



DATEN SCHUTZ

im Kinderdorf

Quelle/Zeichnungen: Datenschutzbeauftragter Kt. Zürich (<http://www.datenschutz.ch>)
Schweizerischer Datenschutzbeauftragten; (www.dsb-cpd.ch)

Zur besseren Lesbarkeit wird nur die männliche Schreibweise gewählt, selbstverständlich sind auch die weiblichen Mitarbeitenden gemeint.

Teil 1: Allgemeine Bestimmungen

Teil 2: Sicherer Umgang mit ICT

„Datenschutz, der Schutz der Privatsphäre, ist ein Grundrecht unserer Rechts- und Gesellschaftsordnung. Mit Daten über unsere Schülerinnen und Schüler gehen wir äusserst sorgsam um. Akten dürfen das Kinderdorfareal nicht verlassen. Beim Datenversand über das Internet ist darauf zu achten, dass Personalien der Schülerinnen und Schüler nicht erkenntlich sind.“
(Auszug aus den Kinderdorfregeln)

Datenschutzkonzept – Teil 1: Allgemeine Bestimmungen

► Grundlagen

• Rechtsgrundlagen

Für den Datenschutz im Kinderdorf kommen das eidgenössische Datenschutzgesetz und/oder das kantonale Datenschutzgesetz zur Anwendung.

Zusätzlich sind die Artikel 53, 54 und 55 des Kantonalen Jugendgesetzes zu beachten.

• Grundbegriffe

→ *Personendaten* (Daten) sind alle Angaben (Informationen), die sich auf eine Person beziehen.

→ *Bearbeiten* beinhaltet jeden Umgang mit Personendaten, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten.

► Geltungsbereich, Verantwortung und Meldepflicht

Die vorliegenden Bestimmungen gelten grundsätzlich für alle Mitarbeitende des Kinderdorfes.

Alle Mitarbeitende müssen und können ihren Teil an der Verantwortung für Datenschutz und Datensicherheit tragen. In bestimmten Bereichen kann jeder verhindern, dass Schäden entstehen oder Persönlichkeitsrechte verletzt werden.

Jeder Mitarbeitende ist verantwortlich, dass keine Daten in die Hände Unbefugter gelangen oder missbraucht werden.

Bei möglichem Datenmissbrauch oder beim Erkennen von Sicherheitslücken und Mängeln ist jeder Mitarbeitende verpflichtet, die Direktion zu unterrichten!



► Datenschutz - ein Grundrecht

• Datenschutz, der Schutz der Privatsphäre, gibt das Recht ...

... *auf ungestörte Privatsphäre.*

Ziel des Datenschutzes ist, die Privatsphäre jedes Menschen umfassend zu schützen. Dieses Grundrecht auf Privatsphäre ist durch die Bundesverfassung sowie die Europäische Menschenrechtskonvention garantiert.

... *auf Verschwiegenheit der Institution.*

Die Privatsphäre ist geschützt, wenn die Daten im Kinderdorf verbleiben und nicht unberechtigterweise weitergegeben werden. Hierfür sorgt neben dem Datenschutzgesetz auch die Schweigepflicht jedes Mitarbeitenden des Kinderdorfes.

... *auf Transparenz im Umgang mit Personendaten.*

Personen resp. deren gesetzliche Vertretung, von welchen Daten angelegt werden haben das Recht, Auskunft über die eigenen Daten zu erhalten, wozu sie dienen, wer sie bearbeitet und an wen sie allenfalls übermittelt werden. Dieses Recht kann nur in Ausnahmefällen eingeschränkt werden.

... *dass Daten im vorbestimmten Bereich verbleiben.*

Daten dürfen nur zum vorgesehenen Zweck bearbeitet werden, weshalb der Anspruch besteht, dass sensible Personaldaten nicht für andere Zwecke verwendet werden.

