

# CODE OF CONDUCT

for operators of social communities in the FSM

As of 11/03/2009

# Contents

<b>A Preamble</b>	<b>3</b>
<b>B Background</b>	<b>4</b>
I. What is Web 2.0	4
II. What are social communities	4
III. Potential risks for minors	4
IV. Responsible parties involved in dealing with social communities	5
<b>C General principles for operation of the services</b>	<b>7</b>
I. Data use, data security, data economy and information rights	7
II. Awareness	8
III. Criminal prosecution and protective measures	9
IV. Information on external complaints offices and information sources	10
<b>D Regulations for designing the services</b>	<b>11</b>
I. Design and integration of rules of behaviour	11
II. Registration process	12
III. Profile	12
IV. Pseudonym/clear names	13
V. Access by search engines	13
VI. Search function	13
VII. Upload of data	13
VIII. Communication	14
IX. System of reporting	14
X. Advertising	15
IX. Blacklists	15
<b>E Final provisions</b>	<b>16</b>
<b>F List of signatories</b>	<b>17</b>

# Sub-code of conduct for operators of social communities of the FSM

## Youth protection and data protection in social communities

As of 11/03/2009

### A Preamble

The goal of this sub-code of conduct of the operators of social communities organised in the Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e. V. (FSM – Voluntary self-control multimedia service providers) is to improve the protection of children and young people, consumer protection and data protection in the use of social communities in Germany.

Studies document that children and young people use the Internet primarily to communicate with each other and to present themselves. Furthermore, they show that communication platforms are very heavily used by minors. The operators of social communities united in the FSM are aware of the resulting social responsibility incumbent on them to protect children and young people. This sub-code of conduct is an expression of this awareness and its corresponding voluntary commitment. The document applies exclusively to the operators of German-language social communities and the German social communities of companies that operate internationally. The sub-code of conduct refers to the WWW-products of the operators.

In part, the various social communities show considerable differences in their design, usability and technology. The measures established in this sub-code of conduct are target values. How they are implemented in detail can differ from product to product. The individual operators are responsible for deciding which route to take.

The operators have set themselves the goal of making allowance for the best possible protection of personal data and the privacy of the user in social communities. In general, the operators base their actions in this respect on the protection of young people and take data protection concerns into account. This basic constellation sometimes results in tensions between youth protection issues and those of data protection. The operators must consequently weigh up the diverging objects for protection. When in doubt, they will decide in favour of youth protection in this context.

This sub-code of conduct is a voluntary independent commitment on the part of the operators, modelled on controlled self-regulation. The sub-code of conduct does not represent any agreement between the operators signing it, but rather provides principles to which the companies within the FSM have committed themselves.

## **B Background**

### **I. What is Web 2.0?**

The further development of the Internet from about 2005 is described as Web 2.0. The term Web 2.0 is characterised by the technical and social change of the Internet, specifically the World Wide Web (WWW). In technical terms Web 2.0 describes the acceleration of the Internet: websites which were previously for the most part static were further developed into dynamic websites on a large scale. This was accompanied by a significantly more frequent change in the contents offered. On the user side, this was associated with a change in the technical situation, in which broadband networks were increasingly expanded (and still are being) and where flat rates could be used, for example.

In a social sense, Web 2.0 is characterised by changes in usage behaviour on the part of users. Users no longer see themselves as purely passive recipients of web content, but rather, thanks to the technical innovations, become “transmitters” themselves by actively designing the Internet in their own terms through producing and processing content. The previously strict separation between content providers and recipients of content is becoming increasingly blurred as a result. There is simultaneously an increased degree of networking between users.

### **II. What are social communities?**

A social community (also called social network) currently represents one of the most prominent examples of Web 2.0 applications. The term ‘social community’ describes an online community in which users meet old and new friends and present themselves in a profile. The social community permits users to upload their own contents, such as a profile of their own and usually photos, music, videos, etc. However, in contrast to purely photo or video communities, pride of place in social communities is taken by mutual contact and interlinking of users. For this purpose the operator provides the users with various communication tools such as pin boards, guest books, personal mailboxes, integrated chats, etc.

