Schriftliche Frage Nr. 136 vom 26. Februar 2026 von Herrn Hoffmann an Minister Franssen zum Schutz von minderjährigen Nutzern der von der Deutschsprachigen Gemeinschaft bereitgestellten Schullaptops (Nachfrage zur SF Nr. 116)[1]

Frage

Ihre Antwort auf meine schriftliche Frage Nr. 116 vermittelt auf den ersten Blick ein beruhigendes Bild: ein einheitliches, hohes Schutzniveau durch zentrale Administration, Firewall, Webfilter und verpflichtende Nutzung von NextDNS. Gleichzeitig erklären Sie aber, dass Schule, Schulträger, Ministerium und Regierung nicht für besuchte Internetseiten und deren Inhalte verantwortlich gemacht werden können, und ordnen dies als Haftungsausschluss für Inhalte Dritter ein.

Hinzu kommt, dass uns Eltern mehrfach berichtet haben, dass auf den Geräten sowohl in der Schule als auch zu Hause ohne erkennbare Barrieren gesurft werden kann. Diese Rückmeldungen sind konkret und wiederholt erfolgt. Wenn gleichzeitig von einem hohen Schutzniveau gesprochen wird, dann muss dieses auch in der Praxis spürbar sein und nicht nur auf dem Papier bestehen. Gerade bei zentral verwalteten staatlich bereitgestellten Geräten darf ein behauptetes Schutzniveau nicht nur behauptet, sondern muss organisatorisch und technisch nachweisbar sein.

Genau an diesem Punkt beginnt das Problem: Wenn die Geräte zentral bereitgestellt, konfiguriert und administriert werden und Eltern weder Filter einstellen noch technisch eingreifen können, kann die politische und organisatorische Verantwortung für die Schutzarchitektur nicht hinter dem Hinweis auf Drittinhalte verschwinden. Die Frage der Haftung für fremde Inhalte ist das eine. Die Verantwortung für funktionierende Schutzmechanismen, klare Standards, wirksame Kontrolle und nachvollziehbare Nachsteuerung ist etwas anderes und ergibt sich im Kern auch aus Ihrer Antwort.

Gerade deshalb braucht das Parlament hier mehr Klarheit. Denn Ihre Antwort bestätigt zugleich, dass bewusst auf altersgestufte Benutzerprofile verzichtet wird und für alle Schülerinnen und Schüler ein einheitliches Schutzprofil gilt. Das mag administrativ einfacher sein, wirft aber im Sekundarbereich erhebliche Fragen auf, wenn 12- oder 13-Jährige technisch im selben Raster geführt werden wie ältere Jugendliche oder Volljährige.

Hinzu kommt: Sie verweisen auf automatisierte und zeitnahe Updates sowie auf eine kontinuierliche Überprüfung und Nachjustierung der Schutzmaßnahmen. Wenn aus der Praxis dennoch Hinweise auf Lücken oder uneinheitliche Konfigurations- bzw. Aktualisierungsstände gemeldet werden, dann reicht ein allgemeiner Verweis auf ein „hohes Schutzniveau" nicht aus. Dann braucht es überprüfbare Angaben zu Zuständigkeiten, Intervallen, Reaktionszeiten und Wirksamkeit.

Zudem ist festzuhalten, dass eine DNS-basierte Filterlösung wie NextDNS funktional nur einen Teilbereich des Jugendschutzes abdecken kann. Sie kann insbesondere plattforminterne Inhalte (z. B. innerhalb von YouTube), Chat-Kommunikation, Bildschirmzeit-Regelungen oder App-Nutzung nicht in gleicher Weise steuern wie weitergehende Endgeräte- oder Plattformlösungen.

Vor diesem Hintergrund bitte ich um Beantwortung der folgenden Fragen:

1. Auf welcher konkreten rechtlichen Grundlage stützt sich die in den Nutzungsbedingungen enthaltene Klausel, wonach Schule, Schulträger, Ministerium und Regierung nicht für besuchte Internetseiten und deren Inhalte verantwortlich gemacht werden können?
2. Wer hat die betreffende Klausel in den Nutzungsbedingungen inhaltlich ausgearbeitet, rechtlich geprüft und genehmigt?

[1] Die nachfolgend veröffentlichten Texte entsprechen den hinterlegten Originalfassungen.