... *dass Daten gegen unbefugtes Bearbeiten gesichert werden.*

Wenn Personendaten durch Mitarbeitende des Kinderdorfes bearbeitet werden, muss die Vertraulichkeit der Daten gewährleistet sein. Alle Personen haben deshalb einen Anspruch, dass angemessene Sicherheitsmassnahmen gegen das unbefugte Bearbeiten getroffen werden.

... *auf Berichtigung unzutreffender Daten.*

Erweisen sich bearbeitete Daten als unzutreffend, kann die betroffene Person resp. deren gesetzliche Vertretung verlangen, dass diese entweder berichtigt oder vernichtet werden.

... *die Weitergabe der Daten zu untersagen.*

Jede Person resp. deren gesetzliche Vertretung kann die Weitergabe der Daten untersagen.

▸ Grundsätze



• Datenerhebung

- *Daten dürfen nur rechtmässig beschafft werden.*
Daten dürfen nur bei der betroffenen Person oder ihrer gesetzlichen Vertretung beschafft oder von jemandem übernommen werden, der von der berechtigten Person zur Weitergabe berechtigt wird.

• Dateninhalt

- *Daten müssen richtig sein.*
Der betroffenen Person oder deren gesetzlichen Vertreter sind die gesammelten Daten bekannt zu geben, damit sie diese wenn nötig berichtigen oder zum Inhalt Stellung nehmen kann.
- *Die Datensammlung muss dem bei der Beschaffung der Daten angegebenen Zweck entsprechen.*
Datensammlungen dürfen nicht unterschiedlichen Benützenden (z. B. Kinderdorf und zugleich Behörden) dienen. Es dürfen keine Daten auf Vorrat gesammelt werden, für welche vorerst gar keine Verwendung besteht.

• Datenweitergabe

- Vor allem die von den Pädagogen, Therapeuten und der Administration des Kinderdorfes gesammelten Daten beziehen sich auf den intimsten Bereich der Persönlichkeit. Deshalb gehören sie zu den ‚besonders schützenswerten Daten‘, d.h. sie gehören zu den durch das Gesetz am strengsten geschützten Daten.
- Daten dürfen nur unter einer der folgenden Voraussetzungen (mündlich oder schriftlich) weitergegeben werden:
 - wenn dies in einem Gesetz ausdrücklich vorgeschrieben ist.
 - wenn die betroffene Person oder deren gesetzlicher Vertreter ausdrücklich eingewilligt hat.
Die Zustimmung
 - ... muss vor der Datenweitergabe eingeholt werden.
 - ... ist mündlich oder schriftlich gültig (bei mündlicher Zustimmung Vermerk in den Akten).
 - ... welche auf einem Formular blanko oder allgemein für sämtliche künftigen Auskünfte erteilt wird, ist unwirksam.
 - ... kann widerrufen werden.
- Bei der Weitergabe darf nur der Adressat Zugriff erhalten.
Achtung bei Telefonaten und Telefax: nicht berechtigte Dritte sollen nicht mithören bzw. mitlesen können; beim Gebrauch von E-Mail müssen die Daten verschlüsselt werden.
- Auskünfte an ...
 - ... *Kinder und Jugendliche und/oder deren Eltern oder die gesetzliche Vertretung*
Die Kinder und Jugendlichen, bzw. die gesetzliche Vertretung, sind über die gesammelten Daten auf Verlangen vollständig zu orientieren.
 - ... *einen geschiedenen oder getrennt lebenden Elternteil*
Eltern ohne Sorgerecht haben in gleicher Weise wie der Inhaber der elterlichen Sorge das Recht, Auskünfte über den Zustand und die Entwicklung des Kindes zu erhalten.
 - ... *an andere Pädagogen und Therapeuten innerhalb des Kinderdorfes*
Es dürfen nur die für die Zusammenarbeit und die Arbeit der Pädagogen und Therapeuten notwendigen Informationen weitergegeben werden.
 - ... *Fachpersonen und Fachstellen*
Die Zusammenarbeit mit Fachpersonen (inkl. Ärzte) und Fachstellen ist wichtig. Die Datenweitergabe darf aber nie ohne Einverständnis und Orientierung der betroffenen Person bzw. ihrer gesetzlichen Vertretung erfolgen. Dass Fachpersonen an ein Berufsgeheimnis gebunden sind, ändert daran nichts.
 - ... *an Versicherungen*
Versicherungen (Krankenkassen, Invaliden-, Unfall-, Militärversicherung etc.) brauchen gewisse Daten, damit sie die Leistungsvoraussetzungen beurteilen und die Vergütung ausrichten können. Obligatorische Versicherungen (Unfall-, Militärversicherung, Krankenkasse) verlangen Auskünfte gestützt auf einer gesetzlichen Grundlage; es ist also keine ausdrückliche Einwilligung des Betroffenen nötig.
Private Versicherungen (private Kranken-, Unfall-, Haftpflicht-, Lebens-, Taggeldversicherungen, etc.) hingegen haben die Einwilligung des Betroffenen resp. dessen gesetzliche Vertretung nachzuweisen.

