German School Association Ltd · Douglas House · Petersham Road · Richmond · TW10 7AH · Großbritannien

RICHTLINIE ZU E-SAFETY

Titel	SR03 – Richtlinie zu E-Safety
Version	1.6 / August 2019
Erstellt von	Schulleitung
Gültig für	Schüler, Eltern, Mitarbeiter, dritte Parteien
Nächste Überarbeitung	August 2022 oder früher, sofern erforderlich

1. Zweck und Anwendungsbereich

Wir sind der Meinung, dass Kinder in der Lage sein sollten, das Internet und digitale Medien für Bildungszwecke und die persönliche Weiterentwicklung zu nutzen, wobei jedoch Zugriffsbeschränkungen erforderlich sind, um eine sichere Verwendung zu ermöglichen.

Wir wissen, dass der Lernprozess durch den Einsatz von Technologien, darunter auch das Internet und die Online-Kommunikation, verbessert werden kann, und Kinder von sozialen und bildungsbezogenen Vorteilen profitieren können. Neue Technologien beinhalten auch Risiken, die gemäß den gesetzlichen Richtlinien „Statutory Guidance Keeping Children Safe in Education 2018“ in folgende Kategorien fallen:

- Online-Inhalte – Vorhandensein gesetzeswidriger, unangemessener oder gefährlicher Inhalte, wie Pornographie, gefälschte Nachrichten (Fake News), rassistische, radikale oder extremistische Ansichten
- Online-Kontakt – Gefährliche Online-Interaktion mit anderen Benutzern, wobei sich beispielsweise Erwachsene als Kinder oder junge Erwachsene ausgeben
- Online-Verhalten – Persönliches Online-Verhalten, das zu schädlichen Verhaltensweisen führt, beispielsweise Erstellung, Versendung und Erhalt expliziter Bilder oder Cyber-Mobbing

Mit diesen Richtlinien soll Folgendes sichergestellt werden:

- dass die Schulgemeinschaft der Deutschen Schule über angemessene Verhaltensweisen informiert ist, die einzuhalten sind, um Schüler vor diesen Risiken zu schützen;
- dass die Sicherheit und das Wohlbefinden der Schüler beim Einsatz von ICT (Informations- und Kommunikationstechnologie) von höchster Wichtigkeit ist;
- dass die Schule beim Einsatz von ICT stets die Werte und Vorgaben der Schule einhält.

Wir sind dazu verpflichtet, sicherzustellen, dass alle Schüler vor möglichen Online-Gefahren geschützt werden und dass alle Kinder, unabhängig von Alter, Behinderungen, Geschlecht, Rasse, Religion oder Überzeugungen oder sexueller Ausrichtung, das Recht haben, vor sämtlichen Arten von Gefahren oder Missbrauch geschützt zu werden.

Diese Richtlinie gilt für alle Mitglieder der Schulgemeinschaft, darunter Schüler, Eltern/Betreuer, Besucher und Mitarbeiter, die Zugriff auf die ICT-Systeme der Schule haben und diese verwenden, inklusive von Fest- als auch mobile Geräte (PCs, Laptops, Mobiltelefone, Webcams, Tablets, digitale Whiteboards und Video-/Videokonferenz-Systeme), die sich entweder im Besitz der Schule befinden oder auf das Schulgelände mitgebracht werden. Sie gilt auch für den Einsatz von Technologie außerhalb des Schulgeländes, sofern sich dieser Einsatz auf das Wohlergehen der Schüler auswirkt, dem Ethos der Schule widerspricht oder den guten Ruf der Schule gefährdet.

Im Rahmen dieser Richtlinie bedeutet „Mitarbeiter“ alle Mitarbeiter der Schule, Angestellte oder ehrenamtliche Helfer sowie externe Dienstleister.