3. Wie grenzt die Regierung rechtlich und praktisch die Haftung für Inhalte Dritter im Internet einerseits und die Verantwortung für technische Schutzmaßnahmen, organisatorische Vorgaben und deren Kontrolle andererseits ab?
4. Ist die Regierung der Auffassung, dass Eltern Verantwortung für ein System (Hardware und Software) tragen sollen, welches sie technisch weder konfigurieren noch kontrollieren können?
5. Welche konkrete Verantwortung trägt das Ministerium, wenn sich herausstellt, dass zentrale Schutzmechanismen (z. B. Filterregeln, Konfigurationen oder Aktualisierungen) nicht wirksam greifen oder nicht korrekt umgesetzt wurden?
6. Gibt es hierfür eine interne Zuständigkeits- und Eskalationsregelung? Falls ja, wie ist diese strukturiert (zuständige Stellen, Meldeweg, Reaktionsfristen)?
7. Wie viele Meldungen oder Beschwerden zu problematischen Inhalten, unzureichender Filterung oder Sicherheitslücken auf Schullaptops sind seit Einführung des Systems eingegangen (bitte nach Jahren seit 2022 aufschlüsseln)?
8. Wie viele dieser Meldungen führten zu systemweiten Anpassungen der Schutzmaßnahmen (z. B. Filterregeln, Konfigurationen oder organisatorischen Vorgaben)?
9. Welche Kennzahlen oder Prüfkriterien verwendet das Ministerium, um die Wirksamkeit der eingesetzten Schutz- und Filtersysteme zu bewerten (z. B. erkannte Vorfälle, Nachjustierungen, Reaktionszeiten)?
10. In welchen verbindlichen Intervallen werden die zentralen Schutzmechanismen (Firewall-Regeln, Filterkategorien, sicherheitsrelevante Konfigurationen) überprüft und angepasst?
11. Welche Inhaltsbereiche bzw. Kategorien sind im Schutzsystem derzeit bewusst nicht gesperrt, und wer entscheidet über diese Freigaben bzw. Nicht-Sperrungen?
12. Wie wird konkret sichergestellt, dass auf allen Schullaptops sicherheitsrelevante Software und Konfigurationen auf einem einheitlichen und aktuellen Stand sind, und wie werden Abweichungen festgestellt und behoben?
13. Wer trägt die operative Verantwortung für die Kontrolle der Versions- und Konfigurationsstände auf den Endgeräten, und welche Reaktionszeit gilt bei festgestellten Abweichungen?
14. Sie begründen den Verzicht auf altersgestufte Benutzerprofile mit einem einheitlichen hohen Schutzniveau. Wurde eine altersabhängige Zugriffsdifferenzierung dennoch geprüft? Falls ja, mit welchem Ergebnis; falls nein, warum nicht?
15. Wie begründet die Regierung pädagogisch und technisch, dass im Sekundarbereich jüngere Minderjährige und ältere Jugendliche bzw. Volljährige mit demselben technischen Schutzprofil arbeiten?
16. Welche ergänzenden technischen oder organisatorischen Maßnahmen bestehen für Bereiche, die durch DNS-basierte Filter systembedingt nur begrenzt erfasst werden können (z. B. plattforminterne Inhalte)?
17. Welche konkreten Instrumente setzt die Regierung ergänzend ein, um auf schulischen Geräten Bildschirmzeit, App-Nutzung und Chat-Kommunikation im schulischen Kontext zu regeln bzw. pädagogisch-technisch zu begleiten?
18. Wird das Gesamtsystem der Schutzmaßnahmen regelmäßig unabhängig überprüft (Audit/Externevaluation)? Falls ja, wann zuletzt und in welcher Form; falls nein, warum nicht?

Antwort eingegangen am 27. März 2026

1. Auf welcher konkreten rechtlichen Grundlage stützt sich die in den Nutzungsbedingungen enthaltene Klausel, wonach Schule, Schulträger, Ministerium und Regierung nicht für besuchte Internetseiten und deren Inhalte verantwortlich gemacht werden können?

Die Grundlage bilden die allgemeinen Bestimmungen des Straf- und Zivilrechts.

