



KlickITSafe



Syllabus Version 1.0

Copyright © 2010 Dienstleistungsgesellschaft für Informatik (DLGI) und dem Projekt Klicksafe.de

DLGI Dienstleistungsgesellschaft für
Informatik mbH
Am Bonner Bogen 6
53227 Bonn
E-Mail: info@dlgi.de
Web: www.dlgi.de

Klicksafe.de
c/o Landeszentrale für Medien und
Kommunikation (LMK) Rheinland-Pfalz
Turmstraße 10
67059 Ludwigshafen
E-Mail: info@klicksafe.de
Web: www.klicksafe.de

Übersicht

| | |
|---|----|
| Konzept IT-Sicherheitszertifikat | 2 |
| 1. Umgang mit Informationen aus dem Netz..... | 4 |
| 2. Kommunikationsmöglichkeiten und Onlinespiele im Netz | 5 |
| 3. Selbstdarstellung im Web 2.0..... | 7 |
| 4. Recht und Gesetz im Internet..... | 9 |
| 5. Unerwünschtes aus dem Netz | 10 |
| 6. Schutzmaßnahmen und Sicherheitseinstellungen..... | 11 |
| 7. Sicheres Surfen..... | 13 |

Konzept IT-Sicherheitszertifikat „KlickITSafe“

Die Nutzung von Medien gehört heute bei Kindern und Jugendlichen zum Alltag. Computer, Internet, Handy, Spielekonsolen, Suchmaschinen – die Medienumwelt von Heranwachsenden hat sich in den letzten Jahren rasant verändert.

Das Leben in der digitalen Welt stellt vor allem die Bereiche Bildung und Erziehung vor neue Aufgaben. Insbesondere der Schule kommt hier eine Schlüsselrolle zu. Hier können und sollten frühzeitig die Grundlagen für einen kompetenten Umgang mit den Neuen Medien gelegt werden. Je früher ein reflektierender Umgang mit dem Internet eingeübt wird, Chancen und Risiken erkannt werden, desto nachhaltiger kann sich Medienkompetenz aufbauen.

Mit einem IT-Sicherheits-Zertifikat kann der Lernende die notwendige Kompetenz nachweisen und für die weitere schulische und private Mediennutzung eine solide Grundlage schaffen.

Zielsetzung:

Der IT-Sicherheitstest prüft, ob Schülerinnen und Schüler über die Kenntnisse und Fertigkeiten verfügen, um den Computer, das Internet und andere Medien kompetent und sicher zu nutzen.

Die zu prüfenden Inhalte basieren auf dem Lehrerhandbuch von Klicksafe.

Umsetzung:

Der Tests wird mit einem Online-Prüfungssystem abgenommen. Der Test ist inhaltsvalide bezogen auf den Lehrplan (Syllabus) und liefert dem Teilnehmenden eine verlässliche Aussage über seine Kenntnisse im Bereich der kompetenten und sicheren Mediennutzung.

Der Test hat 32 Fragen und ist innerhalb von 35 Min zu absolvieren. Wurden mindestens 75 % Fragen richtig beantwortet, ist der Test bestanden.

Bei den Tests handelt es sich um eine repräsentative Auswahl aus allen Inhaltsbereichen des Lehrplans. Paralleltests und Fragenpools pro Inhaltsbereich stellen sicher, dass häufig wechselnde Fragen gestellt werden.

Zielgruppe:

Kernzielgruppe sind Schülerinnen und Schüler der 7. – 10. Klassen, aller Schulformen. Auch für Schülerinnen und Schüler der Sek. II und der beruflichen Schulen ist das Zertifikat geeignet.

Pädagogisches Konzept:

Der Test fragt praxisorientiert die für eine sichere und kompetente Nutzung von Medien erforderlichen Kenntnisse ab. Schwerpunkt des Tests ist die Abfrage von Medienkompetenz anhand praxisorientierter Fragestellungen.

Aspekte der IT-Sicherheit im engeren Sinne (technische Sicherheit) kommen ergänzend hinzu.

