**Csillagkert Balatonarácsi Református Óvoda**
**OM szám: 203228**
**Székhely: 8230 Balatonfüred, Iskolalépcső u. 4.**

**☎: +36 20 268 2714**
**E-mail: csillagkertovoda.aracs@gmail.com**
**www. aracsiref.hu**

# Csillagkert Balatonarácsi Református Óvoda

## Adatbiztonsági Szabályzata

A Csillagkert Balatonarácsi Református Óvoda (továbbiakban együtt: Adatkezelő szerv) vezetője az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 25/A.§ (3) bekezdés rendelkezése alapján az adatbiztonság érdekében az alábbi szabályzatot alkotja meg, illetve az alábbi szabályzat alkalmazását rendeli el.

## 1. A szabályzat célja

A Szabályzat célja, hogy meghatározza az Adatkezelő szerv által folytatott adatkezelések működésének jogszerű rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését, valamint célja, hogy biztosítsa az érintettek személyes adatainak védelmét.

## 2. A Szabályzat hatálya

Jelen szabályzat **személyi hatálya** kiterjed az Adatkezelő szervnél foglalkoztatottakra, valamint a munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatottakra, továbbá azon személyekre, akik – munkatapasztalatszerzési, kutatási vagy képzési célból – szakmai gyakorlatukat az Adatkezelő szervnél töltik. (a továbbiakban együttesen: munkavállaló).
Jelen szabályzat **tárgyi hatálya** kiterjed az Adatkezelő szerv kezelésében lévő személyes adatok védelmére, kezelésére.

## 3. Fogalmak, értelmező rendelkezések

Az értelmező rendelkezések tekintetében az új általános adatvédelmi rendelet (továbbiakban: GDPR), valamint az Infotv. rendelkezései az irányadóak.

## 4. Személyes adatok védelme

### 4.1 Általános szabályok

A személyes adatok védelméért, az adatkezelés jogszerűségéért az Adatkezelő szerv törvényes képviselője (továbbiakban: Intézményvezetője) a felelős.
Az Adatkezelő szerv által kezelt személyes adatok védelméről az adatvédelemmel kapcsolatos szabályok foglalkoztatottak általi megismeréséről, és betartásáról az Adatkezelő szerv Intézményvezetője gondoskodik.
Az Adatkezelő felelős a személyes adatok szabályszerű kezelésének megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („elszámoltathatóság”).

### 4.2. Az előzetes tájékoztatás követelménye

Magyarország Alaptörvénye VI. cikk (3) bekezdésében foglaltak szerint mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez, azaz a rögzített személyes adatok védelméhez való jog egyik legfontosabb alkotmányos követelménye az, hogy „mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatkezelés egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát.”

Ezen alkotmányos követelmény az adatkezelés megkezdése előtt az előzetes tájékoztatáson keresztül érvényesülhet. Az érintett az előzetes, megfelelő tájékoztatás alapján képes felismerni azt, hogy az adott adatkezelés milyen hatással van az információs önrendelkezési jogára és a magánszférájára. Az érintettek a megfelelő tájékoztatáson keresztül ismerhetik meg a személyes adataikra vonatkozó adatkezelést, illetve ezáltal érvényesülhet az információs önrendelkezési joguk. A GDPR (39) preambulumbekezdés alapján a személyes adatok kezelésének jogszerűnek és tisztességesnek kell lennie. A természetes személyek számára átláthatónak kell lennie, hogy a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, azokba, hogy tekintenek bele vagy milyen egyéb módon kezelik, valamint azzal összefüggésben, hogy a személyes adatokat milyen mértékben kezelik vagy fogják kezelni.

Az előzetes tájékoztatásra vonatkozó követelményeket a jogalkotó az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 16. §- abban is megfogalmazta.
Az előzetes, megfelelő tájékoztatás kötelezettségének központi elemét tehát tartalmazza a GDPR, valamint az Infotv., amely felsorolja azokat az alapvető adatkezelési körülményeket, amelyekről az adatkezelőnek tájékoztatást kell nyújtania.
Emellett az előzetes tájékoztatás vonatkozásában is jelentős szerepe van az Infotv. 4. § (1) bekezdés második mondatában megfogalmazott tisztességes adatkezelés alapelvének. Az adatok gyűjtésének és kezelésének tisztességessége az előzetes tájékoztatással összefüggésben az Infotv. 16. §-ában megfogalmazottakon túlmenően további követelmények érvényesülését jelenti. Az Infotv. 16. § (1)-(2) bekezdés alapján az előzetes tájékozódáshoz való jog érvényesülése érdekében az adatkezelő az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek megkezdését megelőzően vagy legkésőbb az első adatkezelési művelet megkezdését követően haladéktalanul az érintett rendelkezésére bocsátja:
a) az adatkezelő és - ha valamely adatkezelési műveletet adatfeldolgozó végez, az adatfeldolgozó - megnevezését és elérhetőségeit,
b) az adatvédelmi tisztviselő nevét és elérhetőségeit,
c) a tervezett adatkezelés célját, és
d) az érintettet a törvény alapján megillető jogok, valamint azok érvényesítése módjának ismertetését.