### **III. Potential risks for minors**

Web 2.0 brings provides its users with enormous added value in terms of participation and transmission of information as well as with regard to interlinking and mutual communication. The time young people spend on the Internet is of great significance for their further development. The intensive use of this medium can promote learning and the development of important social skills and media competence.

These are for example:

- interpersonal communication on the Internet
- critical handling of media
- critical interaction with information
- dealing with networks and groups of friends
- active design of media (instead of passive consumption)

Social communities (should) reflect reality and represent social networks, which already existed and exist in the same or similar form in the online world up until now and of course in the real world. However, apart from positive learning effects, they also hold risks for children and young people for this reason.

The potential risks include the adoption of impermissible and/or unsuitable content for particular age groups. In addition, it may result in the initiation of unsuitable contacts or so-called cyber-bullying (mobbing and harassment on the Internet). Moreover, open self-presentation on the Internet holds the risk of abuse of personal information.

#### **IV. Responsible parties involved in dealing with social communities**

Among the responsible parties involved in dealing with social communities, apart from the operators and users, are also groups such as parents, teachers, politicians and society at large.

##### **– Operators**

The operators of social communities have entered into dialogue and mutual exchanges concerning ways of combating potential risks for minors in the networks. The sub-code of conduct arising from this is an expression of the observation of their social responsibility.

Apart from the operators, additional actors are responsible for the minimisation of possible risks for minors in social communities.

Consequently, the operators will support parents and teachers in this central role within the boundaries of their possibilities and for example offer information especially for these social groups on safety in dealing with social communities on their portals. Moreover, the operators are working intensively to inform users on how to use social communities safely and, as far as is feasible, to provide technology for extensive protection of the latter's' privacy within the social community.

##### **– Users**

Social communities live through their users. Consequently, they are also of fundamental importance for the safety of underage users in networks. Through acceptance of, and setting an example of the rules of conduct established in the individual products, adult (and underage) users decisively influence (other) underage users positively in appropriate forms of behaviour within the social communities and on the Internet in general.

##### **– Parents and teachers**

As first contacts, and as persons whom children and the young trust, parents and teachers occupy a very special position in terms of conveying and setting an example of media competence. Regular discussions with children and young people on their media use behaviour, lessons on conveying safe and deliberate dealing with media and joint use of media products are important elements in training children and young people to deal with the Internet.

**– Politics and society**

In state facilities such as kindergartens and schools, political institutions have a decisive role in creating conditions that provide children and young people with the relevant knowledge and skills for correct and appropriate usage of the Internet. It is also the task of politics to ensure that prosecutors and courts are appropriately equipped to be able to prosecute and combat criminal online activities appropriately.

The whole of society is charged with the task of conducting a continuing discussion and examination of ethical principles with regard to the requirements for appropriate conduct on the Internet and in social communities in particular.

## **C General principles for operation of the services**

### **I. Data use, data security, data economy and information rights**

#### **1. For all services**

In the data protection declaration (and partly in other suitable places as well), the operators are to inform users as to whether personal data is collected, stored and used and whether temporary or permanent cookies are placed on the computer of the user.

If data protection law consent is required due to the specific design of a service, this is obtained.

Except in the case of contracted data processing, the operators are to inform users in the data protection declaration or at another appropriate point as to what personal data relating to them might be passed on to third parties and for what purpose such transfer occurs. In general, the trust of users is the most valuable asset of a successful social community. For the operators not disappointing this trust of the users goes without saying. Passing on personal data to third parties for commercial or academic purposes without effective data protection law consent being available is ruled out for this reason.

The operators guarantee the technical and organisational measures for data protection, which are required to meet the legal standards for data protection and data security.

Users in a social community can terminate their contractual relationship with the operator at any time. For this purpose they are provided with an easy to find cancel function by the operator (e.g. button, form, e-mail contact, etc) with which the termination can be declared electronically. Furthermore, users can declare the cancellation in written or text form vis-a-vis the operator.

For service reasons the operator may offer reactivation of the cancelled use relationship within a period of four days. This is intended to enable the user to restore his account should he have accidentally terminated his use relationship. There is no obligation to do so.

