.
- c. See earlier comments on access to the different services and in relation to malicious calls (para 46).

#### 50. Combating unwanted bulk, illegal or offensive content

- a. We assume that a comma should have appeared between the words “bulk” and “illegal”.
- b. In relation to the proposal in Annex B, we are unclear as to how this would be implemented. Is it envisaged that the IWF might *not* be asked to undertake the roles set out in the document? That would seem a strange outcome.

#### 51. Implementation and Enforcement of the Code

- a. Clearly we would like to see the code adopted and implemented as soon as possible. A date of July 2004 is referred to but it is not clear whether or not this is a cut off point of any kind. Our expectation would be that on or by July 2004 all MNOs will have signed up to and be observing the code.

- b. We also await clarification of how the MNOs propose to deal with all the legacy issues e.g. persons under the age of 18 may already have bought and be using devices which give access to services, content and experiences which will later be the subject of the code. The longer the MNOs delay implementing the code the larger will be the legacy issue with which they will have to deal. Similar issues arise in relation to parents or adult siblings passing on older handsets, and in relation to purchases in the second-hand market.

52. Anonymity and Traceability

- 53. MNOs appear to have given little detailed consideration to the implications of the existing fixed internet industry's policy on traceability. We believe this is a hugely important oversight which ought to be addressed as a matter of urgency.
- 54. In the fixed internet world, where someone dials in to a server and the system detects that they have disabled or do not have CLI (Caller Line Identification) the functionality they can then access is normally severely restricted by default. This is part of the ISP world's contribution toward reducing the potential for users to abuse the cloak of anonymity. It allows the ISP, and if necessary the police, to pin point a physical location and the time at which certain transactions took place. This can be enormously helpful in an investigation and acts as a significant disincentive to potential criminals. With a pre-paid mobile, whose original owner may never have been authenticated in any way, this possibility simply would not exist. It would be highly regrettable if, through the medium of pre-paid mobiles phones, this important contribution to crime reduction by the fixed Internet world was effectively rendered obsolete.
- 55. In their publication *ChatWise StreetWise* ([www.internetcrimeforum.org.uk](http://www.internetcrimeforum.org.uk)) the Internet Crime Forum said the following:
  - “76. Whilst anonymity can serve a useful purpose in a number of contexts on the Internet, including the protection of children's own privacy and identity, it is important to address the abuse of anonymity for posting illegal content or making inappropriate contact, as well as for other computer misuse offences. A draft Best Current Practice paper by the London Internet Exchange (LINX) highlights the importance of preserving the right to anonymity for vulnerable users such as persecuted minorities and victims of abuse. However, it stresses that "anonymity should be explicitly supported by relevant tools, rather than being present as a blanket status quo, open to use and misuse."<sup>34</sup> It also makes the distinction between ensuring that activity on the Internet can be traced back to the person responsible and the routine monitoring of online activity: "the only purpose of traceability is to allow misuse, once detected, to be rooted out."<sup>35</sup>
- 56. The MNOs should therefore consider restricting the functionality accessible to pre-paid mobile phones where the owner has not been authenticated in a reliable way.

\*\*\*\*\*