

+43 1 531 20-0  
Minoritenplatz 5, 1010 Wien

Herrn  
Präsidenten des Nationalrates  
Dr. Walter Rosenkranz  
Parlament  
1017 Wien

Geschäftszahl: 2026-0.211.428

Die schriftliche parlamentarische Anfrage Nr. 5192/J-NR/2026 betreffend Sicheres Internet für Schüler, die die Abgeordneten zum Nationalrat Michael Fürtbauer, Kolleginnen und Kollegen am 6. März 2026 an mich richteten, darf ich anhand der mir vorliegenden Informationen wie folgt beantworten:

Zu Frage 1:

- *Über welche statistischen Befunde zu den Anteilen von Cybermobbing und sexueller Belästigung im Internet im schulischen Kontext verfügt das Ressort und auf welche Erhebungen stützen sich diese Daten?*

Das Bundesministerium für Bildung analysiert nationale und internationale Studien sowie thematische Erhebungen. Nationale Quellen sind insbesondere die Jugendstudien von Saferinternet.at sowie der Jugend-Internet-Monitor. Relevante Erkenntnisse werden auch aus dem aktuellen Durchgang der EU Kids Online-Studie erwartet, an dem Österreich teilnimmt.

Zu Frage 2:

- *In welchem Umfang werden Themen der Internetsicherheit von Lehrpersonen im Unterricht behandelt?*

In Volksschulen werden Schülerinnen und Schüler im Unterrichtsgegenstand Sachunterricht und über übergreifende Themen („Informatische Bildung“, „Medienbildung“) altersgemäß an die sichere und verantwortungsvolle Nutzung von Informationstechnologien herangeführt.

In Mittelschulen und der AHS-Unterstufe erfolgt die Auseinandersetzung mit Internetsicherheit vor allem im Pflichtgegenstand „Digitale Grundbildung“, in dem

grundlegende Datenschutzfragen ebenso behandelt werden wie Gefahren (z.B. Betrug im Internet oder Phishing). Über die oben genannten übergreifenden Themen erfolgt eine einschlägige Sensibilisierung zudem auch in anderen Unterrichtsgegenständen.

Auch in den Lehrplänen für den sonderpädagogischen Bereich sind die übergreifenden Themen „Informatische Bildung“ und „Medienbildung“ verankert.

In der AHS-Oberstufe werden grundlegende Aspekte der Internetsicherheit im Pflichtgegenstand sowie im Wahlpflichtgegenstand „Informatik“ sowohl explizit als auch implizit thematisiert. Die Schülerinnen und Schüler werden mit rechtlichen Grundlagen und Maßnahmen rund um Datensicherheit, Datenschutz und Urheberrecht vertraut gemacht. Insgesamt wird im Unterricht für Informatik nicht nur technisches Verständnis aufgebaut, sondern auch das Bewusstsein für die gesellschaftlichen und persönlichen Auswirkungen digitalen Handelns gestärkt – mit dem Ziel, den Schülerinnen und Schülern eine reflektierte und sichere Nutzung digitaler Technologien zu ermöglichen.

Wie in der Unterstufe ist Internetsicherheit auch in der Oberstufe in mehreren übergreifenden Themen (u.a. „Informatische Bildung“, „Medienbildung“) verankert und wird damit verbindlich fächerübergreifend behandelt.

In den künftigen Lehrplänen der AHS-Oberstufe wird die Behandlung von Internetsicherheit weiter gestärkt und systematisiert. Die neuen Pflichtgegenstände „Informatik und Künstliche Intelligenz“ und „Medien und Demokratie“ greifen Fragen der Internetsicherheit aus dem Blickwinkel der Informatik, der Medien- und der Demokratiebildung auf.

Im Bereich der berufsbildenden Schulen ist das Thema der Internetsicherheit bereits in hohem Ausmaß präsent, wobei es nicht nur in einem einzelnen Fach isoliert betrachtet, sondern als Querschnittsmaterie behandelt und in den didaktischen Grundsätzen und im allgemeinen Bildungsziel explizit ausgeführt wird. Das bedeutet, dass Absolventinnen und Absolventen berufsbildender Schulen moderne Informationstechnologien sicher und kompetent anwenden, gesetzliche Rahmenbedingungen und Datensicherheit berücksichtigen, Medien kritisch analysieren sowie Internetauftritte auf ihre rechtliche Konformität beurteilen können.