... *an sonstige Dritte*

An andere aussenstehende Personen darf grundsätzlich keine Auskunft erteilt werden, auch nicht nach Abschluss der Schulzeit oder des Arbeitsverhältnisses im Kinderdorf. Die Auskunft ist nur zu erteilen, wenn der urteilsfähige Jugendliche bzw. seine gesetzliche Vertretung oder die Person eine schriftliche Vollmacht erteilt hat oder persönlich beim Gespräch anwesend ist.

- **Besucher**

Praktikanten, Mitglieder von Behörden, Aufsichtsinstanzen oder andere Personen dürfen die Klassen, Gruppen und/oder Therapien besuchen, wenn zuvor eine Zustimmung durch die Direktion erteilt worden ist.

- **Fachberatung, Falldarstellungen, Statistik, Verwendung von Bildmaterial, usw.**

Die Bearbeitung von Daten für Ausbildung/Fort- und Weiterbildung, wissenschaftliche Zwecke oder für die Statistik ist zulässig, wenn die Daten anonymisiert (keine Rückschlüsse mehr auf eine individuelle Person möglich) sind und die Verwendung nicht auf eine einzige oder eine Gruppe erkennbarer Personen bezogen ist. Einem Dritten dürfen die Daten nicht zur Bearbeitung - dazu gehört auch die Anonymisierung - überlassen werden, sondern nur die anonymisierten Ergebnisse.

Illustrationen mit Bildmaterial wie Fotos und Videoaufnahmen dürfen nur verwendet werden, wenn vor der Aufnahme über die Verwendung aufgeklärt und eine Zustimmung durch das Kind/Jugendlichen resp. dessen gesetzliche Vertretung dazu erteilt worden ist.

- **Aufbewahrung von Daten**

Personendaten dürfen nur solange aufbewahrt werden, wie es für die Erreichung der Ziele, für die sie angelegt worden sind, notwendig ist. Nicht mehr benötigte Personendaten sind zu vernichten.

Die Akten oder Speichermedien sind an einem Ort aufzubewahren, wo sie ausreichend sicher sind vor Zerstörung und vor dem Zugriff durch nicht bevollmächtigte Dritte (passwortgeschützt). Schränke dürfen nicht einer unbestimmten Anzahl Personen oder durch Passepartout zugänglich sein.

Die ehemaligem Schüler resp. deren gesetzliche Vertretung haben das Recht, jederzeit die Herausgabe der Originale oder von Kopien zu verlangen (Ausnahme: Persönliche Arbeitsmittel der Pädagogen und Therapeuten). Die Herausgabe der Akten oder Kopien ist unentgeltlich.

