BEE SECURE

INTERNET IN DER MAISON RELAIS?

ABER SICHER(ER)!

RATGEBER

ÜBERBLICK

✖ Dieser Ratgeber richtet sich an Verantwortliche und Mitarbeiter (ErzieherInnen) in den Maison Relais und widmet sich folgender Frage:

„Wie kann eine sichere Internetnutzung in der Maison Relais ermöglicht werden – sowohl für Mitarbeiter, als auch für Kinder?“

Der Ratgeber ist als Wegweiser für die Erstellung eines bedarfsgerechten Sicherheitskonzeptes für das Internet in der Maison Relais gedacht. Er gibt einen praxisorientierten Überblick über die wichtigsten Überlegungen zu dieser Thematik und leitet daraus Prinzipien zur Erstellung des eigenen Konzeptes ab. Dabei werden sowohl technische, rechtliche als auch pädagogische Aspekte berücksichtigt.

In enger Zusammenarbeit zwischen der Croix Rouge und BEE SECURE wurde 2017 ein Pilotprojekt in der Maison Relais Dippach durchgeführt. In diesem Pilotprojekt wurde die Nutzung eines Tablets als pädagogisches Angebot getestet. Erkenntnisse und Erfahrungen daraus flossen in diesen Ratgeber mit ein. Des Weiteren wurden Empfehlungen aus dem 2013 entwickelten Aktionsplan für Jugendhäuser „Secure MJ“ für die Gegebenheiten in der Maison Relais angepasst.

SICHERHEIT IST RELATIV.
SICHERHEIT IST KEIN ZUSTAND, SONDERN EIN PROZESS.

BEE SECURE

Herausgeber : SNJ
Annexe Forum Geesseknäppchen
40, bld. Pierre Dupong
L-1430 Luxembourg
B.P. 707 · L-2017 Luxembourg

snj@bee-secure.lu
www.snj.lu

ISBN: 978-2-9199499-3-9

Service National de la Jeunesse · kanner jugend telefon · SECURITY MADE IN.LU
LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG · Co-financed by the European Union Connecting Europe Facility

Impressum

Diese Publikation wurde vom SNJ (Service National de la Jeunesse) im Rahmen des Projekts BEE SECURE produziert.
Das Projekt wird gemeinsam vom Service National de la Jeunesse (SNJ), dem KannerJugendTelefon (KJT) und securitymadein.lu umgesetzt.

Grafikdesign von: Takaneo

Auflage 500 Exemplare
Internet in der Maison Relais - 12.2018

INHALTSVERZEICHNIS

EINLEITUNG

Jede Maison Relais braucht Sicherheitsvorkehrungen für das Internet.

Digitale Gesellschaft, vernetztes „Smart Home“ und in nicht allzu ferner Zukunft selbstfahrende Autos - die Liste der Schlagworte und Themen, die mit der sogenannten „Digitalisierung“ unseres Lebens in immer mehr Bereichen einhergeht, ist in den letzten Jahren rasant gewachsen. Computer und Internet sind auch aus der Verwaltung und Organisation der Maison Relais als Einrichtung nicht mehr wegzudenken.

Das Personal, Eltern und weitere Personen (Praktikanten, Besucher, etc.) tragen meist (private) Smartphones während des Aufenthaltes in der Einrichtung bei sich und sind mobil oder durch hauseigenes Wi-Fi vernetzt. Die Einrichtung selber hat eine eigene Online-Präsenz (Webseite), E-Mails gehören ganz selbstverständlich zur professionellen Kommunikation dazu und Daten von Personal sowie Kindern werden oftmals auf digitalen Speichermedien (bspw. Festplatten, USB-Stick, Cloud) gespeichert.

Kinder und das Internet: Lebenswelt und Bildungsauftrag.

Kinder wachsen also mittlerweile ganz selbstverständlich in einer vernetzten Welt auf, in der sie die Möglichkeiten des Internets immer früher entdecken und auch selber ausprobieren. Umso wichtiger ist es, Kinder beim Erwerb wichtiger (Medien-) Kompetenzen mit Hinblick auf die Möglichkeiten und Herausforderungen der (digitalen) Welt von heute und morgen zu fördern.

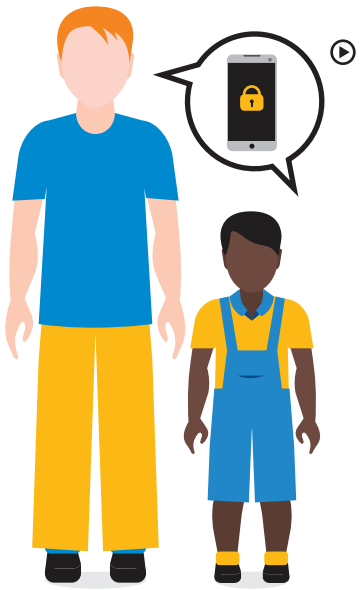
Ein wichtiges Ziel dieser Förderung sollte dabei stets sein, die Kinder für einen positiven, verantwortungsvollen und kritischen Umgang mit neuen Medien und Technologien zu sensibilisieren. So ist die Förderung von Medienkompetenzen und der Einsatz digitaler Medien in der Maison Relais auch fester Bestandteil des Bildungsauftrages, der im Rahmenplan zur non-formalen Bildung im Kindes- und Jugendalter näher beschrieben ist.

Der Nationale Rahmenplan (2018) sieht in der Rubrik „Kommunikation, Sprache, Medien“ für die Maisons Relais vor, dass digitale Medien als fester Bestandteil der alltäglichen Lebenswelt von Kindern in Form von individuell passenden Medienangeboten pädagogisch behandelt werden sollen:

„Digitale Medien sind in einer technisierten Wissensgesellschaft fester Bestandteil der alltäglichen Lebenswelt von Kindern. Der Bildungsauftrag non-formaler Einrichtungen bezieht sich daher auch auf die Förderung kindlicher Medienkompetenz. Diese befähigt die einzelnen Mädchen und Jungen, unterschiedliche Medien zunehmend selbstgesteuert und reflektiert einzusetzen sowie für eigene Anliegen, zum sozialen Austausch und zur gesellschaftlichen Partizipation zu nutzen. Der lustvolle, kreative und praxisorientierte Umgang älterer Grundschulkinder mit Kommunikations- und Informationsmedien wird unter anderem in der Entwicklung und Anwendung einer eigenen Jugendsprache sichtbar, die durch die jeweilige Peergruppe geprägt ist und vorwiegend in der digitalen Kommunikation mittels SMS oder Internet Verwendung findet.

Die kreativ-spielerische Auseinandersetzung mit digitalen Medien wird mit zunehmendem Alter durch den gezielten Einsatz von Medien als Arbeits- und Informationsmittel erweitert. Die Kooperation mit den Eltern erlaubt es Pädagoginnen und Pädagogen, auf den Vorerfahrungen der Kinder aufzubauen, individuell passende ergänzende Medienangebote zu planen und damit zum Chancenausgleich beizutragen.“ [1]

[1] Zitat aus: Nationaler Rahmenplan zur non-formalen Bildung im Kindes- und Jugendalter, S.64 Edition 2018



Medienkompetenzen fördern – mit und ohne Internet

Förderung von Medienkompetenzen kann auf vielfältige Weise geschehen. Es gibt viele tolle Möglichkeiten, die auch für ErzieherInnen spannend zu entdecken sein können – denn mittlerweile ist es normal, dass man als Erwachsener schnell einmal das Gefühl bekommen kann, so gar keine Ahnung mehr von dem zu haben, womit Kinder und Jugendliche scheinbar mit Leichtigkeit und ganz selbstverständlich umgehen.