Az (1) bekezdésben foglaltakkal egyidejűleg, azzal azonos módon vagy az érintettnek címzetten az adatkezelő az érintett számára tájékoztatást nyújt:
a) az adatkezelés jogalapjáról,
b) a kezelt személyes adatok megőrzésének időtartamáról, ezen időtartam meghatározásának szempontjairól,
c) a kezelt személyes adatok továbbítása vagy tervezett továbbítása esetén az adattovábbítás címzettjeinek - ideértve a harmadik országbeli címzetteket és nemzetközi szervezeteket - köréről,
d) a kezelt személyes adatok gyűjtésének forrásáról, és
e) az adatkezelés körülményeivel összefüggő minden további érdemi tényről.

*Az általános adatvédelmi tájékoztató táblázatok formájában – az adatkezelési tevékenység nyilvántartási adatlapjait is bemutatva - foglalja össze az előzetes tájékoztatás kötelező tartalmi elemeit.*

### 4.3. Az adatvédelmi nyilvántartásba való bejelentési kötelezettség

A GDPR alkalmazása előtti időszakban az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény értelmében az adatkezelők bejelentései alapján az Adatvédelmi Hatóság nyilvántartást vezetett az érintettek tájékozódásának elősegítése érdekében, amelyben fel kellett tüntetni az adatkezelésre vonatkozó minden lényeges körülményt (így például az adatkezelés célját, jogalapját, időtartamát).
Ez a bejelentési kötelezettség 2018. május 25. napjától megszűnt, a GDPR ugyanis nem tartalmaz a tagállami felügyeleti hatóságok által vezetendő országos adatvédelmi nyilvántartásra vonatkozó szabályozást.
Ezen időpontot követően a GDPR 30. cikke alapján az adatkezelőknek (adatfeldolgozóknak) kell nyilvántartást vezetniük a saját adatkezelési tevékenységeikről a rendeletben írt tartalommal.

### 4.4 Adatbiztonsági rendszabályok

Az adatminőség biztosítása céljából személyes adatot csak az érintett személyének azonosítására alkalmas és érvényes hatósági igazolványból, különleges adatot az érintett írásos hozzájárulása szerint szabad felvenni. Az adatfelvétel és a további adatkezelés folyamán ügyelni kell a személyes adatok pontosságára, teljességére és időszerűségére, valamint azok védelmére, hogy emiatt az ügyfelek jogai ne sérülhessenek.
Az ügyiratba nem kerülő papíralapú fogalmazványban rögzített személyes és különleges adatokat – további felhasználásuk megakadályozása érdekében – azonosításra alkalmatlanná kell tenni. A számítástechnikai eljárás során keletkezett munkapéldánnyal, illetőleg rontott vagy egyéb okból feleslegessé vált példányokkal - további felhasználásuk megakadályozása érdekében – azonosításra alkalmatlanná kell tenni. Az ügyintézőnél vagy az irattárban lévő iratba az ügyintéző munkavállalón kívül más személy csak akkor tekinthet be, ha ezt jogszabály lehetővé, vagy a munkaköri tevékenységével összefüggő feladatellátás szükségessé teszi.
Az érintett vagy meghatalmazott képviselője betekintési jogának gyakorlása során úgy kell eljárni, hogy ez által mások jogai ne sérülhessenek (a más személyre vonatkozó személyes, vagy védett adatokat adott esetben ki kell takarni vagy más módon felismerhetetlenné tenni). Ugyanígy kell eljárni a másolat, kivonat készítésekor is.
Az Adatkezelő szerv munkavállalója a nála lévő, személyes adatnak minősülő adatokat tartalmazó iratokat köteles munkaidőn túl – és amelyeket lehetséges munkaidőben is – zárható szekrényébe elzárva tartani, az asztalon és az irodában egyéb helyen hivatalos iratok csak a munkavégzés céljából és annak tartama alatt, más iratoktól elkülönítve tárolhatók. Az iratok elzárásáért az a munkavállaló a felelős, akinél azok a munkaidő befejezésekor találhatók**.**
Az egyéb szempontokon túl adatvédelmi megfontolásból azokat a helyiségeket, ahol közös használatú nyomtató vagy másológép üzemel, az adatbiztonsági követelmények figyelembevételével kell használni.
Az egyéb szempontokon túl adatvédelmi megfontolásból azokat a szobákat, helyiségeket, ahol számítógép, munkaállomás üzemel, úgy kell használni, hogy az megfeleljen az adatvédelmi, tűzrendészeti és informatikai biztonsági követelményeknek.
A munkavállaló köteles a számítógépet és az ahhoz alkalmazott adathordozókat úgy kezelni, tárolni, hogy - az informatikai biztonsági szabályok *(Különösen, de nem kizárólagosan az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra*

*vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet)* figyelembe vételével - a védelmet igénylő adatokat illetéktelen személy ne ismerhesse meg. Köteles továbbá a munkaidő végeztével a munkaállomást kikapcsolni, az ajtót bezárni. A tűzrendészeti előírásokat be kell tartani, az Adatkezelő szerv Tűzvédelmi Szabályzata alapján.
Személyes adatokat is tartalmazó iratot az Adatkezelő szerv hivatalos helységéből kivinni – munkaköri feladat ellátásának kivételével – csak a közvetlen felettes vezető engedélyével lehet. Az ügyintéző ez esetben is köteles gondoskodni arról, hogy az ne vesszen el, ne rongálódjon vagy semmisüljön meg és tartalma illetéktelen személy tudomására ne jusson.

A célhoz nem kötött és olyan adatokat, amelyekre nézve az adatkezelés célja megszűnt vagy módosult – eltérő rendelkezés hiányában az Adatkezelő szerv Iratkezelési Szabályzatában foglaltakkal összhangban – haladéktalanul, illetve az előírt megőrzési határidő leteltével meg kell semmisíteni. A személyes adatokat tartalmazó egyéb iratanyagok megsemmisítéséről szintén a szükséges biztonsági intézkedések mellett kell gondoskodni. A számítógépen rögzített adatokat, ha céljukat betöltötték – további felhasználásuk megakadályozása érdekében – felismerhetetlenné kell tenni.
Az adattörlés maradéktalan megvalósítása érdekében az ügyintézőnek kellő gondossággal, pontosan kell meghatározni az irattározásra kerülő anyagok selejtezési idejét megjelölő irattári tételszámot az Irattári Terv alapján. Az egyes nyilvántartások (természetes személy foglalkoztatott, ügyfél/kérelmező/ellátott, hozzátartozó, jogi személy kapcsolattartója) adatkezelések tekintetében a hozzáférési jogosultságot az Adatkezelő szerv vezetőjének személyre lebontottan meg kell határoznia, és az időszerű állapotnak megfelelő nyilvántartásukról gondoskodnia kell. A foglalkoztatási jogviszony megszűnése/megszüntetése esetén a munkakör átadás-átvételi szabályok alapján kell gondoskodni a munkakörhöz kapcsolódó adatok további kezeléséről, védelméről.

### 4.5 Adattovábbítás, az adatkezelések összekapcsolása

A személyes adatokat továbbítani, vagy adatszolgáltatást teljesíteni, illetőleg a különböző adatkezeléseket összekapcsolni csak akkor lehet, ha ahhoz az érintett hozzájárult, vagy jogszabály ezt előírja, illetve megengedi és az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek.
Az adattovábbítást regisztrálni kell (adattovábbítási nyilvántartás), annak érdekében, hogy megállapítható legyen milyen adat, kinek, milyen felhatalmazottság alapján, mikor került továbbításra vagy kiszolgáltatásra (pl. belföldi jogsegély, stb.).
Az adattovábbításról vezetett nyilvántartást – eltérő jogszabályi rendelkezés hiányában – személyes adatok esetében minimum 5 évig, különleges adatok vonatkozásában pedig minimum 20 évig kell megőrizni. Hiányos adatkérés esetén a hiány pótlására kell felkérni az adatkérőt. Nem kell hiánypótlást kérni, ha az adatkérés jogalapja, az adatszolgáltatás adattartalma e nélkül is megállapítható. Abban az esetben, ha az adattovábbítást nem lehet jogszerűen teljesíteni, vagy az igény elbírálásához szükséges információkat az igénylő a felkérést követően sem jelölte meg, úgy – eltérő rendelkezés hiányában - az adattovábbítást meg kell tagadni. Az adattovábbítás megtagadásáról – annak indokolásával együtt – írásban kell értesíteni az igénylőt. Az érintettet az adattovábbításra vonatkozó jogszabályi felhatalmazás hiányában nyilatkoztatni kell – különleges adatai tekintetében írásban – a kérelmére indult eljárásban, hogy hozzájárul-e személyes adatainak a továbbításához, ha ügye elintézéséhez más szerv megkeresése szükséges.

