



► **Abteilungskonferenz Mittelschulen**

Vorgehen bei Betrugsverdacht während digitalen Prüfungen (Schwerpunkt: Exam.net im Hochsicherheitsmodus mit SEB)

I. Rechtlicher Rahmen: Mitwirkungspflicht

Bei begründetem Verdacht (vgl. Beispiele in III.) müssen die Lernenden gemäss ihrer Mitwirkungspflicht die von den IT-Spezialisten verlangten Inhalte ihrer Laptops diesen und den Aufsicht habenden Lehrpersonen aktiv zugänglich (im Sinne von *Einsicht**) machen (z.B. hinsichtlich allfällig manipulierten Betriebssystems/Programmen, verwendetem Netzwerk oder bezüglich installierten Betrugs-Tools).

Wichtig: Die IT-Spezialisten selbst nehmen dabei keine Manipulierung an den BYOD-Laptops vor, sondern die Lernenden zeigen die notwendigen Inhalte in ihren Laptops den Lehrpersonen.

Eine Verweigerung dieser Mitwirkungspflicht oder der Nachweis eines Betrugs genügen der zuständigen Lehrperson bei schriftlichen Leistungserhebungen als Grundlage für die Reduktion der Note bis zur niedrigsten möglichen Bewertung.

Bei Maturaprüfungen würden die Verweigerung der Mitwirkungspflicht oder der Nachweis eines Betrugs zum Ausschluss von den Maturitätsprüfungen führen.

*Die geforderte Einsicht bezieht sich nur auf prüfungsrelevante technische Informationen (z. B. laufende Prozesse/Logs/Netzwerk), keine Durchsicht privater Dateien ohne schulischen Bezug.

II. Ablauf bei Betrugsverdacht während BYOD-basierten Prüfungen (closed book):

Die folgenden Schritte beziehen sich in erster Linie auf Betrugsverdacht hinsichtlich der Verwendung manipulierter oder verbotener Programme, externer Hilfe via Internet oder der Verwendung von KI-Programmen in BYOD-basierten Prüfungen (closed book, z.B. Exam.net im Hochsicherheitsmodus). Bei Betrugsverdacht hinsichtlich heimlicher Handy-Nutzung, Spickzettel-Verwendung, etc. ist ein Hin-zuziehen des IT-Supports und eine Untersuchung des Laptops nicht nötig.

1. Die Lehrperson greift bei begründetem Betrugsverdacht (siehe III.) ein. Sie kommuniziert dem/der Lernenden den Betrugsverdacht. Die Kommunikation gegenüber der lernenden Person erfolgt sachlich und ohne Vorverurteilung. Begriffe wie „Betrug“ sollen im Prüfungsraum vermieden werden. Es handelt sich um eine „technische Abklärung“. Falls sinnvoll, kann die Lehrperson Fotos mit ihrem

- Handy vom Bildschirm des Laptops anfertigen (z.B. um ein erscheinendes Betrugs-Tool abzulichten).
2. Die Lehrperson erklärt dem/der Lernenden den folgenden Ablauf und weist den Lernenden resp. die Lernende an, den Laptop angeschaltet zu lassen, die Prüfung nicht zu beenden resp. das geöffnete Programm nicht zu schliessen.
 3. Die Lehrperson bittet den Lernenden resp. die Lernende an das Lehrpersonenpult. Dabei muss die Lernende resp. Der Lernende seinen/ihren Laptop (Anweisung durch Lehrperson: nicht zuklappen! Nicht abschalten!) mitnehmen. Wenn der Laptop dennoch vom SUS zugeklappt wird, würde dies ebenfalls als Verweigerung der Mitwirkungspflicht gewertet.
 4. Die Lehrperson achtet darauf, dass der/die Lernende keine Eingaben am Laptop macht, währenddessen kontaktiert die Lehrperson den IT-Support vor Ort. Sollte der IT-Support nicht erreichbar sein, wird die Schulleitung kontaktiert. Bei Maturaprüfungen wird direkt die Schulleitung informiert – welche wiederum den IT-Support hinzuzieht.
 5. Der IT-Support wird bei Erscheinen von der Lehrperson knapp über den Betrugsverdacht informiert. Der IT-Support und der/die Lernende verlassen zusammen mit dem Laptop den Prüfungsraum, um die anderen Lernenden nicht zu stören.
 6. Der IT-Support weist den Lernenden resp. die Lernende an, Operationen am Laptop durchzuführen, sodass der IT-Support technische Auffälligkeiten begutachten kann, z.B. Betrug mittels installierter Tools, mehreren parallel geöffneten Betriebssystemen, etc. (siehe III.) Beispiele: «Öffnen Sie den Task-Manager», «Öffnen Sie den Ordner mit der SEB-Installation und öffnen Sie das Logfile XY.» Währenddessen hält die Lehrperson schriftlich fest, was ihre Beobachtung bezüglich Betrugsverdacht war. Die pädagogisch-disziplinarische Bewertung bleibt bei der Lehrperson/Schulleitung. Damit die Aufsicht habende Lp in einer Prüfung den Prüfungsraum nicht verlassen muss, können der IT-Support/die PICTS der Schule hinzugezogen werden - ausser an Maturaprüfungen, wo es empfehlenswert ist, pro Prüfungsraum mind. 2 Aufsichtslehrpersonen einzusetzen, sodass eine der beiden Lp dann bei Betrugsverdacht den Raum verlassen kann.
 7. Sollte vor oder während der Laptop-Untersuchung der/die Lernende den Betrug/Betrugsversuch zugeben, wird dies schriftlich detailliert festgehalten und sowohl von dem/der Lernenden sowie dem IT-Support unterschrieben (Siehe Vorschlag für eine Protokollvorlage am Ende dieses Dokuments) Die Lehrperson wird daraufhin informiert. Die Prüfung ist für den Lernenden resp. die Lernende beendet.
 8. Sollte der Betrugsverdacht entkräftet werden, kann der/die Lernende im Prüfungsraum die Prüfung fortsetzen. Er/sie erhält die «verlorene» Zeit als zusätzli-