Hier lohnt es sich, am besten in praktischen Fortbildungen und Workshops zu erfahren, wie vielseitig Medienpädagogik gestaltet werden kann und sich mit Fachkollegen über Erfahrungen auszutauschen (siehe Ansprechpartner und Links im Anhang). Mittlerweile haben sich im Internet zudem viele Foren zum Wissens- und Erfahrungsaustausch herausgebildet, in denen es sich zu stöbern lohnt. Hier findet man auch Ideen wie man die Medienkompetenzen der Kinder fördern kann.

Des Weiteren ist es wissenswert, dass Aktivitäten, die die Förderung von Medienkompetenzen zum Ziel haben, nicht unbedingt immer einen Internetanschluss voraussetzen, wie zum Beispiel:

- Das gemeinsame Aufstellen von Regeln für die Nutzung des Internets in der Maison Relais

- Pädagogische Brettspiele wie „Tubes“ von BEE SECURE

- Weitere Aktivitäten und Arbeitsblätter (siehe „Pädagogischer Leitfaden“ von BEE SECURE[2])

- Aktivitäten mit Tablets, wie zum Beispiel Computerspiele selber zu programmieren mit der kindgerechten, einsteigerfreundlichen Programmiersprache „Scratch“[3] (auch ohne Internetverbindung nutzbar)

Selbstverständlich gibt es aber auch viele Aktivitäten, die am besten mit Internetzugang stattfinden sollten:

- Angebote wie „Computerecken“

- Medienwerkstätten bzw. -projekte (Comics/Poster erstellen, eigene Zeitung)

- Aktivitäten mit Tablets (Lernspiele, kreatives Gestalten von Audio-, Bild-, Videomaterial, bspw. Hörspiel selber aufnehmen, Informationssuche, Recherchen für Hausaufgaben,...)

[2] www.bee-secure.lu/leitfaden
[3] https://scratch.mit.edu/

I. SICHERHEIT HEIßT RISIKOMINIMIERUNG

Die Nutzung von IT (Informations-Technologien) geht immer mit Sicherheitsrisiken einher. Das liegt sozusagen „in der Natur der Technik". Welche Risiken das sind und wie hoch überhaupt die Wahrscheinlichkeit ist, dass „etwas Schlimmes passiert", hängt dabei von verschiedenen Dingen ab.

ZIEL SOLLTE ES GRUNDSÄTZLICH SEIN, DIE GRÖßTMÖGLICHE SICHERHEIT FÜR DEN SPEZIFISCHEN ANWENDUNGSBEREICH VON IT ZU ERREICHEN[4].

Man spricht gerne davon, dass jeder konkrete Anwendungsbereich mit einer Vielzahl von „Bedrohungsszenarien" einhergeht, von denen manche mehr oder weniger wahrscheinlich bzw. realistisch sind.

Ein Beispiel

Die Server (=Rechner zum Speichern von Daten) einer großen, weltweit agierenden Bank sind durch das massenhafte Speichern sensibler Daten einem größeren Risiko ausgesetzt, von Wirtschaftskriminellen attackiert bzw. „gehackt" zu werden, als der kleine Computer zur Hausaufgabenrecherche im Medienraum einer Maison Relais.

Doch würden Sie dort trotzem ihre Finanzdaten speichern wollen? Und was ist mit den Verwaltungsrechnern in der Maison Relais - welche (vertraulichen) Daten sind dort gespeichert? Wer hat dort Zugriff auf vertrauliche Informationen, wie beispielsweise Name, Adresse und gesundheitliche Informationen eines Kindes? Nur der/die Verantwortliche des Hauses, oder auch MitarbeiterInnen - vielleicht sogar auch Praktikanten oder vielleicht sogar jede/r, der den Raum betritt?

[4] Für weitere interessante Überlegungen zum Thema „Risikomanagement in der Informationssicherheit" siehe: https://www.cases.lu/risikomanagement.html

Abgesehen vom plakativen Beispiel des „klassischen Daten-Hacks" - welche Bedrohungen sind bei der Nutzung des Internets durch die Personen im Hause (Verwaltung, Betreuungspersonal, Kinder, Eltern, Besucher, ...) und außerhalb des Hauses (bspw. externer Zugriff auf Geräte/Daten in der Maison Relais per Internetverbindung) eigentlich zu beachten?

Sicherheit zu schaffen ist also ein Prozess des Abwägens zwischen dem (gewünschten) Nutzen und den (möglichen) Risiken. Was heißt das nun konkret für das Ziel, Internetsicherheit in der Maison Relais zu schaffen?

Es bedeutet, dass zur Sicherheit zwei Ebenen gehören, die im Zusammenspiel die bestmögliche Risikominimierung bzw. das bestmögliche Sicherheitslevel gewährleisten:

1. Das Verhalten der Erzieher/Nutzer

2. Die technische Ebene
Einrichtung getrennter Netzwerkzonen, Internetfilter, Sicherheit der Geräte, Wartungen

Warum es nicht einfach ausreicht, ein Antivirusprogramm zu installieren, damit die Kinder im Internet „geschützt" sind und um zu verstehen, warum ein kritisches Verhalten des Nutzers (hier: das Kind) im Internet so wichtig ist, wird im folgenden Kapitel ein kurzer Überblick über die Risiken, denen Kinder grundsätzlich im Internet gegenüberstehen, gegeben.

INTERNETRISIKEN FÜR KINDER: EIN ÜBERBLICK

Die Risiken im Wandel der Zeit

Kinder sind gewissen Risiken ausgesetzt, vor allem, wenn sie alleine (ohne erwachsene Begleitung) im Internet unterwegs sind.

Aus diesem Grund bietet BEE SECURE seit Jahren Schulungen zur Grundsensibilisierung für einen sicheren und verantwortungsvollen Umgang mit dem Internet an. Aus dem daraus resultierendem Erfahrungsschatz und dem Austausch mit internationalen Experten zeigt sich, dass neue Trends auch jeweils spezifische Risiken bergen können.

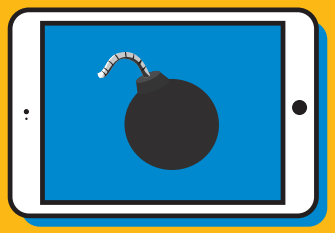
WESENTLICHE RISIKOBEREICHE FÜR KINDER UND JUGENDLICHE SIND JEDOCH RELATIV UNABHÄNGIG VON SOLCHEN KURZFRISTIGEN TRENDS.

Ein Beispiel hierfür ist „Cybermobbing". Darunter versteht man das absichtliche Beleidigen, Bedrohen, Bloßstellen oder Belästigen anderer mithilfe von Internet- und Mobiltelefondiensten über einen längeren Zeitraum hinweg. Cybermobbing findet im Internet (bspw. in Sozialen Netzwerken, in Video-Portalen) und über Smartphones (bspw. durch Instant-Messaging-Anwendungen wie WhatsApp, lästige Anrufe etc.) statt. Gerade unter Kindern und Jugendlichen kennen Opfer und TäterInnen einander aber meist aus dem „realen" persönlichen Umfeld wie z. B. der Schule, dem Wohnviertel, dem Dorf oder der ethnischen Community. Deswegen geht das Cybermobbing oft mit Mobbing in der Offline-Welt einher: Teils wird das Mobbing online weitergeführt, teils beginnt Mobbing online und setzt sich dann im Schulalltag fort. Aus diesem Grund sind Mobbing und Cyber-Mobbing in der Mehrheit der Fälle nicht voneinander zu trennen.
Risiken wie diese, die auch jenseits der „Online-Welt" im Wahrnehmungsfeld der Pädagogik liegen (sollten), finden sich dabei also auch in unterschiedlichen Ausprägungen in der „Online-Erlebniswelt" von Kindern wieder. Dies sind quasi „alte" Risiken in neuem Gewand.

IM ZUGE DER DIGITALISIERUNG KÖNNEN JEDOCH AUCH „NEUE" RISIKEN ENTSTEHEN, DIE SICH DAUERHAFT IM WAHRNEHMUNGSFELD DER PÄDAGOGIK ETABLIEREN SOLLTEN.