Darüber hinaus gibt es sowohl im Bereich der technisch-gewerblichen Lehranstalten als auch der Handelsakademien spezifische Schwerpunktsetzungen betreffend Cyber Security bzw. auch fachrichtungsspezifische Vertiefungen, beispielsweise im Lehrplan der HTL für Informatik, bei dem es insbesondere in den Bereichen Betriebssysteme, Datenbanken und Informationssysteme, Netzwerksysteme und verteilte Systeme sowie Sicherheit, IT-Recht und Gesellschaft um die gegenständliche Thematik geht. Ähnliches gilt für den kaufmännischen Bereich, wo unter anderem auf den rechtlichen Rahmen im Umgang mit elektronischen Medien sowie das Recht im Internet, E-Commerce, das Signaturgesetz,

Fernabsatzbestimmungen und Urheberrecht oder auf die Besonderheiten des Onlineverkaufs fokussiert wird.

Zu Frage 3:

- *Aus welchen dem Ressort vorliegenden Daten ergeben sich strukturelle, organisatorische oder ressourcenbezogene Faktoren für die sinkende Teilnahme an Fortbildungen zum Thema sicheres Internet?*

Die angesprochenen Daten stammen aus einer Recherche im Wege von PH Online. Erfasst wurden Lehrveranstaltungen zu den Themen sicheres Internet, digitale Medien sicher, Safer Internet, IT-Security, Cyber Mobbing/Bullying/Crime/Sicherheit, Gewalt im Netz/Hass im Netz, Internetbetrug/Fake News, Kinder- und Jugendschutz im Internet, Hacker(n), Datenschutz, Datensicherheit, DSGVO sowie Urheberrecht.

Der Empfehlung des Rechnungshofes wird insofern nachgekommen, als die Hintergründe für die rückläufige Entwicklung von 2019/20 bis 2023/24 mit allen Pädagogischen Hochschulen insbesondere im Burgenland und in Kärnten beleuchtet wurden.

Ergänzend sei bemerkt, dass mittlerweile die Zahlen der Veranstaltungen wie auch der Teilnehmenden wieder gestiegen sind, was folgende vergleichende Auswertung der beiden Studienjahre 2023/24 und 2024/25 zeigt, die jedoch außerhalb des Prüfzeitraums des Rechnungshofs liegt.

<b>Studienjahr 2023/24</b>		
<b>Pädagogische Hochschule</b>	<b>Veranstaltungen</b>	<b>Teilnehmende</b>
PH Burgenland	27	488
PH Kärnten	12	267
PH Niederösterreich	22	516
PH Oberösterreich	28	588
PH Salzburg	14	237
PH Steiermark	30	747
PH Tirol	7	178
PH Vorarlberg	10	190
PH Wien	36	1.224
PPH Linz	5	236
PPH Augustinum	2	18
KPH Wien/NÖ	11	337
<b>Gesamt</b>	<b>204</b>	<b>5.026</b>

Studienjahr 2024/25		
Pädagogische Hochschule	Veranstaltungen	Teilnehmende
PH Burgenland	30	676
PH Kärnten	15	281
PH Niederösterreich	28	748
PH Oberösterreich	37	810
PH Salzburg	11	217
PH Steiermark	25	592
PH Tirol	7	297
PH Vorarlberg	6	139
PH Wien	37	1.162
PPH Linz	8	197
PPH Augustinum	1	17
KPH Edith Stein	2	63
KPH Wien/NÖ	12	280
<b>Gesamt</b>	<b>219</b>	<b>5.479</b>