► **Weitere Informationen im Netz**

- [Bundesgesetz über den Datenschutz](http://www.admin.ch/ch/d/sr/23.html#235) (<http://www.admin.ch/ch/d/sr/23.html#235>)
- [Eidgenössischer Datenschutzbeauftragter](http://www.edsb.ch/) (<http://www.edsb.ch/>)
- [Walliser Datenschutzkommission](http://www.vs.ch/navig/navig.asp?Language=de) (<http://www.vs.ch/navig/navig.asp?Language=de>)
- [Datenschutzbeauftragter Kt. Zürich](http://www.datenschutz.ch) (<http://www.datenschutz.ch>)
- [Virtuelles Datenschutzbüro](http://www.privacyservice.org/) (<http://www.privacyservice.org/>)



Datenschutzkonzept – Teil 2: Der sichere Umgang mit ICT

Schweizerischen Datenschutzbeauftragten; www.dsb-cpd.ch; Juni 2002

► Vorbemerkungen

- Nachfolgende Bestimmungen gelten vor allem für den Umgang mit dem Kinderdorfnetzwerk mit Firewall und Proxy-Server.
- Die Arbeitsstationen sind Eigentum des Kinderdorfes und bleiben auch bei einem allfälligen Zimmerwechsel im angestammten Raum. Bei einem Zimmerwechsel sind alle Daten auf dem Laufwerk C: zu löschen (siehe unten).
- Das Netzwerk und die Arbeitsstationen sind so installiert, dass die nötigen Sicherheitsfunktionen (mit Firewall, Proxy-Server, Optionen des Browsers) bereits voreingestellt sind. Änderungen an der Browsereinstellung sind zuerst mit dem ICT-Systembetreuer abzusprechen.
- Das Kinderdorfnetzwerkssystem (Back up) ist so angelegt, dass auf dem Server abgelegte Daten automatisch und regelmässig gesichert werden. Daher sind arbeitsrelevante Daten auf dem Server abzulegen.
- Es sollen keine vertraulichen und/oder arbeitsrelevanten Daten auf lokalen Arbeitsplätzen (Laufwerk C:) gespeichert werden. Diese werden nicht automatisch gesichert und der Schutz ist nicht gewährleistet. Für Daten, welche nicht auf dem Server abgelegt sind (z. B. Laufwerk C:, Disketten, USB-Stick, usw.), trägt für die Datensicherung jeder einzelne selber die Verantwortung.
- Es dürfen ausschliesslich nur die zur Verfügung gestellte und/oder rechtmässig lizenzierte Software installiert werden! Die Verwendung anderer Software kann rechtliche Folgen nach sich ziehen (z. B. wegen der Verletzung von Lizenzbestimmungen).

► Schutz gegen Zugriff unberechtigter

• Passwort

- Zweck eines Passwortes

Passwörter sollen sicherstellen, dass nur Berechtigte Zugriff auf ein System oder bestimmte Anwendungen und deren Daten haben. Geschützt werden kann namentlich: jede einzelne Datei, Laufwerke, und Datenträger, Bios, Betriebssystem. Ansonsten besteht die Gefahr, dass Daten von Unberechtigten eingesehen, manipuliert oder gelöscht werden.

- Ein gutes oder starkes Passwort (siehe auch Passwort-Check auf <http://www.datenschutz.ch>)

- besteht aus mindestens 8 oder mehr Zeichen.
- ist aus Zahlen, Buchstaben und Sonderzeichen kombiniert.
- schreibt sich aus Gross- und Kleinbuchstaben.
- Kann man sich gut merken, aber nur schwer zu erraten, z. B. Sonn**EN00schein, fRan?ziska57.
- besteht nicht aus zwei gleichen aufeinander folgenden Zeichen, aus Wörtern und Namen, wie sie in einem Wörterbuch oder Lexikon zu finden sind und nicht nur aus Zahlen wie z. B. Telefonnummern, Geburtsdaten oder Auto-Kennzeichen.

- Handhabung des Passwortes

- Passwort auf alle Fälle geheim halten!
- Passwort alle 2 Monate ändern, bei Verdacht auf Missbrauch sofortige und Meldung an den ICT-Systembetreuer und an die Direktion!
- Nie exakt dasselbe Passwort für verschiedene Anwendungen verwenden!

• Verlassen des Arbeitsplatzes

- Bei kurzer Abwesenheit

- sollte stets ein Bildschirmschoner mit Passwortschutz aktiviert sein.
- dürfen vertrauliche Daten (Papiere, Dossiers, Datenträger) für andere nicht zugänglich sein.