Ein Beispiel hierfür sind vernetzte Spielzeuge: Dass manche Spielzeuge mit Mikrofon, Kamera und Internetverbindung ausgerüstet sind und welche Risiken bzw. Gefahren dies bergen kann (bspw. für die Privatsphäre von Kind und Familie), ist derzeit noch nicht jedem bewusst, der diese Spielzeuge kauft bzw. nutzt. Diese technische Entwicklung ist noch recht neu, wird jedoch sicherlich für längere Zeit ein Sicherheitsthema bleiben.

Zunächst ist es einmal wichtig, wesentliche Risikobereiche, die sich für Kinder und Jugendliche herauskristallisiert haben, zu kennen.



✖ Die verschiedenen Risikokategorien

Um die typischen Risiken, denen Kinder im Internet ausgesetzt sind, besser zu überblicken, und die daraus resultierenden Schutzbedürfnisse ableiten zu können, kann es praktisch sein, Risiko-Kategorien zu bilden:

- **Kontaktrisiken („contact risks“)**
- **Inhaltsrisiken („content risks“)**
- **Konsumrisiken („consumption risks“)**

Auch wenn diese drei Bereiche nicht absolut trennscharf voneinander zu unterscheiden sind und es Überschneidungen geben kann (bzw. manche Beispiele auch in mehrere Kategorien passen könnten), so ermöglicht diese Einteilung zum Einstieg eine gute Orientierung.

KONTAKTRISIKEN

Wenn Kinder mit anderen Menschen über das Internet in Kontakt treten (contact risk), bestehen vor allem folgende Risiken:

▸ Cybermobbing
Cybermobbing (Synonym zu „Cyberbullying“) bedeutet Mobbing mithilfe von Internet- und Mobiltelefondiensten (siehe S.10 für ausführliche Beschreibung).

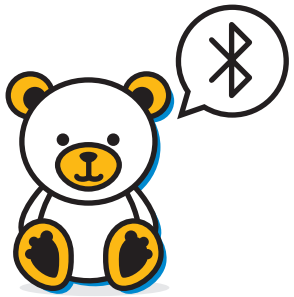
▸ Grooming
Grooming beschreibt einen Vorgang, bei dem ein Erwachsener über einen längeren Zeitraum (Wochen oder Monate) ein Vertrauensverhältnis zu einem Minderjährigen im Internet aufbaut, mit dem Ziel, ihn/sie zu sexuellen Handlungen (online und offline) zu überreden.

▸ Sexting
Der Begriff „Sexting" setzt sich aus den Wörtern „Sex“ und „Texting“ zusammen. Er beschreibt das Austauschen intimer Fotos über Mobiltelefone und soziale Netzwerke Die größte Gefahr beim Sexting: Nacktaufnahmen, die als privater Vertrauensbeweis gedacht waren und plötzlich öffentlich im Netz zirkulieren. Sexting ist ein Phänomen, das sich immer mehr, vor allem unter Jugendlichen und jungen Erwachsenen ausbreitet.

▸ Sextortion
Sextortion bedeutet Erpressung anhand von Material mit sexuellem Inhalt (Bilder, Videos). Das Opfer wird dazu gebracht, Fotos/Videos der eigenen Person mit sexuellen Posen per Nachricht an den Täter zu schicken und wird später damit erpresst bzw. Erpressung findet statt unter der Behauptung, peinliche Nacktaufnahmen des Opfers zu besitzen (z.B. durch „Hacken“ des Computers) und zu veröffentlichen.

▸ Online Challenges
Nicht immer muss es bei gefährlichem-Kontakt mit anderen um sexuelle Handlungen bzw. Missbrauch oder um Mobbing gehen; es bestehen auch andere Risiken, die durch psychologische Manipulation an Kindern denkbar und möglich sind. „Online Challenges“ sind gefährliche Spiele, die häufig über soziale Netzwerke Verbreitung finden und die Teilnahmer zu gefährlichem oftmals selbstverletzendem bis lebensgefährdenen Handlungen anstacheln. Solche gefährliche Phänomene können manchmal innerhalb kürzester Zeit zum Trend und dadurch besonders reizvoll für Kinder und Jugendliche werden.

▸ Kettenbriefe
Ein sehr häufig auftretendes und damit beinahe schon Alltagsphänomen sind Kettenbriefe, die per Chatapp, Email oder auf ähnlichen Wegen verbreitet werden. Oftmals sollen diese Angst und Schrecken verbreiten, indem Drohungen an den Enpfänger ausgesprochen werden, wenn dieser nicht eine bestimmte Handlung innerhalb einer gewissen Zeit ausführe (bspw. die Nachricht schnell weiterzuleiten).



▸ **„Smart toys“**
engl. vernetzte Spielzeuge
Es gibt immer mehr Spielzeuge auf dem Markt, die mit dem Internet verbunden sind. Solche „smart toys“ können nützlich sein, jedoch auch verschiedene Risiken bergen. Im Falle eines vernetzten Teddybären („cloud pet“) konnten sich Fremde aus einer Distanz von 10 m über die Bluetooth-Verbindung im Teddybären Gespräche des Kindes mit dem Teddy bzw. die stattfindenden Gespräche im Raum mithören.

Zudem war es auch sehr einfach, solche Gespräche aus Haushalten, in denen dieser Bär aktiviert war, im Internet anzuhören, da die Sprachdateien vom Teddybären über Bluetooth auf das Smartphone und von dort an einen recht ungeschützten Server im Internet geschickt und dort gespeichert wurden. Sowohl im Hinblick auf den Schutz der Privatsphäre als auch auf die Gefahr, dass Fremde sich durch unzureichend geschützte vernetzte Spielzeuge ggfs. Kontakt zum Kind aufbauen können, sind „smart toys“ immer kritisch zu prüfen.

Hier ist die Besonderheit hervorzuheben, dass oftmals weder dem Kind, noch den Eltern bewusst ist, dass "smart toys" (vernetzte Spielzeuge) überhaupt mit dem Internet verbunden sind. Und damit ist dann, im Gegensatz zum Nutzen von "traditionellen" vernetzten Geräten (wie Computer, Laptop, Smartphone oder Tablet), oftmals gar kein Bewusstsein für damit einhergehende Risiken vorhanden.[5]

[5] Hilfreiche Tipps zum Kauf solcher Spielzeuge und ausführliche Informationen über die jeweiligen Risiken, gibt es auf www.bee-secure.lu/factsheet/smart toys

INHALTSRISIKEN

Es gibt viele Inhalte, die nicht für Kinder geeignet sind bzw. sogar schädlich sein können. Diese sind in Form von Fotos, Bildern, Videos, Spielen oder auch Texten zu finden. Außerdem gilt es zu beachten, dass Kinder nicht mehr nur Inhalte von anderen begegnen, sondern immer früher auch selber zum/r Produzent/In von Inhalten werden.

Zu problematischen Inhalten gehören folgende:

▸ **Sexueller Kindesmissbrauch Online**
Sexueller Kindesmissbrauch nimmt eine online Dimension an, wenn beispielsweise sexuelle Missbrauchstaten an Kindern fotografiert oder gefilmt und dann hochgeladen und online zugängig gemacht werden, sei es für persönlichen Gebrauch oder zum Teilen mit anderen. Jedes erneute Ansehen oder Teilen dieses Materials stellt ein erneutes Vergehen gehen die Kinderrechte dar. Inhalte von sexuellem Missbrauch an Kindern können an die BEE SECURE Stopline (stopline.bee-secure.lu) gemeldet werden.

▸ **Pornographie**
Pornographie kann aus verschiedenen Gründen sehr problematisch werden, vor allem dann, wenn die Kinder das Gesehene und dabei Erlebte nicht einordnen können und/oder falsche Vorstellungen über Sexualität entwickeln.

