Behörde für Schule und Berufsbildung
IT-Infrastruktur Schule, BHZ, Dienststellen
Hamburger Straße 37
D – 22083 Hamburg

5. September 2018

Antrag auf ein PR-Benutzerkonto im FHHinfoNET

(bitte umgehend zurücksenden an die Fax Nr.: **4 279 66 – 154**)

Bitte beantworten Sie nachstehende Detailangaben in **Druckschrift:**

Benutzerangaben:

1. Ich arbeite an weiteren Schulen **ja** ☐ **nein** ☐

Wenn ja, wo noch? Schulname _____ Leitzeichen _____/_____

2. Schulwechsel **ja** ☐ **nein** ☐

Wenn ja: Leitzeichen vorher: _____/_____ Leitzeichen jetzt: _____/_____

Schulname _____

Leitzeichen _____/_____

Straße _____

PLZ / Ort _____

Name, Vorname _____

Diensttelefon Nr. _____

Fax-Nr. _____

Funktion _____

Raum Nr. _____

Dienstantritt am: _____

Vorgänger/in in der Funktion:

Name, Vorname _____

Benutzerkonto kann gelöscht werden **ja, sofort** ☐ **ja, am** __.__.____ ☐ **nein, weil …** ☐

Wenn **nein**, Begründung: _____

Hardware (wenn vorhanden):

Rechner: DSNR oder Gerät Serien-Nr.: _____

Drucker: DSNR oder Gerät Serien-Nr.: _____

Monitor: DSNR oder Gerät Serien-Nr.: _____

_____ _____

Schulstempel Unterschrift neue/r Benutzer/in Unterschrift der PR-Vorsitzende/r

Hinweis: Bitte unterschreiben Sie auch die Rahmenbedingungen auf der dritten Seite!

Freie und Hansestadt Hamburg
Behörde für Schule und Berufsbildung

Stand 05.09.2018

Behörde für Schule und Berufsbildung
IT-Infrastruktur Schule, BHZ, Dienststellen
Hamburger Straße 37
D – 22083 Hamburg

Rahmenbedingungen für die Nutzung der Onlinedienste des FHHinfoNET

Vorbemerkung

Die installierten Bildschirmarbeitsplätze in den Verwaltungsbereichen der allgemein bildenden Schulen **sind in wenigen Ausnahmefällen** mit Disketten- und CD-Laufwerken, sowie nutzbaren USB Schnittstellen ausgestattet worden. Dadurch können die Schulen z. B. weitere Programme, die sie für ihre Arbeit benötigen, installieren oder Daten mit Dritten auch über Wechseldatenträger, z.B. CD, Diskette, USB-Speicherstick oder externe Speicherkarten austauschen. Mit diesen erweiterten Möglichkeiten ist eine höhere Verantwortung verbunden. Aufgrund der Einbindung der Geräte in das gesicherte FHHinfoNET könnte ein über einen Wechseldatenträger oder über das Internet eingeschleppter Computervirus das gesamte Stadtnetz und damit die Bildschirmarbeitsplätze von mehreren zehntausend Mitarbeiterinnen und Mitarbeitern lahm legen. Daher sind diese Rahmenbedingungen unbedingt einzuhalten!

Untersagung von Netzöffnungen

Das lokale Datennetz für die Schulverwaltung darf nicht mit dem pädagogischen Datennetz verknüpft werden. Es dürfen keine zusätzlichen Netzöffnungen vorgenommen werden. Daher ist z. B. die Verwendung von Modems, ISDN- oder UMTS-Karten nicht gestattet.

Antivirenprogramm

Das auf den Arbeitsplatzrechnern installierte Antivirenprogramm wird regelmäßig automatisch über das FHHinfoNET aktualisiert. Das Antivirenprogramm darf zu keinem Zeitpunkt deaktiviert werden, da jeder Wechseldatenträger automatisch auf Computerviren geprüft wird. Diese Prüfung darf nicht unterbrochen werden.

Sollte ein Computervirus auf einem Wechseldatenträger festgestellt werden, der vom Antivirenprogramm nicht entfernt werden kann, darf dieser Wechseldatenträger nicht mehr verwendet werden. In jedem Fall sind der Absender des Wechseldatenträgers und der User-Help-Desk (42846-3990) über das Auftreten eines Virus zu informieren.

Softwarelizenzen

Bei der auf den Arbeitsplatzrechnern installierten Software, handelt es sich um urheberrechtlich geschützte und lizenzierte Produkte, deren Vervielfältigung und Vertrieb grundsätzlich nicht gestattet ist.

Für Software, die durch die Schulen zusätzlich installiert wird, muss ein Lizenznachweis in der Schule vorliegen.

ESARI

Sämtliche Veränderungen im Hardwarebereich müssen der Abteilung V-112 mitgeteilt werden. Nicht gemeldete Veränderungen werden bei der Umstellung auf ESARI nicht berücksichtigt.