- Nach Feierabend

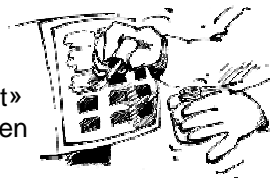
- ist der Computer vom Netzwerk abzumelden und auszuschalten.
- sind alle vertraulichen Daten wegzuschliessen.



- **Löschen, Weitergeben und Speichern von Daten**

- *Löschen von Daten*

- Mit Befehlen wie «delete», «erase», «löschen» oder «(Quick)Format» (=Schnellformatierung) werden Daten nicht definitiv vernichtet, diese bleiben rekonstruierbar.
- Immer zusätzlich auch den ‚Papierkorb‘ auf dem Desktop leeren.
- Daten sind oft an unterschiedlichen Orten vorhanden. Nicht nur die elektronisch gespeicherten, sondern auch die Daten in Papierform sind zu löschen bzw. zu vernichten.



- *Weitergeben von Daten*

- Zur Weitergabe von Daten sind wenn immer möglich, neue Datenträger (z. B. Disketten) oder tragbare Massenspeichermedien (z. B. USB-Stick) zu verwenden.
- Falls gebrauchte Disketten verwendet werden, müssen diese zuvor vollständig formatiert werden (nicht Quickformat, sondern Tiefformatierung: Arbeitsplatz → Datenträger → Datei → Formatieren... → Starten).
- Achtung vor Datenträgerverlust! Passwortschutz verwenden.

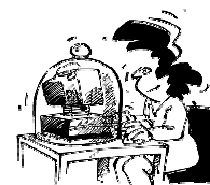
- *Speichern von Daten*

- Vertrauliche Daten sind stets am richtigen Ort abzuspeichern (auf dem Server nicht auf Laufwerk C:), so dass nur Berechtigte Zugriff darauf haben.
- Keine vertraulichen und/oder arbeitsrelevanten Daten auf lokalen Arbeitsplätzen (Laufwerk C:) speichern. Sie werden nicht automatisch gesichert und der Schutz ist nicht gewährleistet.

- **Schutz vor Zerstörung: Viren**

- **Was sind Viren?**

Viren, Würmer, trojanische Pferde oder dergleichen sind kleine Programme, die Computersysteme befallen und Daten und Programme zerstören oder verändern oder andere gravierende Schäden anrichten können.



- **Wie können Viren eingeschleppt werden?**

Über E-Mails und Anhänge (Attachments, Dokumente), über Dateien (z. B. Spiele, Freeware), die beim Surfen im Internet oder beim Herunterladen, aber auch über Disketten, CDs, usw.. Siehe auch die Tipps für einen richtigen Umgang mit E-Mails.

- **Schutz vor Viren**

- Das Virenschutzprogramm automatisch ‚updaten‘.
- Virenschutzprogramme nie deaktivieren.
- Disketten und CDs vor dem Gebrauch immer mit dem Virenschutzprogramm prüfen (meist automatisch durch installiertes Virenschutzprogramm).
- Nur vom Systembetreuer zur Verfügung gestellte und/oder rechtmässig lizenzierte Software verwenden.

- **Vorgehen bei Auftreten von Viren**

- Computer ausschalten.
- Informatik- oder Systemverantwortlicher informieren.
- Systembetreuer oder Direktor informieren.

- **Vorsicht bei so genannten «aktiven Inhalten»!**

Noch gefährlicher als die Viren sind die so genannten "aktiven Inhalte", in der Fachsprache oft auch ActiveX-Controls, Java-Applets oder Scripting-Programme genannt, die beim Surfen auf Ihren PC gelangen können sowie Makro-Viren in Office-Dokumenten. Diese interaktiven Elemente können an Software und Daten grossen Schaden anrichten. Das Sicherheitsrisiko kann mit der richtigen Einstellung des Internetprogramms (Browsers) verhindert werden. Daher sollen diese Sicherheitseinstellung des Browsers nicht verändert werden.