▸ **Gewalt**
Des Weiteren können Gewaltdarstellungen und anderes Bild-/Videomaterial genannt werden, die nicht kindgerecht sind.

▸ **Influencer**
Im Kinder- und Jugendbereich spricht man mittlerweile von sogenannten "Influencern" („Beeinflussern“), die beispielsweise auf Youtube oder Instagram Großzahlen an Kindern und Jugendlichen Publikum erreichen. Durch ihre große Bedeutung für das junge Publikum können sie schnell als verlässliche Informationsquelle wahrgenommen werden, auch wenn bei vielen Selbstdarstellern kommerzielle Motive (Einnahmen durch Werbung) und damit möglichst hohe Klickzahlen meist im Vordergrund stehen. Daher ist es wichtig, dass Kinder auch mit diesen Vorbildern kritisch umzugehen lernen.

All diese Beispiele illustrieren, dass es dem Kindeswohl zuträglich sein kann, wenn auch in der Maison Relais ein Raum vorhanden ist, in welchem Kinder über Erlebnisse und der Konfrontation mit (problematischen) Inhalten berichten können, ohne verurteilt zu werden, und mit Hilfe des Erziehers das Gesehene und Erlebte einordnen können (Fakt vs. Fiktion; Werbung; Medieninhaltskompetenz).

KONSUMRISIKEN

Damit sind weitestgehend alle Risiken gemeint, die mit einer Anmeldung bei Apps/ Plattformen bzw. Services einhergeben können. Zu den häufigsten Konsumrisiken zählen:

▸ **Finanzielle Risiken**
Kostenfallen, Abzocke, unerwartet hohe Handyrechnungen, ...

▸ **Werbung**
Was ist Werbung, was ist Information - woran erkenne ich bei zunehmend verschwimmenden Grenzen den Unterschied? Kinder müssen mit verschiedenen Formen von Werbung, Beeinflussung bzw. Aufforderungen zu bestimmten Handlungen (bspw. dem Kauf von Guthaben/ Spielgegenständen in einer App) umgehen lernen.

▸ **Qualität und Dauer des Konsums/ Nutzens**
Ein „Zuviel" vs „zu wenig" an IT-Nutzung muss dabei immer auch im Zusammenhang bzw. im Verhältnis zur Qualität betrachtet werden. Die Frage: „Warum und wie wird IT genutzt?" sollte in einer solchen Diskussion immer Beachtung finden, um eine gesunde Entwicklung zu begünstigen - im Übrigen gilt das nicht nur für Kinder.

▸ **Datenschutz und Privatsphäre**
manche Apps/Anbieter sammeln auf unterschiedlichen Wegen persönliche Daten des Nutzers, also auch von Kindern, und nutzen und/oder verkaufen diese für kommerzielle Zwecke.

Ein Ziel von Medienerziehung sollte daher sein, Kinder in deren Entwicklung zu kritischen Teilnehmern und Mitgestaltern unserer (digitalen) Gesellschaft zu fördern. Ein bewusster Umgang mit und das Wissen um den Wert der eigenen Daten sollte frühzeitig gelehrt werden. Denn vermeintlich unpersönliche Daten können sehr persönliche Informationen einer Person verraten (Charakter, Gefühle, Aufenthaltsort, etc). Apps und Dienste für Kinder sollten daher stets auch dahingehend kritisch ausgesucht bzw. datenschutzorientiert angewendet werden.

TROTZ RISIKEN, EINEN POSITIVEN BLICK WAHREN

Diese Übersicht über Risiken zeigt, wie wichtig es ist, Kinder nicht nur durch technische Maßnahmen vor schlimmen Inhalten zu schützen (bspw. durch den Einsatz von technischen Inhaltsfiltern, wie unten beschrieben), sondern, dass es bei der Sicherheit im Internet um die gesamte Palette menschlichen Verhaltens und Erlebens gehen kann – und daher ist pädagogische Begleitung und das eigene Vorleben bei der Internetnutzung so wichtig. Da es in diesem Kapitel in geballter Form um negative Aspekte des Internets geht, seien an dieser Stelle abschließend drei wichtige Gedanken in Form von Tipps genannt:

- **Tipp 1: Ausgewogene Sichtweise wahren**
- **Tipp 2: Sie können die Gefahren nicht ändern – aber die Kinder stärken**
- **Tipp 3: Die Ruhe bewahren – für jedes Problem finden sich Lösungen**

Tipp 1
Ausgewogene Sichtweise wahren
Bei der Diskussion um solche Risiken, Sicherheit und Schutz kann es schnell geschehen, dass man sich auf negative/gefährliche Aspekte der IT-Nutzung fokussiert und dabei die positiven, sinnvollen Aspekte aus den Augen verliert. Wenn Sie also die „Sicherheitsbrille" tragen, achten Sie darauf, regelmäßig aktiv über den positiven Nutzen und den Mehrwert von IT nachzudenken, um eine ausgewogene Sichtweise zu wahren.

Tipp 2
Sie können die Gefahren nicht ändern – aber die Kinder stärken
Nehmen Sie die Tatsache zur Kenntnis, dass digitale Medien ein fester Bestandteil der alltäglichen Lebenswelt von Kindern sind und Sie durch ihr pädagogisches Wirken positiv dazu beitragen, dass Kinder diese kompetenter nutzen. Das bedeutet auch, dass sie dazu beitragen, Kinder weniger verwundbar bzw. resilienter im Bezug auf die oben genannten Risiken/Gefahren zu machen.

Tipp 3
Die Ruhe bewahren – für jedes Problem finden sich Lösungen
Wenn ein Gerät/eine App nicht so funktioniert wie es soll, falls ein Kind auf einer unpassenden Seite gelandet ist, falls Sie einen Virus auf dem Gerät vermuten… bleiben Sie besonnen und lassen Sie (nach Möglichkeit) das Kind miterleben, wie Sie das jeweilige Problem zu lösen versuchen.

Die Fähigkeit, mit (unerwartet) auftretenden Problemen konstruktiv umzugehen und Lösungsstrategien zu entwickeln, ist wesentlich für die „digitale Welt" von heute und morgen. Seien Sie sich also gerade darüber im Klaren, dass Sie besonders hier ein positives Beispiel sein können. Dass man schnell an die Grenzen des eigenen Wissens- und Erfahrungsbereichs stoßen kann, ist auch hierbei normal. Finden Sie dann einfach heraus, wo oder von wem Sie Hilfe bekommen können (bspw. wer ist hausinterner Ansprechpartner).

2. SICHERHEITSTIPPS FÜR DIE PRAXIS

„Internetsicherheit" bedeutet also im Fall der Maison Relais, dass eine bestmögliche Sicherheit geschaffen werden sollte, die sich nach den (Schutz-)bedürfnissen von Menschen und deren Daten in der Einrichtung richtet. 100-prozentige Sicherheit gibt es innerhalb und außerhalb des Internets nie, da ist es wie in allen Bereichen des Lebens. Sicherheit ist also relativ.

Sie hängt von einmaligen Maßnahmen, sowie regelmäßigen Prozeduren ab. Damit ist Sicherheit kein Zustand, sondern ein Prozess.

Um diesen Prozess für die Maisons Relais übersichtlich zu gestalten, wurden die folgenden Sicherheitstipps in 5 Bereiche eingeteilt:

✖ 1. Verhalten der ErzieherInnen/NutzerInnen

✖ 2. Technische Maßnahmen

✖ 3. Zuständigkeiten bestimmen

✖ 4. Regeln aufstellen und kommunizieren

✖ 5. Auf dem Laufenden halten

✖ 1. VERHALTEN DER ERZIEHER(INNEN)/NUTZER(INNEN)

Das Thema Sicherheit sollte sich in der Denk- und Handlungsweise der ErzieherInnen/NutzerInnen widerspiegeln. Das eigene Verhalten ist der wichtigste Schutz – auch im Umgang mit dem Internet in der Maison Relais.