Photos, videos and other files which were uploaded to the platform by the particular user and are associated with his/her profile are automatically removed together with the profile in the event of the termination of the use relationship. Commentaries previously made by the particular user in a discussion group or in another area of the platform are as far as is possible to be rendered anonymous. If special reasons exist, an operator may also block a profile. The profile can then no longer be viewed in the social community and can no longer be deleted or processed by the profile holder either. This may be necessary, for example, to preserve evidence in ongoing investigation proceedings, to check matters relevant for liability, in the case of violations of the rules of behaviour of the social community, etc. If such proceedings have been terminated or halted, the operator will once again permit access to the profile by the profile holder or delete the profile.

## **2. Additional provisions for services with a primarily underage target group**

The data protection declaration and other information on the use and collection of data must always be framed in a form and language that is appropriate to the age group involved and in addition must be particularly clearly structured. Terms with which children and young people may be unfamiliar must be explained in understandable form.

Users from the age of 12 may in general exercise the right of access to their personal data alone. Otherwise this right of information may be exercised with or through the legal representative.

If particularly sensitive data are entrusted to the operator by minors, it must be borne in mind that, taking all aspects of the individual case into consideration, the child may be entitled to a right to object to the right of the legal representative to be informed. In any event, the minor should be heard beforehand by the operator in the case of a right to information exercised by the legal representative alone.

Asking for the following especially sensitive data of children and young people is waived in profiles: religious affiliation, health data and information on sexual preferences.

## **II. Awareness**

### **1. For all services**

Social communities offer their users diverse means for dynamic and interactive communication within an extensive network. It is therefore essential that operators inform their users about the security measures available in the social community.

The operators are to provide their users with information that is clear and can always be found on the various options for adjusting the settings of the profile (privacy settings). Directly after the registration process – and not just in the terms of use – users are informed on information pages as to how to protect their privacy in the social community, whether the profile can be found via search engines and what default settings can be used on registration in the network.

Moreover, support and recommendations can be found on the information pages on how users can present themselves and move as securely as possible in the network (best practice examples).

The observance of copyright and personality rights is pointed out to users at a suitable point within the particular functionalities.

Children and young people are also in the possession of the fundamental right of self-determination and may consequently communicate freely and independently. Nevertheless, the legal representatives of a child with limited legal competence may demand the deletion of the latter's account if this is legally necessary.

To ensure that the legal representatives of the corresponding user really are involved in the event of a demand for deletion, the former must apply for the deletion to the operator in writing or text form and provide proof if necessary. In this regard, the information required to identify the account involved (e.g. e-mail address of the child, name of the account) must be provided by the legal representatives, although the operators will naturally provide the legal representatives with assistance in identifying the account.

## **2. Additional provisions for services with a primarily underage target group**

Children and young people should understand that they can protect themselves, their online identity and their reputation, why they should do so and how.

For this purpose, the operators will provide parents and teachers among others with specially prepared information on their social community and in this way support the latter in their educational work.

Information measures and legal texts must be framed in a form and language appropriate to the age group and especially clearly structured.

## **III. Criminal prosecution and protective measures**

### **1. For all services**

If access to data and contents of the users of the social community for the purposes of criminal prosecution and as a protective measure by the criminal prosecution and protective authorities is permitted, the operators will support the authorities in their work as far as this is legally possible and permissible.

Information is in general to be provided to the criminal prosecution and protective authorities only in accordance with the legal guidelines and obligations through personnel that have been specially trained and authorised for this purpose.

This provision of information must be documented.

Examination of the legality of the information request is the responsibility of the authority making the inquiry. The operator checks briefly and insofar as this is reasonable whether the conditions for the provision of information exist.

To avert the risk of a current, otherwise not preventable danger to the life, physical safety and freedom of a person, information may exceptionally be provided to the responsible authority after oral instruction and likewise in oral form after a brief check of legality, if there is a risk in delay. This only applies if information on the personal data is an appropriate method of averting the danger (burden of demonstration is with the authorities averting the danger) and if this form of information provision is legally provided for. The operator is not obliged to re-examination. If possible it will record the statements of the authority making the inquiries. In any event, the protective authorities must be identified and must authenticate themselves. The written information instruction must be submitted later by the protective authorities.