2. Mit dieser Richtlinie zusammenhängende Richtlinien

Diese Richtlinie wird durch weitere Richtlinien und Verfahren der Schule ergänzt, darunter Folgende:

Richtlinie zum Schutz von Kindern (Safeguarding Children and Child Protection Policy)
Anti-Mobbing-Richtlinie (Anti-Bullying Policy)
Richtlinie zu Verhalten und Disziplin (Behaviour and Discipline Policy)
Verhaltenskodex für Mitarbeiter (Staff Code of Conduct)
Richtlinie für Mitarbeiter zur Verwendung von sozialen Medien (Staff Social Media Policy)
Datenschutzrichtlinie (Data Protection Policy)

Verstöße gegen diese Richtlinie werden gemäß den Verfahrensweisen, die in den obigen Richtlinien festgelegt sind, geahndet.

3. Technologien

Diese Richtlinie gilt für den Einsatz von ICT (Informations- und Kommunikationstechnologie), einschließlich, jedoch nicht beschränkt auf den Einsatz von Computern, Mobiltelefonen, Tablets oder anderen elektronischen Geräten und Systemen zur Erfassung, Speicherung, Verwendung und Übermittlung von Daten auf elektronischem Weg, wie E-Mails und webbasierte, mobile Technologien, die die Kommunikation zu einem aktiven Dialog machen („soziale Medien“), z. B. Blogs, Wikis, virtuelle Lernressourcen, Social-Networking-Websites, Podcasts, Foren, Message Boards oder Kommentare zu Online-Artikeln.

Die Schule verwendet verschiedene Geräte, darunter PCs, Laptops, Tablets usw. Um die Schüler zu schützen und den Verlust personenbezogener Daten zu vermeiden, nutzen wir technische Hilfsmittel, wie Software für das Internet Filtering, um den unbefugten Zugriff auf gesetzeswidrige und unangemessene Websites zu verhindern, sowie Software für E-Mail Filtering, um zu verhindern, dass infizierte E-Mails von der Schule versendet werden oder in das Netzwerk der Schule gelangen.

4. Aufgaben/Funktionen und Verantwortlichkeiten

Die Schule hat den IT-Manager als E-Safety-Beauftragten ernannt, der die verschiedenen Verfahren zur Online-Sicherheit koordiniert. Um diese Aufgabe zu erfüllen, arbeitet der E-Safety-Beauftragte eng mit dem Kinderschutz-Beauftragten der Schule zusammen sowie mit einem Team, das aus verschiedenen Lehrkräften besteht, um die Kommunikation sicherzustellen und erforderliche Schulungen anzubieten.

Die IT-Abteilung der Schule ist unter anderem dafür verantwortlich, eine sichere ICT-Infrastruktur bereitzustellen und über technische Fortschritte auf dem Laufenden zu bleiben.

Mitarbeiter werden hinsichtlich ICT, Inhalten und Anwendung dieser Richtlinie entsprechend geschult.

Schüler und Mitarbeiter sind für ihr Online-Verhalten beim Einsatz von ICT genauso verantwortlich wie auch in Situationen, in denen ICT nicht zum Einsatz kommt. Ihre Verwendung von Technologie

hat in Übereinstimmung mit allen, mit dieser Richtlinie zusammenhängenden Vorschriften zu erfolgen.

Wir sind davon überzeugt, dass wir mit den Eltern/Erziehungsberechtigten unserer Schüler zusammenarbeiten müssen, um das Wohlbefinden der Kinder zu fördern und sie dabei zu unterstützen, ICT auf verantwortungsvolle Weise zu verwenden und das Internet sicher zu nutzen. Diese Richtlinie wird Eltern/Betreuern auf der Website der Schule zur Verfügung gestellt. Bei Elternabenden erhalten Eltern/Betreuer von Zeit zu Zeit ebenfalls Tipps zu E-Safety.

Mitarbeiter sind dafür verantwortlich, E-Safety-Vorfälle dem Kinderschutz-Beauftragten zu melden und dazu das in Anhang 1 enthaltene Formular auszufüllen.