Zunächst bedeutet dies, jenseits von allen technischen Sicherheitsmaßnahmen, dass die Verantwortlichen der Einrichtung sowie das dortige Personal sich beim Umgang mit dem Internet/vernetzten Geräten an drei Handlungsprinzipien orientieren sollten:

- Prinzip 1:
Ein datenschutzorientiertes Handeln

- Prinzip 2:
Sich seiner Vorbildrolle bewusst sein

- Prinzip 3:
Das Thematisieren/Begleiten von Internetaktivitäten der Kinder

▸ Prinzip 1:
Ein Datenschutzorientiertes Handeln

AUF EBENE DER VERWALTUNG IST DATENSCHUTZ DAS OBERSTE GEBOT.

Es ist sehr wichtig, vertrauliche Daten von Kindern und Personal grundsätzlich vor unberechtigten Zugriffen zu schützen. Bei rechtlichen Fragen rund um den Datenschutz, beispielsweise zur Rechtskonformität in der eigenen Datenverwaltung, ist die CNPD[6] erster Ansprechpartner[7].

Um konform mit der Datenschutzgrundverordnung zu sein, sollte jede Einrichtung nachweisen können, dass sie bewusst und sicherheitsbedacht mit persönlichen Daten umgeht und diese rechtskonform speichert bzw. nutzt. Dies gilt für alle Arten der Datenspeicherung und -verwaltung – also nicht nur für digitale, sondern auch analoge Formen (bspw. das Ablegen von Dokumenten in Ordnern).

[6] Commission nationale pour la protection des données, www.cnpd.lu
[7] Allgemeine und spezifische Fragen kann man dort jederzeit über das Kontaktformular an die zuständigen Experten stellen. Zudem gibt es auf der Webseite der CNPD auch praktische Empfehlungen, die für die Maison Relais hilfreich sein können.

▸ **Prinzip 2 :**
Sich seiner Vorbildrolle bewusst sein

DAS BETREUUNGSPERSONAL SOLLTE DARAUF ACHTEN, SICH IM EIGENEN UMGANG MIT DEM INTERNET UND VERNETZTEN GERÄTEN VORBILDLICH, SICHERHEITS-BEDACHT UND RECHTS-KONFORM ZU VERHALTEN.

Zum einen, um zur IT-Sicherheit in der Maison Relais im Allgemeinen beizutragen, zum anderen aber auch in ihrer Vorbildrolle als ErzieherIn, damit die Kinder einen guten Umgang mit IT und wichtige Sicherheitsreflexe auch am Modell lernen können.

Hierzu gehört im Kontext der beruflichen Nutzung (während der Arbeitszeit) ein guter Umgang mit IT-Geräten (Computer, Tablets, Smartphones, vernetzte andere Geräte) und Passwörtern, sowie ein reflektierter und kritischer Umgang mit Inhalten (Texte, Videos, Fotos) und das verantwortungsbewusste und rechtskonforme Erstellen und Verbreiten von Fotos/Videos (Recht am eigenen Bild, Urheberrecht). Es kann sehr nützlich sein, konkrete Punkte innerhalb der Einrichtung in Form von einfachen Regeln festzuhalten (siehe Abschnitt „Regeln für das Personal“).

Nicht zuletzt sollte bei der „privaten“ Nutzung außerhalb der Arbeitszeit, beispielsweise in sozialen Netzwerken wie Facebook, auf das Wahren der eigenen Reputation geachtet werden[8].

[8] Mehr Informationen und Tipps dazu im Ratgeber „Auch digital ein Vorbild sein - Ein Ratgeber für Erzieher und Lehrer für den Umgang mit sozialen Netzwerken“ von BEE SECURE (erhältlich auf DE und FR).

▸ **Prinzip 3:**
Das Thematisieren/Begleiten von Internetaktivitäten der Kinder

Gerade wenn es um die „Lebenswelt Internet“ geht, ist es **besonders hilfreich, wenn Kinder eigene internetbezogene Erlebnisse pädagogisch begleitet erzählen,** reflektieren und damit auch diese einzuordnen lernen. Dies ist auch hilfreich, um grundlegende Sicherheitsreflexe zu lernen (bspw., dass man seine Login-Daten/Passwörter nicht an andere weitergibt) und sowohl nachträglich als auch präventiv Situationen zu erkennen, in denen Sicherheitsreflexe greifen sollten (bspw. ein unbekannter Mitspieler fragt das Kind in einem Online-Spiel nach seinen persönlichen Daten – das Kind verrät diese aber nicht und erzählt seinen Eltern oder dem/der ErzierherIn von dieser Situation).

Wenn Kinder das Internet in der Maison Relais nutzen, sollte dies grundsätzlich unter pädagogischer Begleitung stattfinden. Ziel davon sollte es zudem sein, dass der Erzieher ein vertrauenvoller Ansprechpartner auch für die „Lebenswelt Internet“ des Kindes ist.

2. TECHNISCHE MAßNAHMEN

Die folgenden Empfehlungen sind allgemeiner Natur und sollten grundsätzlich für jede Maison Relais umsetzbar sein. Beachten Sie aber, dass Ihre (internen oder externen) Techniker vor Ort einen genauen Überblick über Sinn (oder Unsinn) der folgenden technischen Schutzmaßnahmen und deren Realisierbarkeit für Ihre spezifische Einrichtung haben und ggfs. mit anderen Vorschlägen bzw. Lösungen aufwarten werden. Dies ist auch in Ordnung, solange diese Lösungen sich nach den Bedürfnissen der Menschen und Daten in der Einrichtung richten. Viele Wege führen nach Rom – die Folgenden jedoch ohne allzu viele Zwischenstopps.

Die drei folgenden technischen Schutzmaßnahmen gilt es zu beachten:

- Schutzmaßnahme 1:
Internetzugang sichern

- Schutzmaßnahme 2:
Getrennte Netzwerkzonen einrichten

- Schutzmaßnahme 3:
Internet-Filter einsetzen

▸ Schutzmaßnahme 1: Internetzugang sichern

In manchen Einrichtungen wird der Internetzugang von der umliegenden Schule, der Gemeinde und/oder einem sonstigen Träger bereits betreut und ist vielleicht sogar schon nach entsprechenden Sicherheitsvorgaben eingerichtet. Es kann also hilfreich sein, sich nach den Sicherheitslösungen zu erkundigen, welche die Schule/Gemeinde/bzw. sonstige relevante Akteure und Einrichtungen gewählt haben um herauszufinden, ob und wie diese für die Maison Relais herangezogen werden könnten.

Ansonsten gibt es auch die Möglichkeit, mit einer externen Firma zusammenzuarbeiten, welche die technische Einrichtung und ggfs. auch die Wartung sowie weitere Dienstleistungen übernehmen kann, die im Folgenden angesprochen werden (Einrichtung einer Blacklist bzw. Whitelist für Webseiten; Einteilung des Netzes in verschiedene Zonen, etc.).

Der unbefugte Zugang zum Netzwerk durch Außenstehende sollte durch gängige Sicherheitsmaßnahmen erschwert werden. Das heißt, bei Wi-Fi sollte darauf geachtet werden, verschlüsseltes WLAN (WPA2) mit einem sicheren Passwort zu nutzen und für kabelgebundenes Netzwerk (LAN) sollte auf Portkontrolle/ Mac-Adressenfilter geachtet werden.