## **IV. Information on external complaints offices and information sources**

### **1. For all services**

The operators are to indicate direct means of contact for user care in an appropriate place (e.g. in the masthead of the website). It must be easy for users to tell how they can contact the operator and lodge complaints on the contents in a way which is also independent of the existing, internal platform reporting systems.

In addition, the operators are to provide references to external complaint offices and information sources in an appropriate place. The operators in particular point out the possibility of complaining via [www.fsm.de](http://www.fsm.de).

### **2. Additional provisions for services with a primarily underage target group**

To do justice to the special information needs of those with legal guardianship rights and teachers, the operators are to provide additional information for parents and teachers. At the very least, they are to refer to the website [www.klicksafe.de](http://www.klicksafe.de) where more information and pedagogical notes on media can be found.

## D Regulations for designing the services

### I. Design and integration of rules of behaviour

#### 1. For all services

Responsibility for the contents uploaded by users lies with the users themselves. The operators do not check any contents without a specific cause, but they react immediately after knowledge of a complaint. However, to protect users and especially minors, the operators have undertaken to produce internal community rules which must be observed by all users of the respective social community.

In their internal community rules (for example, terms of use and/or rules of behaviour) the operators are to make clear that users may not upload any absolutely impermissible contents to the website of the community. Such contents are in particular, but not exclusively:

- propaganda material and symbols of anti-constitutional organisations (§§ 86, 86 a StGB [Criminal Code], § 4 (1) No. 1 and 2 JMStV [Interstate Treaty governing the Protection of Minors in the Media]),
- incitements to hatred and the Auschwitz-lie (§ 130 StGB, § 4 (1) No. 3 and 4 JMStV),
- representation of violence (§ 131 StGB, § 4 (1) No. 5 JMStV),
- encouragement to commit or instructions on crimes (§§ 111, 130 a StGB, § 4 (1) No. 6 JMStV),
- contents glorifying war (§ 4 (1) No. 7 JMStV),
- infringements of human dignity (§ 4 (1) No. 8 JMStV),
- erotic pictorial representations of minors (§ 4 (1) No. 9 JMStV),
- pornography featuring children, animals and violence (§ 184 a, 184 b, 184 c StGB, § 4 (1) No. 10 JMStV),
- on account of a violation of the telemedia put on the index by the StGB and telemedia with identical content (§ 4 (1) No. 11 JMStV).

The operators are also to lay down in their internal community rules that the users may not upload contents in accordance with § 4 (2) JMStV and contents deleterious to development according to § 5 JMStV.

The nature of the listing/clarification is at the discretion of the respective operator. An analogous presentation may also occur.

Furthermore, the operators are to regulate in their internal community rules that the users must respect the rights and interests of other users or other third parties, especially their personal rights.

In addition, the internal community rules are to encourage and call for the reporting of behaviour of other users in contravention of the rules and establish the sanctions for infringements of the rules – depending on the severity of the infringement up to deletion of the account of the corresponding user.

The terms of use and – if regulated separately – the internal community codes of conduct behaviour must be easy to find for all users. Every user must agree to the terms of use on registration and – if regulated separately – to the internal codes of conduct behaviour.

## **2. Additional provisions for services with a primarily underage target group**

The internal community codes of behaviour must be framed in a form and language suitable to the age group involved.

### **II. Registration process**

Every user must agree to the terms of use on registration and – if regulated separately – to the internal codes of behaviour.

If this is necessary for the use of the social community, data protection law consent to the storage and processing of personal data by the user must be obtained as part of the registration process.

At the registration of a user, he/she is given an indication of the default settings on the visibility of his profile. In this way the user immediately recognises who can see his/her details.

Observance of any minimum age for users imposed by the operator itself for registration in the social community must be compared during the registration process with the stated age of the user and if applicable the user may not be admitted to the social community if he/she is under the minimum age. The operators are to be aware that such a check function cannot guarantee the validation of the real age of the user.