In Fällen, in denen das Kind stark gefährdet wurde oder das Risiko besteht, dass das Kind stark gefährdet wird, wird die Richtlinie zum Schutz von Kindern (Safeguarding and Child Protection Policy) der Schule zu Rate gezogen.

5. Regeln für E-Mail-Nachrichten

Die Kommunikation mit allen Personen, die am Schulleben beteiligt sind, sollte offen und respektvoll sein. Dies gilt für alle Arten der Kommunikation, insbesondere für E-Mail-Nachrichten. Zuerst sollten Inhalte und Probleme mit den Personen besprochen werden, die direkt daran beteiligt sind.

E-Mails dienen dem Informationsaustausch. E-Mails sollen nicht als Mittel für Diskussionen, Beschwerden oder Konfliktlösung verwendet werden. Der Ton in E-Mails soll respektvoll und neutral sein. E-Mails sollen präzise, deutlich und höflich formuliert sein. Die Mitarbeiter der DSL beantworten E-Mails während der Arbeitszeit innerhalb einer angemessenen Zeitspanne. Auskünfte zu den schulischen Leistungen von Schülern werden nicht per E-Mail versendet.
Ausnahmen von dieser Regel sind durch die Schulleitung zu genehmigen.

Wenn versendete oder erhaltene Inhalte als unangemessen angesehen werden und nicht unseren Regeln zum gegenseitigen, respektvollen Umgang entsprechen, werden diese Inhalte an das Team weitergeleitet, das für den Verhaltenskodex zuständig ist (Code of Conduct Team).

6. E-Safety-Informationen für Schüler

E-Safety wird während des ICT-Unterrichts auf altersgerechte Weise unterrichtet. E-Safety ist Bestandteil des Lehrplans, wobei wir uns nach der KMK von Baden Württemberg richten, da ICT in den meisten Unterrichtseinheiten verwendet wird. Daher bindet die Schule Informationen zur Sicherheit im Internet in den gesamten Lehrplan ein. Alle Lernprozesse werden durch E-Safety-Informationen ergänzt, was für alle Unterrichtsfächer und alle Veranstaltungen in der Aula gilt.

Während des Unterrichts stellen wir sicher, dass alle Schüler der Grundschule und der Sekundarstufe mit den Vorgaben der Schule zu akzeptablem Online-Verhalten vertraut sind und diese auch wirklich verstehen (wie nachstehend aufgeführt).

7. Schüler mit sonderpädagogischen Bedürfnissen und Behinderungen (Special Educational Needs and Disabilities, SEND)

Schüler mit sonderpädagogischen Bedürfnissen und Behinderungen (SEND), insbesondere Schüler, die Schwierigkeiten mit der Kommunikation und Interaktion haben, sind besonders anfällig für Online-Gefahren.

Wir passen unsere oben genannten Unterrichtsmethoden entsprechend an, um dieses Risiko zu minimieren.

8. Einsatz von Technologie

In Übereinstimmung mit unseren Grundsätzen erfolgt die Kommunikation innerhalb der Schulgemeinschaft sowie online respektvoll und offen.

Straftaten, wie Hacking, Diebstahl von Kennwörtern, Kopieren von Software dritter Anbieter ohne Lizenz, können strafrechtlich verfolgt werden, wobei die Schule niemanden vor der Strafverfolgung schützen kann.

Wenn E-Mail-Konten für Schüler eingerichtet werden, liegt der Hauptzweck darin, dass sie mit anderen Schülern und Mitarbeitern der Schule kommunizieren können; der Internetzugang wird bereitgestellt, um den Lernprozess der Schüler zu unterstützen.

Kindergarten- und Vorschulkinder haben keinen unüberwachten Zugriff auf ICT/Online-Ressourcen.