- che Prüfungszeit, sofern die Pausenzeit dafür ausreicht. Ansonsten müsste alternativ eine andere anforderungsgleiche Nachholprüfung angesetzt werden
9. Sollte der Betrugsverdacht nicht entkräftet werden können und gibt der/die Lernende den Betrug/Betrugsversuch nicht zu, wird die Schulleitung hinzugezogen und entscheidet. Die Lehrperson im Prüfungsraum wird entsprechend informiert.
 10. Wenn mehr Zeit für die Untersuchung/Abklärung benötigt wird), kann der Laptop der/des Lernenden für eine kurze Zeit (z.B. für 24 Stunden) vom IT-Support eingezogen werden. Dazu wird der Laptop zugeklappt und der/die Lernende wird angewiesen, zu einem weiteren Untersuchungstermin zu erscheinen. Er/sie wird informiert, dass bis dahin der Laptop beim IT-Support bleibt, aber in der Zeit vom Schulpersonal nicht betätigt wird. Während der Prüfung kann die Schülerin/der Schüler dann auf einem ihr auszuhändigenden Schulgerät weiterschreiben, solange der Verdacht nicht erhärtet ist.

Wichtig: Im ganzen Prozess sollte zurückhaltend mit Druck, Verdächtigungen und Anschuldigungen umgegangen werden, um das Verhältnis zu dem/der Lernenden nicht unnötig schwer zu belasten.

III. Verdachtsbegründete Situationen (Beispiele)

Die Entdeckung der unter III. geschilderten Verdachtssituationen ist nur möglich, indem während Prüfungen (A) eine Aufsichtslehrperson gezielt hinter den SuS steht und auf deren Bildschirme schaut und (B) die Aufsichtsperson im Überwachungsfenster in Exam.net die Aktivierung des Hochsicherheitsmodus von jedem SuS regelmässig überprüft. Dies muss via die PICTS an jedem Standort geschult werden.

Situation	Verdacht
Die «Textentstehung» auf dem Laptop-Bildschirm des Lernenden ist nicht synchron zu den Tastatureingaben des/der Lernenden.	Der Text wird online von einer anderen Person geschrieben (z.B. per Remote Control). Oder: Die oder der Lernende hat gleichzeitig weitere Online-Kanäle oder betrügerische Tools offen, die den Laptop resp. den Browser des/der Lernenden verlangsamen. Oder: Der/die Lernende streamt sein Prüfungsfenster per Internet an eine andere Ressource, um über einen anderen Weg per Internet illegale Unterstützung zu erhalten.
Der/die Lernende hat neben dem Browser mit Exam.net noch weitere Fenster geöffnet.	Der/die Lernende umgeht den Hochsicherheitsmodus und nutzt andere Programme/Dateien/Kanäle während der Prüfung.
Der/die Lernende befindet sich nicht im Hochsicher-	Verdacht: Der/die Lernende verwen-