### **III. Profile**

A profile must always be linked to at least one fixed piece of data, which cannot be changed by the user and permits a clear identification of the corresponding profile (e.g. user ID).

The profile data can be released or blocked by the user for defined groups of people within the social community. These differentiated privacy settings permit free configurability of the profile data, but are not necessarily associated with a freely selectable level of detail in setting options. (For example: not all groups simultaneously visible or invisible, not individually selectable for each group).

At least in the case of all users under 14, stricter privacy settings must be preset as defaults: In general, the profile information here can only be seen by friends. Further release can always only occur by the user himself. However, a general inability to locate minors by contrast calls into question the fundamental right to informational self-determination of minors as well as the creation and existence of interpersonal networking in social communities.

A basic version of the profile, which includes at least the name and profile image of the user, can be viewed by all users of the social community even in the case of the strictest privacy setting.

#### **IV. Pseudonyms/Clear names**

The idea of social communities is to reproduce contacts and groups of friends on a platform and to simplify private communication in this way. Someone who uses a social community wishes to be found within it, but also wants to know with whom they are dealing. The use of real first and second names for identification by contrast with pseudonyms in the user profiles is necessary and desired. However, this produces risks especially regarding personal data. But these are counter-balanced by security aspects, due to the authenticity of the social communities, especially for young users: normally, users of social communities know with whom they are communicating. The authenticity of networks leads to more transparent communication paths between the users, promotes social self-control and as a result can lead to a higher level of protection for young people. For these reasons, the operators are in favour of the use of clear names. Utilisation of the social communities while using real names is the very purpose of the network and the foundation of actual social networking and social control.

#### **V. Access by search engines**

As far as is technically possible, the user can always reject the possibility of his profile data being selected by search engines through an opt-out (i.e. by retrospective alteration of this setting).

At least in the case of all users who declare that they are under 16, a profile cannot be found by external search engines as far as this is technically possible. This setting cannot be changed by opt-in either (i.e. by explicit advance confirmation of this setting).

#### **VI. Search function**

In communities with a primarily underage target group, a search with the following search criteria is to be impossible: street, mobile phone number and telephone number.

A search according to age is in general possible in the case of underage users, since the users in a community have a considerable interest in looking for users of the same age in order to be able to make new contacts. However, in communities with a primarily underage target group users can block their date of birth via differentiated privacy settings and as a result their age as well.

#### **VII. Uploading of data (e.g. pictures, videos, text documents)**

The person marked on a photo or video (i.e. a person is shown in a photo/video, their name is mentioned there and if applicable there is a link from there to their profile in the social community) must be able at any time to delete this link or, if this is technically impossible, to have it deleted by the operator.

At least in the context of the first upload of data by a user, or at another suitable point, it must be indicated to the user in an appropriate and understandable manner that the personal rights of third parties and other rights of third parties (e.g. copyrights) may not be infringed by the pictures themselves, nor by captions, text documents or other data.

Furthermore, there must be an indication in this context that is appropriate and understandable to the user that the terms of use of the operator and/or the internal community code of behaviour must be respected.

## **VIII. Communication**

Users must be able to exclude other users from their internal community communication and to cancel this exclusion again at any time. This includes the transmission of messages, pictures, videos and other data.

Users must be able to allow communication with themselves to only a particular group of people within the social community. For example, this group of people may correspond to the user's list of friends or contacts in the social community or an age group to be determined by the user.

It must be pointed out to the user at least in the internal community rules that both the distribution of illegal contents and the harassment of other users is forbidden. This applies in particular to areas which can be viewed by everyone (e.g. pin board or guest book, group discussion).

The operators in general reject all forms of cyber-bullying on their platforms and severely punish such incidents.

## **IX. System of reporting**

### **1. For all services**

The operators will remove illegal contents or block access to them as soon as they learn of them. This applies in particular to contents that infringe youth media protection law and/or criminal law provisions.

It must be possible for users to report behaviour in violation of the rules and the law at any time. The operator encourages users to report behaviour in violation of the rules.