Vor diesem Hintergrund wird diese Verantwortungszuordnung auch in der Nutzungsvereinbarung für die schulischen Geräte, die von den Schülerinnen und Schülern sowie den Erziehungsberechtigten verbindlich unterzeichnet wird, ausdrücklich aufgegriffen.

Darin ist festgelegt, dass die Geräte ausschließlich für schulische Zwecke genutzt werden und die Nutzerinnen und Nutzer sich zu einem verantwortungsvollen Umgang – insbesondere im Internet – verpflichten. Zudem wird klargestellt, dass Verstöße gegen diese Regeln nicht nur schulische Maßnahmen nach sich ziehen, sondern auch zivil- und strafrechtliche Folgen haben können.

2. Wer hat die betreffende Klausel in den Nutzungsbedingungen inhaltlich ausgearbeitet, rechtlich geprüft und genehmigt?

Die Nutzungsbedingungen wurden im Rahmen der Einführung der Schülerlaptops durch die zuständigen administrativen Dienste des Ministeriums erarbeitet.

Die rechtliche Prüfung erfolgte durch die hierfür zuständigen Stellen innerhalb der Verwaltung unter Einbezug juristischer Expertise.

Die Genehmigung der Nutzungsbedingungen erfolgte anschließend im Rahmen der üblichen internen Verwaltungsprozesse.

3. Wie grenzt die Regierung rechtlich und praktisch die Haftung für Inhalte Dritter im Internet einerseits und die Verantwortung für technische Schutzmaßnahmen, organisatorische Vorgaben und deren Kontrolle andererseits ab?

Die angesprochene Unterscheidung ist grundlegend und wurde bereits in der Antwort auf die schriftliche Frage Nr. 116 dargelegt.

Die Haftungsklausel in den Nutzungsbedingungen bezieht sich ausschließlich auf die inhaltliche Verantwortung für Internetseiten, die von Dritten betrieben und gestaltet werden und auf deren Inhalte weder Schule, Schulträger noch Ministerium oder Regierung Einfluss nehmen. Für diese Inhalte sind grundsätzlich die jeweiligen Anbieter verantwortlich.

Davon klar zu trennen ist die institutionelle Verantwortung für die Bereitstellung und Ausgestaltung eines angemessenen Schutzrahmens bei der Nutzung der schulischen Geräte. Diese umfasst insbesondere die Konzeption, Implementierung, laufende Anpassung sowie Kontrolle der technischen Schutzmaßnahmen (z. B. Filter- und Sicherheitssysteme) und der organisatorischen Vorgaben.

Diese wird durch Regierung und Ministerium aktiv wahrgenommen, unterliegt einer kontinuierlichen Weiterentwicklung und ist nicht Gegenstand des Haftungsausschlusses.

4. Ist die Regierung der Auffassung, dass Eltern Verantwortung für ein System (Hardware und Software) tragen sollen, welches sie technisch weder konfigurieren noch kontrollieren können?

Die technische Verantwortung für die Konfiguration, Administration und Umsetzung der Schutzmaßnahmen liegt eindeutig beim Ministerium sowie bei den zuständigen schulischen IT-Verantwortlichen. Es handelt sich um zentral verwaltete Geräte, auf deren technische Ausgestaltung Eltern keinen direkten Einfluss haben.

Vor diesem Hintergrund wird von Eltern auch keine technische Kontrolle des Systems erwartet.

Die Nutzungsbedingungen regeln vielmehr die allgemeinen Verhaltens- und Sorgfaltspflichten im Umgang mit den Geräten. Sie betreffen insbesondere einen verantwortungsvollen Gebrauch im schulischen Kontext, begründen jedoch keine technische Verantwortung der Eltern für das zugrunde liegende Schutzsystem.

5. Welche konkrete Verantwortung trägt das Ministerium, wenn sich herausstellt, dass zentrale Schutzmechanismen (z. B. Filterregeln, Konfigurationen oder Aktualisierungen) nicht wirksam greifen oder nicht korrekt umgesetzt wurden?

Das Ministerium trägt die Systemverantwortung für die technische Infrastruktur sowie die eingesetzten Schutzmechanismen. Diese umfasst insbesondere die Verpflichtung, bekannt gewordene Schwachstellen zeitnah zu beheben, Konfigurationsfehler zu korrigieren und auf gemeldete Sicherheitslücken angemessen zu reagieren.