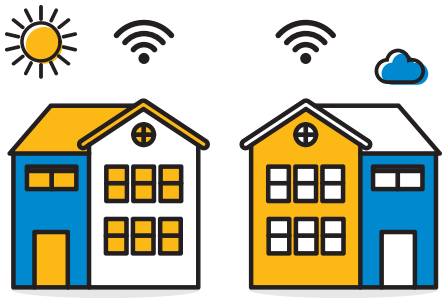
▸ Schutzmaßnahme 2: Getrennte Netzwerkzonen einrichten

Grundvoraussetzung für eine gelungene Kontrolle des Zugriffs auf Informationen ist die Einteilung des internen Netzwerkes in getrennte Netzwerkzonen für verschiedene Benutzergruppen: eine für Kinder und eine für das Personal. Optional kann auch darüber nachgedacht werden, eine dritte Zone für Besucher hinzuzufügen. In den meisten Maisons Relais sollten jedoch zwei Netzwerkzonen für Kinder und Personal ausreichen.

Warum ist die Einteilung in Netzwerkzonen wichtig?

Wenn alle Geräte im Haus (PCs, Tablets, Laptops, Drucker,etc) an dasselbe Netzwerk angeschlossen sind, können diese Geräte prinzipiell aufeinander zugreifen bzw. miteinander kommunizieren. Übrigens: diese Kommunikation der Geräte miteinander kann bei den meisten Routern/Access Points deaktiviert werden und in kabelgebundenen Netzwerken kann man mithilfe von Firewalls auch entsprechende Einstellungen vornehmen, die dieser Kommunikation gewünschte Grenzen setzt.

Kinder sollten jedenfalls nicht über ihre vernetzten Geräte (bspw. Tablets, PC) die Möglichkeit haben, auf die Verwaltungs-Computer zuzugreifen, oder andere Geräte im Netzwerk (wie einen Drucker in der Personalverwaltung) auf unerwünschte Art und Weise anzusteuern. Dabei geht es nicht nur um die Vermeidung von



möglichem Unfug, den die Kinder anstellen könnten. Vielmehr geht es auch um eine grundsätzliche Risikominimierung im Bezug auf Schadsoftware (Computerviren bzw. Malware) und Hacker, welche sich sonst zu leicht Zugang zu allen im Netzwerk befindlichen Geräten über das Gerät des Kindes verschaffen könnten.

Auf technischer Ebene gibt es verschiedene Möglichkeiten, getrennte Zonen anzulegen, so zum Beispiel durch eine Einrichtung spezifischer Firewall-Regeln oder das Hintereinanderschalten von zwei oder mehreren Routern.

Die Unterteilung in Netzwerkzonen ermöglicht allen Beteiligten eine an ihre Bedürfnisse und Befähigungen angepasste Benutzung des Internets und der informatischen Systeme in der Maison Relais. Sie sind, entsprechend den Zuständigkeiten ihrer Benutzer, an verschiedene Freiheiten gebunden.

Die **erste Zone heißt „Kinder“** und umfasst den Internetzugang für alle Geräte, die von Kindern genutzt werden dürfen. Diese Zone wird von den Kindern unter Aufsicht von ErzierherInnen genutzt und darf keinerlei persönliche Informationen oder Daten enthalten. Sie dient dem Nutzen vernetzter Geräte im Rahmen pädagogischer Aktivitäten. Das Internet, auf das die Kinder Zugriff haben, ist gefiltert (siehe „gefiltertes Internet“). Dies soll verhindern, dass Minderjährige mit gefährdenden oder illegalen Inhalten in Kontakt kommen.

Die **zweite Zone heißt „Betreuungspersonal“** und richtet sich auch an selbiges. Sie darf nur von hauptamtlichen Mitarbeitern benutzt werden (nicht von Zeitarbeitern oder Praktikanten), da sie den Zugriff auf persönliche Informationen gewährt. Es ist unbedingt notwendig, dass sich das Betreuungspersonal über ein sicheres Passwort in das Netz einloggt. Login-Daten dürfen unter keinen Umständen an die Kinder oder an sonstige Personen außerhalb des berechtigten Kreises gelangen, um Missbrauch und Verletzung des Datenschutzes zu verhindern.

Die optionale **dritte Zone ist die „Mittelzone“**. Sie kann am besten an individuelle Bedürfnisse angepasst werden. Somit eignet sie sich als Zone für nichtpermanente Mitarbeiter oder auch Besucher, denen mehr Freiheiten im informatischen System zugestanden werden. Über diese Zone gibt es keinen Zugriff auf persönliche Informationen. Sie lässt sich entsprechend der aktuellen Bedürfnisse individuell konfigurieren.

Je nach Räumlichkeiten und Bedürfnissen kann auch die Nutzung eines räumlich begrenzten **Wi-Fi-Hotspots** interessant sein. Dieser kann lokal so eingerichtet werden, dass beispielsweise der Internet-Zugang für Kinder per Tablet (welches meist nicht per LAN-Kabel, sondern nur per Wi-Fi bzw. Drahtlosnetzwerkverbindung online gehen kann) in einem eigens dafür vorgesehenen Medienraum gewährleistet ist. Ausserhalb dieses Raumes ist dann jedoch keine Internetnutzung für die Kinder möglich, was je nach räumlichen Gegebenheiten eine durchgehende Begleitung von Kindern während der Online-Nutzung in der Praxis erleichtern kann.

Um also zu vermeiden, dass es zu unbefugtem Zugriff durch nicht berechtigte Benutzer kommt, sind die zwei bzw. drei Zonen streng voneinander getrennt. Es ist empfehlenswert, dass jeder Benutzer sich anhand eines Benutzernamens und eines Passwortes identifiziert. So kann nachvollzogen werden, wer sich zu welchem Zeitpunkt in welcher Zone aufgehalten hat. Die Trennung der Netze ist wesentlich, um eine Kontrolle des Internets und eine Absicherung der informatischen Vorgänge in der Maison Relais a priori zu gewährleisten. Sie ermöglicht mit einfachen Mitteln die Vergabe von individuell abgestimmten Rechten. So wird der gesicherte Zugriff zum Internet, der Zugriff auf Informationen sowie der präventive Schutz vor Malware (Schadprogramme, wie der „klassische Computervirus“) vereinfacht.

▸ **Schutzmaßnahme 3:**
Internet-Filter einsetzen

KINDER KÖNNEN DURCH ANWENDUNG VON „INTERNETFILTERN“ VOR DEM DIREKTEN ZUGRIFF AUF SCHÄDLICHE INHALTE IN DER MAISON RELAIS GESCHÜTZT WERDEN.

Man unterscheidet dabei zwischen zwei Filterarten: „**Blacklists**“ und „**Whitelists**“.

✖ Blacklist:
Bei einer „Blacklist“ werden bestimmte Internetseiten oder Domainnamen auf eine „schwarze Liste“ gesetzt, so dass diese für den Internetnutzer, in diesem Fall das Kind, gesperrt werden. Solche Blacklists werden daher beispielsweise für Jugendhäuser empfohlen. Die Einrichtung eines solchen Filters kann auch als grundlegende Maßnahme für den Internetzugang der Einrichtung (auch für Erwachsene) empfohlen werden, da illegale/gefährliche Inhalte automatisch gesperrt werden. Einige der sogenannten Blacklists gibt es für Schulen bzw. Bildungseinrichtungen sogar kostenlos[11].

✖ Whitelist:
Für Kinder bis 12 Jahre kann sich jedoch der Einsatz einer „Whitelist“ in vielen Fällen besser eignen, da diese wesentlich einfacher einzurichten ist und zudem „noch mehr Schutz“ vor Inhalten bieten kann als eine Blacklist. Bei der "Whitelist" wird eine Liste erstellt mit Seiten bzw. Domains, die vom Nutzer (also dem Kind) erreicht werden können. Alle Seiten bzw. Domains, die nicht auf dieser Liste eingetragen sind, sind grundsätzlich gesperrt. Das bedeutet zum Beispiel auch, dass Werbefenster, die oftmals von externen Seiten (Servern) kommen, nicht angezeigt werden. Jedoch auch kindgerechte Inhalte, die von externen Servern kommen, werden zunächst durch den Whitelist-Filter gesperrt. Allerdings kann man, je nach Filter, auch nachträglich weitere Seiten der Whitelist hinzufügen[12].