Zertifikat

Das Zertifikat KlickITSafe wird von der DLGI als der zertifizierenden Stelle ausgestellt, sobald der Test erfolgreich absolviert wurde. Wie bei den ECDL-Tests kann der Test nur unter Aufsicht bei einer autorisierten Stelle abgenommen werden.

Themenschwerpunkte:

Folgende Themenschwerpunkte, die im Klicksafe Leitfaden für Lehrkräfte veröffentlicht sind, liegen dem Lehrplans (Syllabus) zu Grunde.

1. Umgang mit Informationen aus dem Netz
2. Kommunikationsmöglichkeiten und Onlinespiele im Netz
3. Selbstdarstellung im Web 2.0
4. Recht und Gesetz im Internet
5. Unerwünschtes aus dem Netz
6. Schutzmaßnahmen und Sicherheitseinstellungen
7. Sicheres Surfen

1. Umgang mit Informationen aus dem Netz

| Kategorie | | Ref | Aufgabenbeschreibung |
|---|---|-------|--|
| 1. Umgang mit Informationen aus dem Netz | 1.1 Interpretation von Suchmaschinen-ergebnissen | 1.1.1 | Bei der Suche im Internet den Unterschied zwischen manuell erstellten Ergebnisseiten (Katalog) und automatisch erstellten Ergebnisseiten (Suchmaschine) kennen und benennen können. |
| | | 1.1.2 | Die Arbeitsweise von Suchmaschinen benennen und die Ergebnisse interpretieren können. Wissen, dass es „natürliche Links“, Werbung und Suchmaschinenspamming auf den Ergebnisseiten gibt. |
| | | 1.1.3 | Altersgerechte Alternativen zu Google kennen und benennen können. |
| | | 1.1.4 | Die drei häufigsten Suchstrategien anwenden können. („UND“ und „NICHT“ Verknüpfung sowie die Phrasensuche) |
| | | 1.1.5 | Die „12 goldenen Suchmaschinenregeln“ von klicksafe.de kennen und anwenden können. |
| | 1.2 Glaubwürdigkeit und Qualität von Internetseiten | 1.2.1 | Wissen, dass die Glaubwürdigkeit von Internetseiten überprüft werden sollte und dies benennen können. |
| | | 1.2.2 | Kriterien benennen, mit deren Hilfe die Glaubwürdigkeit von Internetseiten beurteilt werden kann. |
| | 1.3 Werbung | 1.3.1 | Erklären können, warum Werbung als häufig genutzte Finanzierungsform von Internetseiten genutzt wird. |
| | | 1.3.2 | Den Unterschied zwischen redaktionellem Inhalt und Werbung erkennen und benennen können. |
| | | 1.3.3 | Verschiedene Werbeformate im Internet, wie z.B. Produkt- und Marketingwebsites, Werbebanner, Sponsoring, Pop-Ups und Online-Gewinnspiele unterscheiden und bestimmen können. |