#### Zu den Fragen 4 und 5:

- *Wie viele Schulen setzen nach den dem Ressort vorliegenden Daten keine technisch-inhaltlichen Schutzmaßnahmen ein?*
  - a. *Welche dem Ressort bekannten Vorfälle oder dokumentierten Risikolagen stehen in Zusammenhang mit dem Fehlen solcher Schutzmaßnahmen im schulischen Alltag?*
- *Wie stellen sich nach den dem Ressort vorliegenden Daten die quantitativen Unterschiede zwischen gemeldeten Vorfällen und der Wahrnehmung von Gefahren durch Schulleitungen dar?*

An Schulstandorten kommen grundsätzlich und bereits technisch bedingt Schutzmaßnahmen wie Firewalls mit Contentfilter zum Einsatz, als Netzwerkgeräte sowie auf Endgeräten in Form von Software, die den Datenverkehr regeln und Filterregeln anwenden. Vor dem Hintergrund dieser etablierten Infrastruktur bestehen seitens des Bundesministeriums für Bildung keine Hinweise darauf, dass Schulen von der bisherigen Praxis abweichen.

Das zitierte Umfrageergebnis zeigt allerdings auf, dass regelmäßige Informationen zu diesem Thema zweckmäßig sind. Dementsprechend stellt das Bundesministerium für Bildung sicher, dass Schulleitungen im Rahmen von Dienstbesprechungen sensibilisiert und auch qualifiziert werden, um ihrerseits dafür sorgen, dass dies im Rahmen von Konferenzen am Schulstandort auch für die Lehrenden und Bediensteten der Fall ist.

Zusätzlich setzt das Bundesministerium für Bildung im Rahmen der Geräteinitiative eine bundesweite Kinderschutzmaßnahme direkt auf den Endgeräten der Schülerinnen und Schüler um. Durch den Einsatz von Webfiltern und einheitlichen Empfehlungen zu Gerätekonfigurationen, welche im Mobile Device Management durch die Schulen

umgesetzt werden, wird der Zugriff auf unangemessene Internetinhalte nicht nur im Schulnetzwerk, sondern auch darüber hinaus wirksam eingeschränkt, und ein Standard geschaffen. Die Konten der Schülerinnen und Schüler werden dafür ohne administrative Rechte eingerichtet, um ein Umgehen der Schutzmechanismen zu verhindern. Gleichzeitig werden Erziehungsberechtigten technische Möglichkeiten eingeräumt, mit denen von ihnen gewünschte Einstellungen bzw. Installationen und Anpassungen möglich sind. So ist beispielsweise für eine privat veranlasste Installation einer Anwendung, wie etwa einem Spiel, die Zustimmung der Erziehungsberechtigten mit ihrem lokalen Administratorkonto am Gerät des Schülers bzw. der Schülerin erforderlich. Diese technische Lösung verbindet einen verbesserten und standortunabhängigen Kinder- und Jugendschutz mit elterlicher Mitbestimmung und entlastet die Schulen durch Empfehlungen und technische Unterstützung bei der Umsetzung.

#### Zu Frage 6:

- *Welche Funktionen erfüllen technisch-organisatorische Maßnahmen in den Konzepten des Ressorts zur Internetsicherheit an Schulen und wie sind diese mit pädagogischen Präventionsmaßnahmen verknüpft?*

Mit den Vorgaben zur IT-Standardisierung für die Bildungsdirektionen und Schulstandorte sorgt das Bundesministerium für Bildung für eine technisch-organisatorische Orientierung sowie für die Etablierung eines Mindeststandards. An Schulen fungieren außerdem Lehrpersonen im Bereich der pädagogischen IT-Betreuung, sodass sich Technik und Pädagogik sinnvoll ergänzen.

#### Zu Frage 7:

- *Welche derzeit vom Ressort vorgesehenen oder umgesetzten Programme, Initiativen und Maßnahmen dienen der Sensibilisierung von Schulleitungen, Lehrpersonen sowie Schülerinnen und Schülern im Bereich der Internetsicherheit? Welche operativen und strategischen Anpassungen leitet das Ressort aus den Feststellungen des Rechnungshofes für die Weiterentwicklung bestehender Maßnahmen zum Thema sicheres Internet an Schulen ab?*

Im Rahmen des Ressourcen-, Ziel- und Leistungsplans wurden die Bildungsdirektionen angewiesen, in jedem Bundesland bis Juni 2026 Dienstbesprechungen für Schulleitungen und Schulqualitätsmanagerinnen bzw. -manager umzusetzen, die u.a. auch das Thema IT-Sicherheit zum Schwerpunkt haben.