Die Klassenlehrer und Eltern/Betreuer von Grundschülern müssen sicherstellen, dass die Schüler folgende Regeln verstehen und einhalten, basierend auf den NSPCC-Richtlinien:

1. ICT ist in der Schule ausschließlich für schulische Zwecke zu verwenden.
2. Es dürfen nur E-Mail-Anhänge von Absendern geöffnet werden, die die Schüler kennen oder die von den Lehrern genehmigt wurden.
3. Schüler dürfen anderen Personen nicht ihre Kennwörter für ihr E-Mail-Konto oder ICT-Systeme weitergeben.
4. Schüler dürfen nur eigene Daten öffnen/löschen.
5. Schüler müssen sicherstellen, dass ICT zur Kommunikation mit anderen Schülern und Erwachsenen auf eine höfliche und vernünftige Weise erfolgt.
6. Schüler dürfen Inhalte, die ihrer Meinung nach bedrohlich, beleidigend, illegal sind oder eine Form von Mobbing darstellen, nicht an andere weiterleiten.
7. Schüler dürfen weder nach Inhalten suchen, noch Inhalte speichern oder versenden, wenn diese absichtlich böse gemeint oder unangenehm sind.
8. Schüler müssen ihre Lehrer sofort darüber informieren, wenn sie Inhalte sehen, die unangenehm oder gemein sind.
9. Schüler dürfen persönliche Angaben, wie Name, Telefonnummer oder Adresse, nicht online weitergeben.
10. Schüler dürfen keine Treffen mit anderen Personen vereinbaren, sofern dies nicht im Rahmen eines Schulprojekts erfolgt, das von ihrem Lehrer genehmigt wurde, und bei dem sie von einem verantwortungsbewussten Erwachsenen, den sie kennen, begleitet werden.

11. Schüler sind beim Einsatz von ICT für ihr eigenes Verhalten verantwortlich, da sie wissen, dass die obigen Regeln dafür sorgen, dass sie das Internet sicher verwenden können.
12. Schüler müssen unseren Ansatz zur Sicherheit im Internet unterstützen und dürfen nicht Bilder, Videos, Geräusche oder Texte hochladen oder hinzufügen, die eine andere Person der Schulgemeinschaft absichtlich verletzen könnten.
13. Die Nutzung von ICT durch Schüler wird überprüft und ihre Eltern/Betreuer werden informiert, wenn ein Mitarbeiter der Schule sich Sorgen über die Sicherheit des Schülers macht.
14. Schüler dürfen die IT-Ausrüstung weder beschädigen noch ändern, indem sie beispielsweise die Einstellungen für den Bildschirm ändern und Tasten von der Tastatur entfernen.

Die Klassenlehrer und Eltern/Betreuer von Schülern der Sekundarstufe müssen sicherstellen, dass die Schüler Folgendes verstehen und einhalten, basierend auf den NSPCC-Richtlinien:

1. Schüler dürfen ICT-Systeme in der Schule, darunter Internet, E-Mails, digitale Videos, mobile Technologien usw., nur für schulische Zwecke nutzen.
2. Schüler dürfen persönliche ICT-Ausrüstung nur nutzen, die für den Einsatz in den Systemen der Schule autorisiert wurde.
3. Es ist Schülern untersagt, Software auf die Systeme der Schule herunterzuladen oder zu installieren.
4. Schüler sind dazu verpflichtet, die ICT-Ausrüstung der Schule vor missbräuchlicher Verwendung oder Verstößen gegen den Datenschutz und vor Übergriffen zu schützen und dafür zu sorgen, dass die Geräte nicht beschädigt oder gestohlen werden. Sie müssen Kennwörter verwenden und sich nach der Verwendung immer abmelden.
5. Schüler dürfen sich nur mit dem Benutzernamen und Kennwort, das die Schule ihnen ausgestellt hat, im Netzwerk der Schule/auf der Lernplattform anmelden und dürfen nicht andere Internetquellen verwenden, wie 4G, da dies ein Sicherheitsrisiko für das Schulnetzwerk darstellt.
6. Schüler sind an die Sicherheitsvorgaben des ICT-Systems gebunden und dürfen ihre Kennwörter nicht anderen gegenüber offenlegen; Kennwörter sind regelmäßig zu ändern.
7. Wenn Schüler eine eigene Klassen- oder Schul-E-Mail-Adresse erhalten, dürfen sie ausschließlich diese Adresse für die E-Mail-Kommunikation verwenden.
8. Schüler müssen sicherstellen, dass die gesamte ICT-Kommunikation mit Schülern, Lehrern und anderen Personen auf verantwortungsvolle und vernünftige Weise erfolgt.
9. Schüler müssen verstehen, dass sie selbst für ihr Verhalten verantwortlich sind, wenn sie das Internet benutzen, dazu gehören auch Ressourcen, auf die sie zugreifen, und die Sprache, die sie in der Online-Kommunikation nutzen. Schüler dürfen nicht wissentlich Inhalte aufrufen, herunterladen, hochladen oder weiterleiten, die als beleidigend oder illegal angesehen werden könnten. Wenn sie versehentlich auf solche Inhalte stoßen, müssen sie sofort ihren Lehrer darüber informieren.
11. Schüler dürfen persönliche Angaben, wie Name, Telefonnummer oder Adresse, nicht online weitergeben.

12. Sie dürfen keine Treffen mit anderen Personen vereinbaren, sofern dies nicht im Rahmen eines Schulprojekts geschieht, das von ihrem Lehrer genehmigt wurde.
13. Schüler müssen wissen, dass Bilder von Schülern und/oder Mitarbeitern der Schule nur für schulische Zwecke erstellt, gespeichert und genutzt werden dürfen, wobei die Vorgaben der Schule einzuhalten sind; diese Bilder dürfen außerhalb des Schulnetzwerks ohne die Genehmigung der Schulleitung nicht weitergeleitet werden.
14. Schüler müssen sicherstellen, dass ihre Online-Aktivitäten, darunter auch die Verwendung von sozialen Medien, sowohl innerhalb als auch außerhalb der Schule nicht zu Problemen für die Schule, die Mitarbeiter, für Schüler oder andere Personen führt oder ihrem guten Ruf schädigt.
15. Schüler müssen unseren Ansatz zur Sicherheit im Internet unterstützen und dürfen nicht absichtlich Bilder, Videos, Geräusche oder Texte hochladen oder hinzufügen, die eine andere Person der Schulgemeinschaft verletzen oder beleidigen könnten.
16. Schüler haben die Privatsphäre und das Eigentum der Online-Arbeit anderer jederzeit zu respektieren.
17. Schüler dürfen nicht versuchen, das Internet Filtering System zu umgehen oder VPNs zu nutzen, die nicht von der Schule/dem ITC-Verantwortlichen autorisiert wurden.
18. Schüler müssen wissen, dass ihre Internet- und ICT-Nutzung überwacht und protokolliert werden kann und dass ihre Lehrer darauf zugreifen können.
19. Schüler müssen verstehen, dass diese Regeln zur sicheren Nutzung des Internets dienen und dass die Schule bei Verstößen gemäß der Richtlinie zu Verhalten und Disziplin (Behaviour and Discipline Policy) entsprechende Schritte einleitet und Eltern/Betreuer kontaktiert.
20. Schüler dürfen die IT-Ausrüstung weder beschädigen noch ändern, indem sie beispielsweise die Einstellungen für den Bildschirm ändern und Tasten von der Tastatur entfernen.

9. Cyber-Mobbing

Bei Cyber-Mobbing handelt es sich um Verhalten, das von einer Einzelperson oder einer Gruppe ausgeht, das über einen längeren Zeitraum wiederholt auftritt und eine andere Einzelperson bzw. eine Gruppe absichtlich verletzt, entweder körperlich oder emotional, und mithilfe des Einsatzes von ICT stattfindet, beispielsweise über E-Mail, Textnachrichten, soziale Medien oder Online-Spiele; dabei werden mitunter auch Bilder, Videos und Sexting eingesetzt, also „von Jugendlichen erstellte SMS-Nachrichten mit sexuellen Inhalten“.