2. Kommunikationsmöglichkeiten und Onlinespiele im Netz

| Kategorie | | Ref | Aufgabenbeschreibung |
|--|------------------------|---|--|
| 2. Kommunikationsmöglichkeiten und Onlinespiele im Netz | 2.1 Chatten | 2.1.1 | Erklären können, worin bei vielen der Reiz des Chatten liegt, wie z.B. kostenlos, schnell, direkte Kommunikation, Anonymität („In fremde Rollen schlüpfen können“) oder „hip“ sein. |
| | | 2.1.2 | Gefahren des Chattens kennen und benennen können, wie: Beleidigung und Beschimpfung, sexuelle Übergriffe / Belästigung, Frage nach Videoübertragung, Konfrontation von Kindern mit sex. Äußerungen und pornografischen Bildern, Kontaktaufnahme von Pädophilen |
| | | 2.1.3 | Regeln für sicheres Chatten kennen und anwenden können. |
| | 2.2 ICQ, Skype und Co. | 2.2.1 | Vorteile von ICQ nachvollziehen und benennen können, wie z.B. kostenlose, bzw. kostengünstige Kommunikation, gleichzeitige Übertragung von digitalen Daten. |
| | | 2.2.2 | Die Risiken von Instant Messaging kennen und benennen können, wie z.B. Übermittlung von pers. Daten (Profil), Bullying, Werbung. |
| | | 2.2.3 | Tipps zum sicheren Umgang mit ICQ und Skype kennen und anwenden können. |
| | 2.3 Handy und Internet | 2.3.1 | Möglichkeiten des Handys als mobiles Endgerät mit Inhalten aus dem Internet kennen und benennen können, wie z.B. Spiele, Musik, Fotos, Filme, im Internet surfen. |
| | | 2.3.2 | Risiken und Probleme im Umgang mit dem Handy nachvollziehen und benennen können, wie: Inhalte aus dem Web, Tauschen von Bildern und Videos. |
| | | 2.3.3 | Tipps zum sicheren Umgang mit Inhalten aus dem Internet auf dem Handy anwenden können (Sicherheitseinstellungen am Handy kennen). |
| | | 2.3.4 | Die Problematik von Mobbing und Happy Slapping kennen und sie soziologischen Probleme nachvollziehen können. |
| 2.3.5 | | Rechtliche Grundlagen und Konsequenzen kennen und benennen können. (vgl. Broschüre „Gewalt auf dem Handy“, klicksafe.de) | |

| | | | |
|--|--------------------|-------|--|
| | 2.4 Computerspiele | 2.4.1 | Risiken und Probleme durch übermäßiges Spielen von Computerspielen abschätzen und benennen können, wie z.B. Gewaltproblematik, Sucht, „Abdriften“ in die virtuelle Welt. |
| | | 2.4.2 | Die altersgerechte Einstufung von Computerspielen nach der USK kennen und Gründe (Entwicklungsbeeinträchtigung) dafür nachvollziehen. |
| | | 2.4.3 | Verantwortungsvollen Umgang mit Computerspielen kennen und nachvollziehen können. |
| | | 2.4.4 | Das Konzept von webbasierten Rollenspielen (MMORPGs) verstehen und die Faszination beschreiben können. |
| | | 2.4.5 | Risiken und Gefahren von MMORPGs abschätzen und beurteilen können. (Abhängigkeit, sozialer Druck, Schlafmangel etc.) |
| | | 2.4.6 | Richtigen Umgang mit MMORPGs verinnerlichen und benennen können. |

3. Selbstdarstellung im Web 2.0

| Kategorie | | Ref | Aufgabenbeschreibung |
|--|-------------------------------|-------|--|
| 3. Selbstdarstellung im Web 2.0 | 3.1 Web 2.0 | 3.1.1 | Das Prinzip von Web 2.0 Angeboten nachvollziehen und einige Angebote ihrer Funktion zuordnen können. |
| | | 3.1.2 | Positive Aspekte der Web 2.0 Nutzung nutzen und benennen können. |
| | | 3.1.3 | Persönlichkeitsrechte formulieren und diese anhand von konkreten Beispielen auf Web 2.0 Angebote übertragen können. |
| | 3.2 Communities | 3.2.1 | Das Prinzip von Social Communities formulieren können und einige Beispiele benennen können. |
| | | 3.2.2 | Einige positive und negative Aspekte von Social Communities darstellen können. (Vernetzung) |
| | | 3.2.3 | Das Phänomen der „Selbstaktualisierung“ kennen und bewerten können. |
| | 3.3 Selbstdarstellung im Netz | 3.3.1 | Das Phänomen der Selbstdarstellung im Netz kennen und anhand von Beispielen einordnen können. |
| | | 3.3.2 | Nachvollziehen und wiedergeben können, worin für viele der Reiz liegt, im Netz private Informationen Preis zu geben. |
| | | 3.3.3 | Vor- und Nachteile der Selbstdarstellung kennen und vergleichen können. |
| | | 3.3.4 | Mobbing im Zusammenhang mit social Communitys einordnen können. |
| | | 3.3.5 | Den Begriff „Informationelle Selbstbestimmung“ kennen und Maßnahmen treffen können diesen auf Web 2.0 Angebote / private Homepage übertragen können. |
| | 3.4 Videotauschbörsen | 3.4.1 | Das Grundprinzip von Videotauschbörsen wie youtube kennen und benennen können. |
| | | 3.4.2 | Die Konsequenzen (positive und negative) die eine Veröffentlichung von privatem Videomaterial mit sich bringt benennen und reflektieren können. |
| | | 3.4.3 | Rechtliche Konsequenzen kennen, wenn beim Einstellen von Videos gegen Urheber- oder Persönlichkeitsrechte verstoßen wird. |