Über die Kooperation mit Saferinternet.at steht Schulen ein umfassendes Unterstützungspaket bereit, um den sicheren und verantwortungsvollen Umgang mit digitalen Medien zu fördern. Lehrende erhalten Unterrichtsmaterialien, Leitfäden und fertige Workshop-Konzepte zu Themen wie z.B. Cyber-Mobbing, Datenschutz oder Gestaltung von Privatsphäre im Internet. Für Schülerinnen und Schüler gibt es altersgerechte Tipps und Informationsangebote, die ihnen helfen, Risiken im Netz, wie z.B.

Fake News oder Belästigung, zu erkennen und sich davor zu schützen.

Erziehungsberechtigte finden auf dem Portal von Safer Internet praktische Elternratgeber, Video-Tipps und Leitfäden für die Medienerziehung zu Hause, um ihre Kinder kompetent durch die digitale Welt zu begleiten und bei Problemen richtig zu reagieren. Zusätzlich vermittelt die Plattform Expertinnen und Experten für Vorträge und Workshops an den Schulen.

Für die gezielte Fortbildung von Lehrenden stehen ergänzend zu den Angeboten der Pädagogischen Hochschulen auch flexible Online-Angebote wie Massive Open Online Courses (MOOCs), z.B. zu den Themen Fake News, Hate Speech und Manipulationsstrategien im Internet zur Verfügung, die eine zeitunabhängige und vertiefende Auseinandersetzung mit aktuellen digitalen Herausforderungen ermöglichen. Diese digitalen Lehrgänge bieten nicht nur theoretisches Hintergrundwissen, sondern auch praxisnahe Methoden und Materialien, mit denen die kritische Medienreflexion der Schülerinnen und Schüler gezielt gestärkt werden kann. Die Virtuelle Pädagogische Hochschule (VPH) bietet regelmäßig im Format eLectures Online-Fortbildungen zu aktuellen Medienthemen an, die der Zielgruppe im Nachhinein auch als Aufzeichnungen im Archiv zur Verfügung stehen.

Zur Weiterentwicklung des Schulfächerkanons inkl. neuer Lehrpläne wurde bereits unter Frage 2 eingegangen. Damit verbunden ist auch eine weitere Stärkung jener Kompetenzen, die einen sicheren und verantwortungsvollen Umgang mit digitalen Technologien betreffen. Durch diese curriculare Verankerung wird Internetsicherheit nicht nur als technisches Thema verstanden, sondern auch in ihren gesellschaftlichen, rechtlichen und ethischen Dimensionen aufgegriffen. Ziel ist es, Schülerinnen und Schüler zu einer mündigen, reflektierten und sicheren Nutzung digitaler Technologien zu befähigen.

Einen Beitrag zur Sensibilisierung der Schulen im Bereich der Internetsicherheit leisten auch die verpflichtend zu erstellenden Kinderschutzkonzepte. Bei der Ausarbeitung der Kinderschutzkonzepte müssen sich Schulen u.a. damit befassen, welche digitalen Kommunikationskanäle sie nutzen, welche technischen Maßnahmen sicherstellen, dass Kinder und Jugendliche über ihre Geräte in der Schule nur altersgerechte Inhalte erreichen und wie Schulen Lehrinhalte zur digitalen (Grund-)Bildung im Sinne des Kinderschutzes und unter Berücksichtigung möglicher Gefahren (z.B. Cybermobbing, Fake News, Grooming) gestalten.

Die zielgruppenspezifische Aufbereitung und Kommunikation der zahlreichen Präventionsangebote wird regelmäßig weiterentwickelt, womit das Bundesministerium für Bildung auch einer Empfehlung des Rechnungshofs nachkommt.

Wien, 6. Mai 2026

Christoph Wiederkehr, MA