Cyber-Mobbing kann zu jeder Tageszeit innerhalb oder außerhalb des Schulgeländes auftreten, wobei das Publikum potenziell sehr groß sein kann. Die Schule behält sich das Recht vor, Schritte gegen Fälle von Cyber-Mobbing einzuleiten, die außerhalb der Schule auftreten.

Fälle von Cyber-Mobbing fallen je nach Situation in den Geltungsbereich der Anti-Mobbing-Richtlinie der Schule (Anti-Bullying Policy), der Richtlinie zu Verhalten und Disziplin (Behaviour and Discipline Policy) und der Richtlinie zum Schutz von Kindern (Safeguarding and Child Protection Policy).

10. Kennwörter

Wenn eine Person von der Schule einen Benutzernamen/ein Kennwort erhält, um auf unser Netzwerk und unsere Ressourcen zuzugreifen, muss sie das Kennwort bei der ersten Anmeldung ändern; dabei muss das Kennwort mindestens sechs Zeichen umfassen, darunter Groß- und Kleinbuchstaben sowie Zahlen. Kennwörter dürfen nicht anderen Personen gegenüber offengelegt werden, nicht online gespeichert oder in E-Mails oder andere Arten der elektronischen Kommunikation integriert werden, wie Textnachrichten.

11. Überwachung

Die Schule verwendet Filtering-Software in ihrem Netzwerk, um alle Online-Aktivitäten zu überwachen, darunter auch altersgerechte Zugriffsbeschränkungen für Online-Inhalte. Der IT-Verantwortliche der Schule meldet dem Schutz-Beauftragten unangemessenes Online-Verhalten von Mitarbeitern oder Schülern bei Erkennung unverzüglich.

Wenn die Filtering-Software der Schule die Lernaktivitäten von Schülern versehentlich erschwert, beispielsweise Recherchen, sollten sich die Schüler an ihren Klassenlehrer wenden und um Hilfe bitten.

Durch den Einsatz von Filtering- und Überwachungssoftware stellt die Schule sicher, dass Schüler im Netzwerk der Schule nicht auf extremistische oder terroristische Inhalte zugreifen können.

Anhang I

Formular zur Meldung von E-Safety-Vorfällen

Ihre Angaben		
Ihr Name:	Ihre Position:	Datum und Uhrzeit des Vorfalls:
Details des E-Safety-Vorfalls		
Datum und Uhrzeit des Vorfalls:		
Wo hat der Vorfall stattgefunden? Beispielsweise in der Schule oder Zuhause:		
Wer war an dem Vorfall beteiligt? Kind/Jugendlicher ☐ Name des Kindes……. Mitarbeiter der Schule/Ehrenamtlicher Mitarbeiter ☐ Mitarbeiter der Schule/Ehrenamtlicher Mitarbeiter……. Andere Person ☐ bitte angeben…….		
Beschreibung des Vorfalls (einschließlich IP-Adressen, relevanter Benutzernamen, verwendeter Geräte und Programme)		
Ergriffene Maßnahmen: • Vorfall wurde dem Schutz-Beauftragten gemeldet • Sozialamt/Jugendamt wurden um Rat gebeten • Es wurde eine Überweisung an das Sozialamt/Jugendamt ausgestellt • Der Vorfall wurde der Polizei gemeldet • Der Vorfall wurde der Internet Watch Foundation gemeldet • Der Vorfall wurde dem IT-Beauftragten gemeldet • Zu ergreifende Disziplinarmaßnahmen • E-Safety-Richtlinie ist zu prüfen/zu ändern ☐Anderes (bitte angeben) ……..		
Ergebnis der Untersuchung		