| | | | |
|--|--|-------|--|
| | | 3.4.4 | Den Begriff „Cyber-Bullying“ im Zusammenhang mit Videoportalen darstellen und beurteilen können. |
| | 3.5. Seiten zur Beurteilung von Personen | 3.5.1 | Das Grundprinzip von Seiten zur Beurteilung anderer Personen kennen und benennen können. |
| | | 3.5.2 | Auf die Probleme im Zusammenhang mit öffentlichen Bewertungen anderer Personen aufmerksam werden und sich mit diesen kritisch auseinandersetzen. |
| | | 3.5.3 | Kriterien eines Verhaltenskodex zum Thema „Internet-Mobbing“ kennen und im Internet anwenden können. |

4. Recht und Gesetz im Internet

| Kategorie | | Ref | Aufgabenbeschreibung |
|--|---------------------------------------|-------|--|
| 4. Recht und Gesetz im Internet | 4.1 Urheber- und Persönlichkeitsrecht | 4.1.1 | Relevante Aspekte aus dem Urheber- und Persönlichkeitsrecht kennen und benennen können. |
| | | 4.1.2 | Anhand von Fallbeispielen die Entscheidung darüber treffen können, ob eine Aktion gegen geltende Gesetze verstößt oder nicht. |
| | | 4.1.3 | In simulierten Fällen das eigene Handeln im Web 2.0 reflektieren und eine Entscheidung entsprechend der Gesetzeslage treffen können. |
| | 4.2 Jugendgefährdende Inhalte | 4.2.1 | Das deutsche Jugendschutzgesetz in seinen wichtigsten Punkten kennen und benennen können. |
| | | 4.2.2 | Erklären können, warum bestimmte Inhalte unter das Jugendschutzgesetz fallen. |
| | | 4.2.3 | Fähig sein, beim versehentlichen Aufrufen von jugendgefährdenden Inhalten, entsprechend zu handeln und Aufsichtspersonen, bzw. Meldestellen hinzuzuziehen. |
| | | 4.2.4 | Die wichtigsten Aufsichtsbehörden fürs Internet kennen und ihre Aufgaben benennen können. |

5. Unerwünschtes aus dem Netz

| Kategorie | | Ref | Aufgabenbeschreibung |
|--|---|-------|---|
| 5. Unerwünschtes aus dem Netz: Spams, Malware und illegale Tauschbörsen | 5.1. Spam-Mails | 5.1.1 | Skizzieren können, was Spam Mails sind und Regeln für das Erstellen von sicheren Mail-Adressen kennen und benennen können. |
| | | 5.1.2 | Regeln für das Mailen kennen und diese begründen können. |
| | | 5.1.3 | Das wirtschaftliche Interesse, welches hinter Spam Mails steckt, reflektieren und benennen können. |
| | 5.2 Viren, Würmer, Trojaner, Spyware | 5.2.1 | Viren, Würmer, Trojaner und Spyware als Malware kennen und benennen können. |
| | | 5.2.2 | Nachvollziehen können, warum ein technischer Schutz des Computers wichtig ist und entsprechende Einstellungen vornehmen können. |
| | | 5.2.3 | Antivirenprogramm, Benutzerprofil und Firewall als wichtige Instrumente zum Schutz vor Malware kennen und benennen können. |
| | 5.3 Illegale Downloads und Tauschbörsen (Schwerpunkt Musik) | 5.3.1 | Probleme im Zusammenhang mit illegalen Downloads kennen und benennen können. |
| | | 5.3.2 | Kriterien kennen und benennen können, wie man legale und illegale Downloads unterscheiden kann. |
| | | 5.3.3 | Sich der Konsequenzen von illegalen Downloads bewusst sein und diese benennen können. |