Vergessenes Passwort

Für den Fall, dass ein persönliches Passwort vergessen wurde, ist die Nutzung des Arbeitsplatzrechners zunächst nicht mehr möglich.
Ablauf: Bitte wenden Sie sich in diesem Fall an den UHD von Dataport unter 42846-3990 und machen dort ein Ticket auf. Das Passwort kann nur zentral durch das Sachgebiet V114 zurückgesetzt werden. Im Anschluss werden Sie telefonisch kontaktiert. Zur Authentifizierung wird im Sachgebiet V114 ihre Einverständnisunterschrift hinterlegt.
Bitte nutzen Sie auch den **Passwort-Self-Service**: https://wakpssweb.fhhnet.stadt.hamburg.de/

Datenschutz und Datensicherheit

Unbeschadet der Verantwortung der Dienststellenleitung im Rahmen der Dienst- und Fachaufsicht obliegt **jeder Anwenderin und jedem Anwender** die Einhaltung der einschlägigen Bestimmungen. Dazu gehören u. a. das Hamburgische Datenschutzgesetz (HmbDSG) und die Verordnung über die Verarbeitung personenbezogener Daten in den Schulen (Schul-Datenschutzverordnung). Die entsprechenden Informationen stehen ihnen auch im Unterordner

W:\Transfer_Schulen\Informationen_Schulbehörde

auf den Arbeitsplatzrechnern zur Verfügung.

Die geltende Richtlinie zur Verwaltung von Passwörtern (Passwort-RL) vom 01.03.2007 finden Sie in dem o.a. Verzeichnis und können dort nachgelesen werden.
Schulleitungen werden noch einmal auf die mit der Auslieferung der Geräte gesondert übermittelten Handreichungen zur äußeren Datensicherung und zur Systemadministration hingewiesen.

Einverständnis

Ich habe die vorstehenden Rahmenbedingungen gelesen und akzeptiert.

	_____	_____	_____
Schulstempel-/ Dienststellenstempel	Datum	Name,Vorname (Druckschrift)	Unterschrift

Checkliste: „IT-Sicherheit am Arbeitsplatz“

Persönliche Accounts

- Jeder Mitarbeiter/in der Behördenzentrale und im Verwaltungsbereich der Schulen erhält für die Dienstgeschäfte einen Benutzeraccount. Dieser setzt sich zusammen aus Vorname, Nachname, der Dienststelle BSB (alternativ HIBB oder IfBQ) und Hamburg.de. Mit diesem Account erhalten Sie die Benutzerkennung zum Zugang zum Intranet und Internet, sowie zu allen gängigen Windowsprogrammen. Hinzu kommen die jeweils benötigten speziellen Programme für Ihren Arbeitsplatz.
- Dieser personifizierte Account mit dem dazugehörigen Passwort darf nur von dem Mitarbeiter/in genutzt werden, dem dieser zugeordnet wurde. Das Passwort sollten nur Sie selbst kennen und es darf aus datenschutzrechtlichen Gründen nicht weitergegeben werden.
- Es ist nicht zulässig, dass sich eine andere Person mit Ihrem Account am PC anmeldet und arbeitet.

Verantwortungsvoller Umgang mit Passwörtern

- Notieren Sie Ihre Passwörter keinesfalls auf Zetteln oder Post-its am Monitor, auch nicht an vermeintlich diskreten Stellen wie unter der Tastatur.
- Tragen Sie Sorge dafür, dass Sie bei der Eingabe Ihres Passworts nicht beobachtet werden.
- Nutzen Sie für jedes Gerät und jede Anwendung jeweils verschiedene Passwörter und wechseln Sie diese in regelmäßigen Abständen.
- Falls Sie Ihre Passwörter selbst festlegen können und diese nicht durch die IT-Abteilung vorgegeben werden, wählen Sie ein möglichst sicheres Passwort, das sich nicht leicht erraten lässt – also nicht Ihren Geburtstag oder den Namen Ihres Kindes oder Haustiers.

E-Mails kritisch prüfen

- Damit Sie nicht in die Falle tappen, sollten Sie sich Zeit für den 3-Sekunden-Sicherheits-Check nehmen: Prüfen Sie Absender, Betreff und Anhang vor dem Anklicken.
- Bei E-Mails von externen Kontakten, aber ebenso von „Kollegen und Kolleginnen“, sowie der Führungsebene, vorsichtig sein, da Urheber von Phishing-Mails seriöse Absender immer besser nachahmen.

Einverständnis
Ich habe die Checkliste gelesen und akzeptiert.

_____	_____	_____	_____
Schulstempel-/ Dienststellenstempel	Datum	Name,Vorname (Druckschrift)	Unterschrift