Wird festgestellt, dass zentrale Schutzmechanismen nicht wirksam greifen oder nicht korrekt umgesetzt wurden, erfolgt eine umgehende Analyse der Ursachen. Auf dieser Grundlage werden die erforderlichen technischen und organisatorischen Anpassungen identifiziert und systemweit umgesetzt.

Dieser Verantwortung wird konsequent nachgekommen: Alle bislang bekannt gewordenen Umgehungsmöglichkeiten wurden systematisch analysiert und durch gezielte Gegenmaßnahmen geschlossen.

6. Gibt es hierfür eine interne Zuständigkeits- und Eskalationsregelung? Falls ja, wie ist diese strukturiert (zuständige Stellen, Meldeweg, Reaktionsfristen)?

Ja. Für sicherheitsrelevante Vorfälle und gemeldete Schwachstellen besteht eine klar definierte Zuständigkeits- und Eskalationsstruktur.

Meldungen erfolgen in der Regel zunächst an die schulischen IT-Verantwortlichen, die als erste Anlaufstelle fungieren und eine erste Einschätzung sowie gegebenenfalls unmittelbare Maßnahmen vornehmen. Kann das Problem auf dieser Ebene nicht abschließend gelöst werden oder besteht systemischer Handlungsbedarf, erfolgt eine Weiterleitung über das zentrale Ticketsystem an die zuständigen Dienste des Ministeriums.

Dort werden die eingehenden Meldungen thematisch klassifiziert und nach ihrer Dringlichkeit priorisiert. Sicherheitskritische Vorfälle werden mit hoher Priorität behandelt. Sofern es sich um systemrelevante Sachverhalte handelt, werden die entsprechenden Maßnahmen zentral umgesetzt und auf alle betroffenen Schulen ausgeweitet.

Innerhalb des IT-Betriebs bestehen zudem definierte Reaktionszeitvorgaben für sicherheitskritische Fälle, um eine zeitnahe Bearbeitung und Behebung sicherzustellen.

7. Wie viele Meldungen oder Beschwerden zu problematischen Inhalten, unzureichender Filterung oder Sicherheitslücken auf Schullaptops sind seit Einführung des Systems eingegangen (bitte nach Jahren seit 2022 aufschlüsseln)?

Meldungen zu problematischen Inhalten, unzureichender Filterung oder möglichen Sicherheitslücken auf Schullaptops werden grundsätzlich über das zentrale Ticketing-System erfasst.

Eine gesonderte statistische Auswertung dieser Meldungen nach Kategorien oder Jahren erfolgt derzeit jedoch nicht. Vor diesem Hintergrund können keine belastbaren Zahlen für den angefragten Zeitraum seit 2022 angegeben werden, ohne eine aufwendige manuelle Auswertung der einzelnen Tickets vorzunehmen.

Unabhängig davon werden eingehende Meldungen systematisch bearbeitet und fließen kontinuierlich in die Weiterentwicklung des Systems ein. Insbesondere in der Einführungsphase wurden auf Grundlage von Rückmeldungen aus der Praxis gezielte Anpassungen vorgenommen. In diesem Zusammenhang wurde unter anderem der Dienst NextDNS als zusätzliche Filterlösung implementiert.

Die Wirksamkeit des Systems zeigt sich daher weniger in der statistischen Erfassung einzelner Meldungen als vielmehr in der zeitnahen Reaktion auf Hinweise aus der Praxis sowie in der fortlaufenden Optimierung der eingesetzten Filter- und Sicherheitsmechanismen.

8. Wie viele dieser Meldungen führten zu systemweiten Anpassungen der Schutzmaßnahmen (z. B. Filterregeln, Konfigurationen oder organisatorischen Vorgaben)?

Eine gesonderte statistische Erfassung darüber, welche einzelnen Meldungen zu systemweiten Anpassungen geführt haben, erfolgt nicht. Vor diesem Hintergrund können hierzu keine quantitativen Angaben gemacht werden.

Grundsätzlich ist in diesem Themenbereich eine hohe Dynamik festzustellen: Neue Webseiten, Dienste und Inhalte entstehen fortlaufend, wodurch Filtersysteme und Sicherheitsmaßnahmen regelmäßig überprüft und bei Bedarf angepasst werden müssen, um ein angemessenes Schutzniveau sicherzustellen.