6. Schutzmaßnahmen und Sicherheitseinstellungen

| Kategorie | | Ref | Aufgabenbeschreibung |
|--|-------------------------------|-------|---|
| 6. Schutzmaßnahmen und Sicherheitseinstellungen | 6.1 Passwörter | 6.1.1 | Die Notwendigkeit von sicheren Passwörtern kennen und benennen können. |
| | | 6.1.2 | Ein System kennen und anwenden können, wie sichere Passwörter gebildet werden können. |
| | | 6.1.3 | Einstellungen vornehmen können, dass private Daten nicht im Browser gespeichert werden. |
| | 6.2 Kritisches Surfverhalten | 6.2.1 | Sich darüber bewusst werden, dass im Internet häufig persönliche Daten abgefragt werden und verschiedene Gründe dafür kennen und benennen können. |
| | | 6.2.2 | Das Prinzip der informationellen Selbstbestimmung kennen und benennen können. |
| | | 6.2.3 | Gründe kennen und benennen können, warum der Umgang mit persönlichen Daten im Internet bewusst gesteuert werden sollte. |
| | 6.3 Browser und Internet-Café | 6.3.1 | Sich darüber im Klaren sein, dass der Browser persönliche Daten speichert und diese benennen können. |
| | | 6.3.2 | Die Bedeutung von Verlauf, Cookies, Passwörtern und Cache im Zusammenhang mit den Browser kennen und benennen können. |
| | | 6.3.3 | Einstellungen im Browser ändern und gespeicherte Daten löschen können. |
| | 6.4 W-LAN | 6.4.1 | Vor- und Nachteile von Funknetzwerken kennen und benennen können. |
| | | 6.4.2 | Sicherheitsrisiken eines unverschlüsselten Funknetzes kennen und benennen können. |
| | | 6.4.3 | Techniken kennen und benennen können, mit denen ein Funknetzwerk verschlüsselt werden kann. |
| | 6.5 Datensicherung | 6.5.1 | Sich der Problematik bewusst sein, dass digitale Daten einem hohen Verlustrisiko (Haltbarkeit) ausgesetzt sind und dies benennen können. |
| | | 6.5.2 | Vorbeugende Maßnahmen zur Datensicherheit kennen und benennen können. |

| | | | |
|--|--|-------|--|
| | | 6.5.3 | Möglichkeiten des versehentlichen Datenverlustes und des gewünschten Datenlöschens kennen und benennen können. |
|--|--|-------|--|

7. Sicheres Surfen

| Kategorie | | Ref | Aufgabenbeschreibung |
|---------------------------|-------------------------------|-------|--|
| 7. Sicheres Surfen | 7.1 Tipps zum sicheren Surfen | 7.1.1 | Sich bewusst machen, dass beim Surfen im Netz Gefahren drohen und dies benennen können. |
| | | 7.1.2 | Verschiedene Tipps zum sicheren und verantwortungsvollem Surfen kennen und benennen können. |
| | 7.2 In der Schule | 7.2.1 | Sich darüber im Klaren sein, dass das Surfen in der Schule besonderen Bedingungen unterliegt und dies benennen können. |
| | | 7.2.2 | Verantwortlichkeit der Lehrkraft kennen und nachvollziehen, sowie benennen können. Wissen was zur Aufsichtspflicht der Lehrkraft gehört. |
| | | 7.2.3 | Pädagogische Maßnahmen zum sicheren Surfen an der Schule kennen und benennen können, sowie diese Maßnahmen mit tragen können. |