heitsmodus, obwohl dieser Modus für die Prüfung auf Exam.net festgesetzt wurde. 10:57 Der Test wurde geladen Sicherheitsmodus: Hoch Gerät: macOS (Exam.net app 2.0.9) IP-Adresse: 213.144.154.242 <i>Im Überwachung-Fenster von Exam.net kann der Sicherheitsmodus bei jedem/jeder Lernenden überprüft werden.</i>	det ein Hacking-Tool, mit dem der Hochsicherheitsmodus umgangen werden kann (für diverse Betrugsoperationen).
Der/die Lernende wechselt zwischen verschiedenen Fenstern und/oder Desktop-Oberflächen.	Der/die Lernende verwendet einen virtual Desktop, ein Splitscreen-Programm, eine virtual Machine (VM) oder ähnliche Tools. So kann er/sie zwischen der «Oberfläche» von Exam.net im Hochsicherheitsmodus und einer anderen «Oberfläche» mit freiem Zugriff auf Programme, Dateien und Internet (inkl. KI-Tools) hin und her wechseln.
Der/die Lernende interagiert während der Prüfung mit Technik-«Gadgets» wie zum Beispiel einem «Cheating-Stift», einem Smartphone, einer Smartwatch, einem versteckten Knochenschall-Kopfhörer, einem versteckten Mini-Ohrstecker oder einer «digitalen» Brille (z.B. Google Lens).	Der/die Lernende nutzt «digitale Spickzettel» (gespeicherte Notizen) oder Online/KI-Funktionen.
Der während der digitalen Prüfung entstehende Text zeigt ein Schreibmuster, das nicht einer kontinuierlichen manuellen Texterstellung entspricht. Insbesondere treten Textzuwächse von erheblichem Umfang (z. B. mehr als 120 Wörter) innerhalb sehr kurzer Zeitintervalle (z. B. innerhalb 3 Minuten) auf, ohne dass eine entsprechende Bearbeitungsaktivität nachvollziehbar ist.	Der Text stammt nicht vollständig von dem/der Lernenden, sondern wird mittels externer Hilfe (z.B. textgenerierende KI oder Ghostwriter) produziert.
Die IP des/der Lernenden zeigt Auffälligkeiten: Üblicherweise haben alle Lernenden innerhalb des Schul-WLANs die gleiche IP-Adresse. Diese ist z.B. in Exam.net in dem Überwachung-Fenster einsehbar. 10:57 Der Test wurde geladen Sicherheitsmodus: Hoch Gerät: macOS (Exam.net app 2.0.9) IP-Adresse: 213.144.154.242 <i>Im Überwachung-Fenster von Exam.net kann die IP bei jedem/jeder Lernenden überprüft werden.</i>	Der/die Lernende hat sich nicht mit dem Schul-WLAN, sondern mit einem alternativen Netzwerk verbunden (z.B. Hotspot), um das System besser manipulieren zu können resp. auf Internet-Inhalte zugreifen zu können.
Der/die Lernende verwendet eine veraltete Version des SEB (Windows) oder der Exam.net-App (Mac), obwohl vorab kontrolliert wurde, dass die neueste Version installiert worden ist.	Der/die Lernende hat bewusst die neueste Version deinstalliert und eine veraltete Version installiert, mutmasslich um Sicherheitslücken für Betrug



Exam.net blendet in dem Überwachung-Fenster beim / bei der jeweiligen Lernenden ein oranges Fenster ein, wenn eine veraltete SEB/Exam.net-Version verwendet wird. Die genaue Version kann im Überwachung-Fenster bei jeder/jedem Lernenden überprüft werden.

10:57 Der Test wurde geladen
 Sicherheitsmodus: Hoch
 Gerät: Windows (SEB 3.10.0)
 IP-Adresse: 213.144.154.242

auszunutzen.

IV Vorschlag für Protokoll im Falle eines Betrugsverdachts

Dokumentationsraster – Verdacht auf Betrug in digitalen Prüfungen

Datum / Uhrzeit	
Prüfungsfach	
Raum	
Aufsicht	
Beobachtetes Verhalten	
Screenshot / Fotos	☐ Ja ☐ Nein (Bezeichnung: _____)
Aussagen Lernende*r	
Getroffene Massnahmen	

Entscheid (IT / SL)	IT: _____ SL: _____
Unterschriften	Lehrperson: _____ Lernende/Lernender: _____ IT/SL (falls erforderlich): _____