ДЕТСКА ГРАДИНА № 68 "Ран Босилек" – София,
Люлин VII, ул. "Ив. и Ст. Параскевови №5" ,тел. 02/825-72-40 , 02/925-01-67,
e-mail : odz68@abv.bg, www.dg68-ranbosilek.com

Вътрешни правила по мрежова и информационна сигурност за служителите

1. Цел и обхват

Настоящите правила уреждат как служителите и другите ползватели използват компютри, лаптопи, потребителски профили, училищна мрежа, интернет, електронна поща, облачни системи, принтери, сменяеми носители и други ИКТ ресурси.

Правилата са написани така, че да бъдат разбираеми за нетехнически ползватели, но остават задължителни и при работа с технически системи, когато това е необходимо за сигурността.

2. Общи задължения на всеки потребител

• всеки използва индивидуален профил и не предоставя паролата си на друго лице, дори когато това лице е колега или външен изпълнител;

• служебните устройства и акаунти се ползват само за служебни и образователни цели в рамките на възложените функции;

• не се допуска самоволно инсталиране на програми, разширения, приложения за отдалечен достъп или облачни услуги без разрешение;

• при съмнение за фишинг, злонамерен файл, загубено устройство, неочакван прозорец за вход или друга нередност се уведомява незабавно определеното лице или посоченият вътрешен канал;

3. Правила за профили, пароли и достъп

Достъп до системи и данни се предоставя само при служебна необходимост и по ред, който може да се проследи. Правата следва да съответстват на длъжността и реалните задачи на съответното лице.

• потребителските профили са лични; общи или споделени акаунти се избягват и се допускат само ако има особена необходимост и проследим ред;

• административни профили се използват само за административни дейности, а не за ежедневна работа;

• паролите трябва да са достатъчно силни, дълги и уникални; когато системата го позволява, за административни профили се изисква по-строг режим и не се допуска повторно използване на пароли;

• когато системата позволява, се използва многофакторна автентикация, особено за служебна поща, облачни услуги и отдалечен достъп;

• при напускане, преместване или промяна на длъжност достъпът се променя или прекратява без неоправдано забавяне.

4. Правила за работа с устройства и училищна мрежа

Служителите следва да използват предоставените им устройства внимателно и само по предназначение. Устройството не бива да се оставя без надзор в отключено състояние, когато около него има външни лица или ученици.

• екранът се заключва при напускане на работното място, дори за кратко време;

• не се допуска включване на неразрешени мрежови устройства, рутери, точки за достъп или суичове към училищната мрежа;

ДЕТСКА ГРАДИНА № 68 "Ран Босилек" – София,
Люлин VII, ул. "Ив. и Ст. Параскевови №5" ,тел. 02/825-72-40 , 02/925-01-67,
e-mail : odz68@abv.bg, www.dg68-ranbosilek.com

• промени по мрежовата конфигурация се правят само от упълномощени лица;

• служебната Wi-Fi мрежа не се споделя с неупълномощени лица, а достъпът за гости се използва само по определен ред;

• при повреда, нехарактерно поведение или подозрение за компрометиране на устройство се преустановява работата и се подава сигнал.

5. Електронна поща, интернет и обмен на файлове

• не се отварят подозрителни прикачени файлове, линкове или съобщения, които изискват спешно въвеждане на парола, код или банкови данни;

• служебната поща не се използва за незаконни, подвеждащи, обидни или несъвместими със служебните цели дейности;

• чувствителна информация не се изпраща чрез неофициални канали и не се качва в неразрешени облачни пространства;

• файлове с лични данни, оценки, служебни документи и записи се споделят само по разрешения ред и с минимално необходимия достъп;

• когато има съмнение дали даден имейл или линк е безопасен, съобщението не се отваря, а се препраща за проверка по вътрешния ред.

6. Работа от разстояние

Работа извън контролираната мрежа на детската градина се допуска само когато е необходима и когато има определен защитен ред. Целта е да не се допуска неоторизиран достъп до училищни системи от домашни или публични мрежи.

• отдалечен достъп се ползва само през одобрени защитени канали, например VPN или друго еквивалентно решение с удостоверяване, криптиране и проследимост;

• когато е приложимо, се използва най-малко двуфакторна автентикация;

• не се допуска използване на незащитени, неразрешени или непроверени механизми за отдалечен достъп;

• при дистанционна работа служителят следва да пази екрана и документите от видимост и достъп на неупълномощени лица.

7. Лични устройства, външни носители и печатни материали

• лични устройства се използват за достъп до училищни ресурси само ако това е изрично допуснато и при определени условия за сигурност;

• USB носители, външни дискове и други преносими носители се използват само ако са разрешени и проверени;

• разпечатани документи с чувствителна информация не се оставят без надзор върху бюра, принтери или общодостъпни места;

• при загуба, кражба или съмнение за компрометиране на устройство, носител или документ се уведомява незабавно определеното лице.

ДЕТСКА ГРАДИНА № 68 "Ран Босилек" – София,
Люлин VII, ул. "Ив. и Ст. Параскевови №5" ,тел. 02/825-72-40 , 02/925-01-67,
e-mail : odz68@abv.bg, www.dg68-ranbosilek.com

8. Поведение при инцидент или съмнение за инцидент

Служителят не е длъжен сам да доказва дали има инцидент. Достатъчно е да разпознае съмнителна ситуация и да я докладва незабавно.

• ако се подозира компрометиране на акаунт, паролата се сменя по указания ред и се уведомява отговорното лице;

• ако има съмнение за заразен файл или устройство, не се продължава работата и не се правят самоволни опити за ремонт;

• ако се касае за записи от видеонаблюдение, не се копират и не се изпращат неформално; действа се по вътрешния ред и с протокол;

• ако инцидентът е значим, ръководството решава заедно с определеното лице и техническия изпълнител каква е ескалацията.

9. Потвърждение

Всеки служител или друг ползвател потвърждава запознаването си с настоящите правила чрез подпис или друг проследим електронен механизъм.

Утвърждавам:.....

Директор:.....

Дата:.15.09.2026г.