Rückmeldungen aus der Praxis werden dabei systematisch ausgewertet und fließen kontinuierlich in die Weiterentwicklung des Systems ein. Anpassungen erfolgen sowohl anlassbezogen – etwa bei konkreten Hinweisen auf Umgehungsmöglichkeiten – als auch präventiv im Rahmen der laufenden Systempflege.

Systemrelevante Anpassungen werden zentral umgesetzt und auf alle betroffenen Geräte bzw. Schulen ausgerollt.

9. Welche Kennzahlen oder Prüfkriterien verwendet das Ministerium, um die Wirksamkeit der eingesetzten Schutz- und Filtersysteme zu bewerten (z. B. erkannte Vorfälle, Nachjustierungen, Reaktionszeiten)?

Für die Bewertung der Wirksamkeit der eingesetzten Schutz- und Filtersysteme werden derzeit keine fest definierten Kennzahlen im Sinne eines standardisierten Kennzahlensystems erhoben.

Die Einschätzung der Wirksamkeit erfolgt vielmehr praxisorientiert auf Grundlage der im laufenden Betrieb eingehenden Rückmeldungen und Supportanfragen, die über das zentrale Ticketing-System erfasst werden. Ergänzend fließen Erkenntnisse aus der Bearbeitung konkreter Vorfälle, aus vorgenommenen Nachjustierungen sowie aus der operativen Systembetreuung in die Bewertung ein.

Ziel ist es, die Schutzmechanismen kontinuierlich an neue Entwicklungen und Nutzungsmuster anzupassen und auf dieser Grundlage ein angemessenes und aktuelles Schutzniveau sicherzustellen.

10. In welchen verbindlichen Intervallen werden die zentralen Schutzmechanismen (Firewall-Regeln, Filterkategorien, sicherheitsrelevante Konfigurationen) überprüft und angepasst?

Sicherheitsupdates für Betriebssystem, Schutzsoftware und relevante Anwendungen werden automatisiert und zeitnah eingespielt. Kritische Updates werden dabei priorisiert behandelt.

Die Überprüfung und Anpassung von Firewall-Regeln, Filterkategorien und sicherheitsrelevanten Konfigurationen erfolgen sowohl anlassbezogen – insbesondere bei neuen Erkenntnissen oder gemeldeten Vorfällen – als auch im Rahmen regelmäßiger IT-Überprüfungen.

Ergänzend findet ein strukturierter und kontinuierlicher Austausch mit den schulischen IT-Verantwortlichen statt, um Rückmeldungen aus der Praxis zeitnah in die Weiterentwicklung der Schutzmechanismen einfließen zu lassen.

Ein starrer, einheitlicher Prüfzyklus besteht dabei nicht, da eine flexible und anlassbezogene Anpassung in diesem dynamischen Bereich ein höheres Maß an Wirksamkeit gewährleistet.

11. Welche Inhaltsbereiche bzw. Kategorien sind im Schutzsystem derzeit bewusst nicht gesperrt, und wer entscheidet über diese Freigaben bzw. Nicht-Sperrungen?

Die eingesetzten Schutzsysteme sperren standardmäßig eine breite Palette risikobehafteter Inhaltskategorien (vgl. Antwort auf die schriftliche Frage Nr. 116, Frage 1).

Nicht gesperrt sind grundsätzlich allgemein zugängliche Bildungs- und Informationsangebote, soweit von diesen keine sicherheits- oder jugendschutzrelevanten Risiken ausgehen. Darüber hinaus können – je nach pädagogischem Bedarf – bestimmte Plattformen, wie etwa Videoplattformen, gezielt freigegeben werden.

Die grundsätzliche Konfiguration des Schutzsystems sowie die Definition gesperrter Kategorien erfolgen zentral durch das Ministerium im Rahmen der technischen und organisatorischen Vorgaben.

Im Rahmen dieses vorgegebenen Rahmens obliegt es den Schulen, pädagogisch begründete Entscheidungen über weitergehende Freigaben zu treffen. Diese erfolgen unter Berücksichtigung des Unterrichtskontexts und der jeweiligen Nutzungssituation.

12. Wie wird konkret sichergestellt, dass auf allen Schullaptops sicherheitsrelevante Software und Konfigurationen auf einem einheitlichen und aktuellen Stand sind, und wie werden Abweichungen festgestellt und behoben?