The reporting function can be reached quickly at a prominent place within the platform.

The operator will punish users who violate the rules – up to deletion of the account. The operator informs users of the possibility of sanctions in the event of behaviour in violation of the rules.

### **2. Additional provisions for services with a primarily underage target group**

The operator informs users in a form and language appropriate to the age group involved of the characteristics of behaviour in violation of the rules, the reporting function and possible sanctions.

## **X. Advertising**

### **1. For all services**

Operation of the social communities is cost-intensive, due to the high technological effort required. The placement of advertising is an important pillar for financing the communities, which are essentially free of charge for the users. At the same time, the operators have an interest in offering the users added value with suitable advertising and not disturbing the latter's feeling of well-being. The operators are simultaneously responsible for selecting advertising customers and advertising forms independently insofar as the legal guidelines and the guidelines of this sub-code are complied with.

Target-group specific advertising (targeting) making use of personal data is only possible if data protection law consent of the users is available and the users are informed correspondingly of the use of their data.

In accordance with the requirement to separate advertising and contents, advertising must be identified in a clearly understandable and plain manner (e.g. with the words "Advertising" or "Advert") unless it emerges unmistakably from the design of the advertising format itself that what is involved is advertising (e.g. advertising banner).

### **2. Additional provisions for services with a primarily underage target group**

The design of advertising directed in particular to children and young people must be oriented to the standards of § 6 JMStV. This means in particular, but not exclusively:

- advertising may not exploit the inexperience of children and young people or harm the interests of children and young people
- advertising may not impair the development of children and young people.
- advertising may not include any direct appeal to buy
- advertising may not call on children and young people to urge their parents or third parties to buy the goods or services advertised
- advertising may not exploit the special trust which children or the young have in parents, teachers or other trusted people
- advertising may not show children or young people without a good reason in dangerous situations.

Pop-ups and animated banners which cover the contents of the website and are difficult to close are particularly unsuitable for communities with a young target group, since young users often lack experience in dealing with such forms of advertising.

## **IX. Blacklists**

The operators will collect forbidden profile names, group names and words and produce corresponding blacklists. These blacklists are intended to assist the operators in their daily work, whether it is in support, programming or the further development of functionalities.

## E Final provisions

Online products of greater scope are subject to dynamic changes in modern business transactions, which partially occur automatically. For this reason, the operators cannot completely guarantee that offences against the above obligations will always be ruled out. Consequently, the obligations refer to the operators doing all they can to try to prevent violations of the agreements laid down in this sub-code and in the case of existing violations of which operators become aware, immediately creating remedies after they learn of them.

The members of the FSM signatory to this document agree that in view of the practical work of the FSM, updating of this document must be checked every 12 months. Amendments to the sub-code are possible by consensus with all signatories.

If parts of this self-obligation declaration have not yet been implemented by individual operators, these will be implemented by 31 July 2009 at the latest.

Twelve months after signing the code of conduct, the signatory operators will have the success of the self-commitment and its implementation in their corresponding social communities evaluated by an independent research institution, with practical application tests from a user point of view. The choice of the research institution will be made by consensus of the signatory operators. The evaluation process will be financed by the signatory operators by an assessment system.

If an offence against this sub-code of conduct is determined by the responsible committees of the FSM applying the complaint ordinance of the Freiwillige Selbstkontrolle Multimedia Dienstleister e.V., sanctions can be imposed according to § 11 of the FSM complaint ordinance. The operators undertake for the purpose of clearing up complaints to hand over the data available to them regarding the incident to which objection has been made at the first request to the FSM complaint office.

Operators of social communities which have not yet signed the sub-code, but wish to observe it in future, can likewise sign it. In future they will likewise be able to participate in the development of the code. A condition for the signature is the existence of proper membership of the FSM and that the product complies with this code of conduct.

## **F List of signatories**

The founding signatories of this agreement are the following companies:

- studiVZ Limited for their social communities schuelerVZ.de, studiVZ.de and meinVZ.de,
- Lemonline Media Ltd. for its social community wer-kennt-wen.de,
- lokalisten media GmbH for its social community lokalisten.de.