[11] Eine Beispiel für eine solche Blacklist: http://www.shallalist.de/.
[12] Ein Whitelist mit rund 200 kindgerechten Webseiten findet sich auf www.bee-secure.lu/beefilter

Eine „Do it yourself“ – Lösung für die Einrichtung eines Whitelist-Filters wurde im Rahmen des Pilotprojektes „Secure MR Dippach“ entwickelt und getestet: der „BEE Filter“. Dieser besteht aus einem kleinen Mini-Computer („Rasperry Pi), der als kleiner Server für den Internetzugang für Kinder zwischengeschaltet wird, und den Zugang entsprechend der angegebenen Webseiten auf der Whitelist für Kinder filtert. Dieser hat den Vorteil, kostengünstig (ca. 70 EUR) und selbst von dem/der Geräter-ManagerIn innerhalb der Einrichtung oder einer anderen zuständigen Person veränderbar zu sein[13]. Diese Lösung sollte am besten von einer technikaffinen Person umgesetzt und betreut werden. Sie eignet sich daher für Einrichtungen, in denen eine solche Person vor Ort. verfügbar ist und eine kostengünstige Lösung angestrebt wird.

[13] Eine technische Anleitung inklusive Whitelist findet man hier: https://github.com/msilvoso/beefilter

Eine Überlegung wert:
Das Kind bewegt sich bei einem gefilterten Zugang in einem künstlich begrenztem, „realitätsfremden“ Internet – was je nach Situation (Alter und Entwicklungsgrad des Kindes, pädagogisches Ziel einer Aktivität) als mehr oder weniger sinnvoll betrachtet werden kann.

Es kann also darüber nachgedacht werden, den Internetzugang für alle Kinder grundsätzlich mit einer Whiteliste zu filtern, jedoch je nach Situation/Kind bestimmte Seiten temporär freizuschalten bzw. manche Geräte für bestimmte Kinder temporär in der Mittelzone zuzulassen (welche durch eine Blacklist grundsätzlich geschützt sein sollte und dem Kind erlaubt, unter Begleitung im „echten Internet“ aktiv zu sein). Je nach Aktivität bzw. pädagogischem Ziel und dem Reifegrad des Kindes können Kinder auf diese Weise individuell gefördert werden (bspw. am Beispiel lernen, Werbung von Information zu unterscheiden).

3. ZUSTÄNDIGKEITEN BESTIMMEN

Es gibt verschiedene Möglichkeiten dafür, wer sich praktisch „um die Technik im Haus“ kümmern kann. Verantwortlich für die Internetsicherheit ist jedoch letztendlich immer die Leitung der Einrichtung.

Folgende Möglichkeiten können empfohlen werden:

„Gerätemanager“ im Haus
Ernennen Sie eine zuständige Person, „GerätemanagerIn“ samt StellvertreterIn für Endgeräte (Computer, Tablets, Laptops, vernetzte Geräte,...) im Haus. Diese Person sollte interner Ansprechpartner bei technischen Problemen mit den von Kindern genutzten Endgeräten (Computer, Tablets etc) und dem diesbezüglichen Netzwerk sein. Je nach Kompetenzen dieser Person, kann diese entweder selber die folgenden Aufgaben übernehmen oder alternativ sicherstellen, dass diese **REGELMÄßIG** durchgeführt werden:

- Updates (von Betriebssystemen/ Programmen)
- Backups wichtiger Daten
- Einen sicheren, angemessenen Umgang mit Passwörtern etablieren (Zugänge zu Benutzer-Konten und Geräten mit Passwörtern schützen, ggfs. Passwörter verwalten, Benutzer auf guten Umgang mit Passwörtern hinweisen und Hilfestellung bieten)
- Den „Datenmüll entsorgen“ auf gemeinsam genutzten Geräten (ungenutzte/unwichtige Daten/Programme löschen)
- Die Zugriffsrechte im Blick behalten (wer darf etwas auf einem Gerät installieren? Wer kommt an welche Daten heran?)

Zusatzmöglichkeit:
Fernwartung im Haus
Je nach Situation kann die Wartung der Geräte, wie bspw. Tablets, auch (zusätzlich) durch sogenannte „Fernwartung“ erfolgen. Hierbei kann die/der Techniker/In aus der Ferne per Internet auf das Gerät bzw. die Geräte in der Maison Relais zugreifen und diese(s), je nach genutzter Software, verwalten und auch Filtereinstellungen vornehmen. Für Tablets gibt es mittlerweile auch solche Software, welche bspw. den Download bestimmter Apps sperren kann. In Schulen findet diese Art des Geräte- bzw. Netzwerkmanagements häufig Anwendung.

4. REGELN AUFSTELLEN UND KOMMUNIZIEREN

Regeln für den Umgang mit Computer, Tablet und Internet sollten nicht nur vorhanden sein, sondern auch allen Beteiligten klar kommuniziert werden. In manchen Einrichtungen gibt es bereits Regeln zum Umgang mit dem Internet. Es lohnt sich, diese regelmäßig zu überprüfen und sicherzustellen, dass die Regeln allen Mitarbeitern bekannt sind.

Anstatt Regeln an dieser Stelle en detail vorzuformulieren, empfiehlt dieser Ratgeber individuelle Regeln aufzusetzen, die sich an den konkreten Gegebenheiten des Hauses orientieren... Um jedoch nicht „bei Null anzufangen“, werden in dem weiteren Abschnitt Themen genannt, die in den Regeln angesprochen werden sollten.

Regeln für das Personal
Für das Personal sollten Regeln gelten, die sich an den drei oben genannten Prinzipien (Datenschutz, Vorbild, Begleitung) orientieren. Es ist wichtig, dass alle ErzierherInnen verstehen, dass

JEDER NUTZER EINE MITVERANTWORTUNG FÜR DIE GERÄTE TRÄGT UND GEWISSENHAFT MIT PERSÖNLICHEN DATEN SOWIE DEN GERÄTEN UMZUGEHEN HAT

- auch, wenn ein „Gerätemanager“ im Haus die Geräte und deren regelmäßige Wartung im Blick hat.

Die Regeln sollten zum Ziel haben, im Bezug auf wichtige Themenbereiche Klarheit zu schaffen, und zwar vor allem im Bezug auf den Umgang mit

- Persönlichen Daten (digital und auf Papier)
- Passwörtern/Zugängen
- E-Mails
- Dem (eigenen) Smartphone am Arbeitsplatz
- Fotos und Videos

Weitere Themen ergeben sich sicherlich aus den hausinternen Gegebenheiten. Achten Sie darauf, die Regeln klar und einfach zu halten. Für Jugendhäuser hat BEE SECURE 2013 Regeln für ErzierherInnen ausformuliert, die bei Bedarf auch als Vorlage für die Maisons Relais dienen können[14].

Es kann sehr hilfreich sein, diese Regeln bei regelmäßigen Personalversammlungen zum Thema zu machen und dabei auch regelmäßig eine Zwischenbilanz zu ziehen. So kann gewährleistet werden, dass die Regeln stets aktuellen (technischen) Entwicklungen und sonstigen relevanten Gegebenheiten gerecht werden und zweckdienlich bleiben.