Die eingesetzten Geräte werden zentral administriert. Dadurch können sicherheitsrelevante Updates sowie Konfigurationsänderungen einheitlich und zeitnah über die zentrale Verwaltungsinfrastruktur ausgerollt werden.

Der Aktualisierungs- und Konfigurationsstatus der Geräte wird kontinuierlich über diese Infrastruktur überwacht. Abweichungen vom vorgesehenen Soll-Zustand – etwa infolge längerer Offline-Zeiten oder technischer Besonderheiten einzelner Geräte – werden systemseitig erkannt.

Sobald betroffene Geräte wieder eine Verbindung zum System herstellen, werden ausstehende Updates und Konfigurationsanpassungen automatisiert nachgezogen, sodass ein einheitlicher und aktueller Sicherheitsstand wiederhergestellt wird.

13. Wer trägt die operative Verantwortung für die Kontrolle der Versions- und Konfigurationsstände auf den Endgeräten, und welche Reaktionszeit gilt bei festgestellten Abweichungen?

Die operative Verantwortung für die Kontrolle der Versions- und Konfigurationsstände liegt beim zuständigen Fachbereich IT des Ministeriums der Deutschsprachigen Gemeinschaft in enger Zusammenarbeit mit den schulischen IT-Verantwortlichen.

Die Überprüfung erfolgt im Rahmen der zentralen Geräteverwaltung sowie der laufenden Systemüberwachung. Abweichungen vom vorgesehenen Soll-Zustand werden systemseitig erkannt und entsprechend eingeordnet.

Für sicherheitskritische Abweichungen gilt das Prinzip der prioritären und zeitnahen Behebung. Diese werden mit hoher Priorität behandelt und schnellstmöglich korrigiert.

Allgemeine Konfigurationsabweichungen werden im Rahmen des regulären IT-Betriebs bearbeitet und bei der nächsten Systemverbindung oder im Zuge geplanter Aktualisierungen behoben.

14. Sie begründen den Verzicht auf altersgestufte Benutzerprofile mit einem einheitlichen hohen Schutzniveau. Wurde eine altersabhängige Zugriffsdifferenzierung dennoch geprüft? Falls ja, mit welchem Ergebnis; falls nein, warum nicht?

Eine altersabhängige Zugriffsdifferenzierung wurde im Rahmen der Konzeption des Systems grundsätzlich mitgedacht.

Dabei hat sich gezeigt, dass ein einheitliches, hoch abgesichertes Profil für alle Schülerinnen und Schüler im schulischen Kontext derzeit die verlässlichere und betrieblich stabilere Lösung darstellt. Differenzierte Profile würden die Komplexität der Administration deutlich erhöhen und gleichzeitig das Risiko von Konfigurationsfehlern und Inkonsistenzen steigern, insbesondere bei einer großen Anzahl an Geräten und unterschiedlichen Nutzungsszenarien.

Das gewählte Modell ermöglicht hingegen ein durchgängig hohes und einheitliches Schutzniveau, das technisch konsistent umgesetzt und effizient verwaltet werden kann.

Unabhängig davon wird die Weiterentwicklung des Systems kontinuierlich geprüft. Dabei werden auch Möglichkeiten einer differenzierteren Steuerung – unter Wahrung der Betriebssicherheit und des Schutzniveaus – fortlaufend bewertet.

15. Wie begründet die Regierung pädagogisch und technisch, dass im Sekundarbereich jüngere Minderjährige und ältere Jugendliche bzw. Volljährige mit demselben technischen Schutzprofil arbeiten?

Technisch gewährleistet ein einheitliches Schutzprofil für alle Altersgruppen das höchstmögliche Sicherheitsniveau. Dies gewährleistet eine konsistente und verlässliche Administration und reduziert gleichzeitig potenzielle Fehlerquellen, die bei differenzierten Profilen entstehen können.

Aus pädagogischer Sicht erfolgt die notwendige Differenzierung nicht primär über technische Einschränkungen, sondern über die altersgerechte Begleitung, Anleitung und Sensibilisierung der Schülerinnen und Schüler. Ziel ist es, einen verantwortungsvollen und reflektierten Umgang mit digitalen Medien zu fördern.

Dieses Vorgehen ermöglicht es, innerhalb eines einheitlichen technischen Rahmens flexibel auf unterschiedliche Lern- und Entwicklungsstände einzugehen, ohne unterschiedliche technische Zugänge innerhalb desselben schulischen Kontextes zu schaffen.

16. Welche ergänzenden technischen oder organisatorischen Maßnahmen bestehen für Bereiche, die durch DNS-basierte Filter systembedingt nur begrenzt erfasst werden können (z. B. plattforminterne Inhalte)?

Es ist zutreffend, dass DNS-basierte Filterlösungen systembedingt an Grenzen stoßen, insbesondere bei der Erfassung plattforminterner Inhalte oder bei Kommunikationsfunktionen innerhalb von Anwendungen.

Vor diesem Hintergrund erfolgt der Schutz nicht ausschließlich über DNS-basierte Filter, sondern wird durch weitere technische und organisatorische Maßnahmen ergänzt. Dazu zählen insbesondere zentrale Gerätekonfigurationen, Einschränkungen bei der Installation von Software (keine Administratorrechte für Schülerinnen und Schüler) sowie die Nutzung vordefinierter Anwendungen und Dienste.

Darüber hinaus kommt der pädagogischen Begleitung im schulischen Kontext eine zentrale Rolle zu. Lehrkräfte steuern die Nutzung im Unterricht, vermitteln Medienkompetenz und sensibilisieren für einen verantwortungsvollen Umgang mit digitalen Inhalten.

Eine weitergehende inhaltliche Kontrolle plattforminterner Inhalte würde zusätzliche technische Lösungen erfordern, die über DNS-basierte Ansätze hinausgehen und mit Blick auf Verhältnismäßigkeit, Datenschutz und pädagogische Zielsetzungen sorgfältig abzuwägen wären.

17. Welche konkreten Instrumente setzt die Regierung ergänzend ein, um auf schulischen Geräten Bildschirmzeit, App-Nutzung und Chat-Kommunikation im schulischen Kontext zu regeln bzw. pädagogisch-technisch zu begleiten?

Derzeit werden keine spezifischen technischen Instrumente eingesetzt, um Bildschirmzeit, App-Nutzung oder Chat-Kommunikation auf schulischen Geräten zentral zu steuern oder auszuwerten.

Vor einer möglichen Einführung entsprechender Lösungen besteht zunächst Klärungsbedarf hinsichtlich grundlegender Fragestellungen. Dazu zählen insbesondere die pädagogischen Zielsetzungen, die datenschutzrechtlichen Rahmenbedingungen sowie die grundsätzliche Abwägung, in welchem Umfang eine technische Steuerung oder Überwachung im schulischen Kontext erfolgen soll.

Die Begleitung der Nutzung erfolgt daher in erster Linie über pädagogische und organisatorische Maßnahmen. Lehrkräfte steuern den Einsatz der Geräte im Unterricht, setzen klare Rahmenbedingungen für deren Nutzung und fördern einen reflektierten und verantwortungsvollen Umgang mit digitalen Medien.

Ergänzend trägt ein didaktisch vielfältiger Unterricht dazu bei, Bildschirmzeiten ausgewogen zu gestalten. So kommen neben digitalen auch analoge und haptische Medien zum Einsatz, die unter anderem über die Schulmediotheken bereitgestellt werden und die Nutzung digitaler Anwendungen entsprechend einbetten und begrenzen.

18. Wird das Gesamtsystem der Schutzmaßnahmen regelmäßig unabhängig überprüft (Audit/Externe Evaluation)? Falls ja, wann zuletzt und in welcher Form; falls nein, warum nicht?

Eine förmliche externe Evaluation durch Dritte im Sinne eines vollständigen Audits des Gesamtsystems hat bislang nicht stattgefunden.

Die Konzeption und Ausgestaltung der Schutzmaßnahmen orientieren sich jedoch an den Vorgaben des Centre for Cybersecurity Belgium sowie an anerkannten Sicherheitsstandards und den Anforderungen der NIS-2-Richtlinie. Darüber hinaus erfolgt eine punktuelle Einbindung externer fachlicher Expertise, insbesondere durch spezialisierte Sicherheitsdienstleister.

Ergänzend wird das System regelmäßig durch den zuständigen Fachbereich IT des Ministeriums überprüft und weiterentwickelt.