[14] Die Vorlage findet sich hier www.bee-secure.lu/secure-MJ

▸ Regeln für Kinder

Regeln für das Surfen
Für Kinder sollten im Umgang mit dem Internet Regeln aufgestellt werden. BEE SECURE schlägt als allgemeine Grundlage „10 Regeln für Kinder im Internet“ vor (siehe Anhang), die den Kindern nahegebracht werden sollten. Die wichtigste Botschaft dieser Regeln ist, dass **Kinder in den ErzierherInnen der Maison Relais Ansprechpartner bezüglich Fragen und Problemen sehen sollten und diese frei und ohne Angst vor Strafen äußern dürfen.**

Internetführerschein – ja oder nein?
Ein Internetführerschein kann ein tolles Mittel sein, wenn Kindern das klassische „Surfen“ bzw. Herumstöbern im Internet erlaubt werden soll. Zwei Online-Versionen dieser sogenannten „Surfscheine“ findet man auf der pädagogischen Plattform „internetabc.de“[15].

Diese können sowohl als lehrreiches Spiel genutzt oder als „Prüfung“ ähnlich eines kleinen Führerscheintests tatsächlich als Grundlage für die Erlaubnis des Surfens in der Maison Relais genommen werden. Hier ist abzuwägen, was in der eigenen täglichen Praxis pädagogisch sinnvoll und realistisch umsetzbar ist, da dies sehr von den individuellen Gegebenheiten der Einrichtung abhängt.

Die Durchführung des „kleinen Surfscheins“ dauert ca. 15-20 Minuten und ist eher für ältere Kinder zwischen 9-12 Jahren geeignet. Der große Surfschein kann zwischen 30-60 Minuten dauern und ist auch vom Schwierigkeitsgrad etwas höher als der kleine Surfschein.

Regeln für den Umgang mit Geräten
Des Weiteren ist es sinnvoll, für den guten Umgang mit den Geräten (Computer, Tablets etc.) hausintern Regeln aufzustellen, am besten unter aktiver Beteiligung der Kinder. Dies kann schon eine erste Aktivität sein[16].

[15] https://www.internet-abc.de/kinder/lernen-schule/surfschein/
[16] Zur Inspiration: www.mediennutzungsvertrag.de

× 5. AUF DEM LAUFENDEN BLEIBEN

GERADE IM BEREICH DER MEDIENPÄDAGOGIK IST ES WICHTIG, WIE ANFANGS ERWÄHNT STETS AUF DEM LAUFENDEN ZU BLEIBEN.

▸ Nützliche Quellen
Eine Liste mit nützlichen Webseiten/Portalen findet sich im Anhang. Auf der BEE SECURE Webseite[17] gibt es speziell für Luxemburg viele interessante Informationen und Tipps für ErzieherInnen, LehrerInnen und Eltern zu generellen und aktuellen Themen rund um Internetsicherheit, die relevant für die pädagogische Berufs-Praxis und auch die private Nutzung sind.

▸ Schulung und Fortbildung
Regelmäßige Schulungen, in welchen das Betreuungspersonal die Möglichkeit hat, das eigene Wissen über Internetsicherheit für Kinder und auch im Bezug auf die eigene Nutzung zu erweitern und sich mit Fachkollegen auszutauschen, sind sehr zu empfehlen. Auf der BEE SECURE Webseite gibt es die Möglichkeit, Schulungen über das Kontaktformular[18] anzufragen.

Auch sehr zu empfehlen sind medienpädagogische Fortbildungen, in denen konkrete (kreative) Aktivitäten rund um Internet und vernetzte Geräte für die eigene Praxis ausprobiert bzw. kennengelernt werden können (siehe Portale zur Fortbildung im Anhang).

[17] www.bee-secure.lu
[18] www.bee-secure.lu/form

DIE 10 GOLDENEN REGELN FÜR EINE SICHERE INTERNET-NUTZUNG FÜR KINDER

1 Im Internet bin ich freundlich, respektvoll und beleidige niemanden.

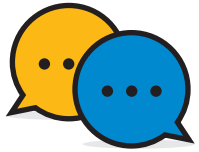
2 Ich verrate niemandem meine persönlichen Informationen. Meinen echten Namen, Adresse, Handynummer und Informationen über Freunde und Familie behalte ich für mich.

3 Ich verrate niemandem meine Passwörter- auch nicht meinen Freunden. Tipp: „Mein Passwort mach' ich mit 'nem Satz und hüte es wie einen Schatz!".

4 Wenn sich jemand aus dem Internet mit mir treffen möchte, gebe ich sofort meinen Betreuern und Eltern Bescheid.

5 Wenn jemand gemein zu mir oder zu anderen ist, gebe ich meinen Betreuern und Eltern Bescheid und hole Hilfe. Kostenlose und anonyme Hilfe und Beratung bekomme ich bei der BEE SECURE HELPLINE (8002-1234). Wenn ich um Hilfe frage, muss ich keine Angst vor Bestrafung haben.

6 Wenn ich unangenehme Nachrichten oder Bilder bekomme, gebe ich sofort meinen Betreuern und Eltern Bescheid. Ich brauche keine Angst davor zu haben und muss mich auch nicht dafür schämen. Wenn sowas passiert, dann ist es nicht meine Schuld.



7 Ich spreche regelmäßig mit meinen Betreuern und Eltern über das, was ich im Internet mache.

8 Fotos/Videos von anderen, darf ich nicht ohne Erlaubnis im Internet oder mit dem Smartphone/Tablet teilen oder weiterleiten.

9 Erst denken, dann klicken! Ich benutze das Internet und Geräte wie Smartphones, Computer, Tablets usw. mit Bedacht und für gute Zwecke.

10 Wenn ich von anderen Kindern oder Erwachsenen Fotos oder Videos machen möchte, muss ich diese vorher immer um Erlaubnis fragen. Umgekehrt müssen andere mich auch um Erlaubnis fragen. Wenn jemand zustimmt, mache ich keine peinlichen Aufnahmen.

ANHANG

Anlaufstellen

BEE SECURE:
▶ www.bee-secure.lu

Commission Nationale pour la Protection des Données (CNPD):
▶ www.cnpd.public.lu

BEE CREATIVE:
▶ www.bee-creative.lu

BEE SECURE HELPLINE: 8002 1234
▶ *Die BEE SECURE Helpline bietet Kindern, Jugendlichen, Eltern und Erziehern eine persönliche kostenlose Beratung und Orientierung in allen Fragen, die den Gebrauch der neuen Medien betreffen.*

Portale zur Weiterbildung für Erzieher

▶ www.bee-secure.lu/trainings
▶ www.enfancejeunesse.lu
▶ www.ifen.lu
▶ www.salto-youth.net

Praktische Links

Sicherheitskonzept für Jugendhäuser „Secure MJ“
▶ www.bee-secure.lu/secure-MJ

Whitelist mit kindgerechten Webseiten
▶ www.bee-secure.lu/beefilter

Leitfaden zur Informationssicherheit
▶ www.bee-secure.lu/leitfaden

Publikationen von BEE SECURE
▶ www.bee-secure.lu/publikationen

Kontaktformular für BEE SECURE Schulungen
▶ www.bee-secure.lu/form

Hilfreiche Tipps zum Kauf von „smart toys“ und Informationen über die Risiken
▶ www.bee-secure.lu/factsheet/smart toys

Ratgeber der CNPD zu Datenschutz für Vereine – auch hilfreich für die Maisons Relais
▶ www.cnpd.public.lu/fr/actualites/national/2018/06/guidance-associations.html

Technische Beschreibung des „BEE Filters“ auf github
▶ www.github.com/msilvoso/beefilter

Beispiel für kostenfreie Blacklist
▶ www.shallalist.de

Workshop-Angebote im Makerspace “Base1” von BEE CREATIVE, die sich auch an Kindergruppen aus den Maisons Relais richten
▶ www.base1.lu/workshops

Internetführerschein (DE)
▶ www.internet-abc.de/kinder/lernen-schule/surfschein

Spiele selber programmieren für Kinder (mehrsprachig):
▶ www.scratch.mit.edu

Regeln für den Umgang mit Geräten
▶ www.mediennutzungsvertrag.de

Notes

Notes

www.bee-secure.lu