### 4.6 Az érintett jogai

Az érintett az Infotv. 14. § rendelkezései alapján jogosult arra, hogy az adatkezelő és az annak megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatai vonatkozásában az Infotv-ben meghatározott feltételek szerint:
a) az adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően tájékoztatást kapjon (a továbbiakban: előzetes tájékozódáshoz való jog),
b) kérelmére személyes adatait és az azok kezelésével összefüggő információkat az adatkezelő a rendelkezésére bocsássa (a továbbiakban: hozzáféréshez való jog),
c) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatait az adatkezelő helyesbítse, illetve kiegészítse (a továbbiakban: helyesbítéshez való jog),
d) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatai kezelését az adatkezelő korlátozza (a továbbiakban: az adatkezelés korlátozásához való jog),
e) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatait az adatkezelő törölje (a továbbiakban: törléshez való jog).

### 4.7 Adatvédelem szervezete

A Szabályzat személyi hatálya alá tartozó munkavállalók a munkaköri leírásra, az Adatkezelővel megkötött szerződésekre tekintettel a GDPR, az Infotv. és az Adatkezelő szerv feladat- és hatáskörébe tartozó ügyek intézésére irányadó jogszabályok, valamint jelen és más Szabályzat adatvédelmi előírásait köteles maradéktalanul betartani.
Azonnali tájékoztatási kötelezettségük van az Adatkezelő szerv Intézményvezetője felé, ha feladatkörükben felmerül bármely adatvédelmi probléma. Észrevétel esetén az adatkezeléssel kapcsolatosan feltárt visszásságot haladéktalanul kötelesek megszüntetni.
Az Adatkezelő szerv Intézményvezetője biztosítja, hogy e Szabályzat hatálya alá tartozó személyek betartsák az adatkezelésre vonatkozó jogszabályok, valamint jelen és más Szabályzat vonatkozó rendelkezéseit, valamint vezeti az adatvédelmi nyilvántartást.

### 4.8. Az Adatkezelő munkahelyi adatkezelés általános adatvédelmi szabályzata különösen az alábbi olyan függeléket tartalmazza, amelyeket jelen szabályzattal együtt kell alkalmazni:

- adatkezelési tevékenység nyilvántartásai és általános adatvédelmi tájékoztató,
- megbízási szerződés adatfeldolgozásra - adatvédelmi tisztviselő megbízása,
- kapcsolattartó hozzájáruló nyilatkozata,
- a szervezeten belüli, a munkáltató jogos érdekén alapuló adatkezeléssel kapcsolatos gyakorlat és érdekmérlegelési teszt,
- hatásvizsgálat és kockázatbecslés.

## 5. Online adatkezelés során a személyes adatok védelme

### 5.1. Azonosítás és feljogosítás az informatikai rendszer használatára

A felhasználó az informatikai rendszert csak egyértelmű azonosítást követően, a számára meghatározott és biztosított jogosultságok keretei között használhatja. Az informatikai rendszer használata során a felhasználók egyértelmű azonosítását folyamatosan biztosítani kell. Minden felhasználót kizárólagos személyi használatú egyedi azonosítóval kell ellátni, amelyhez minimálisan egyedi jelszót kell rendelni. További azonosítási lehetőségek is elfogadottak, amelyek az elektronikus információs rendszer biztonságáért felelős Fenntartó által biztosított rendszergazda személy engedélyével vezethetők be.

A felhasználók azonosítójának a felhasználói nevet tartalmaznia kell. Kivételt képeznek az operációs rendszerek különleges, előre rögzített azonosítói és a különleges informatikai feladatkört ellátók által használt speciális és teszt, vagy szerviz felhasználói nevek. A felhasználói névben törekedni kell a családi és utónév használatára, névazonosság esetén harmadik név vagy emelkedő számozás szolgáljon a felhasználói nevek megkülönböztetésére.

A felhasználói jelszónak legalább az alábbi követelményeket teljesítenie kell:

a) a felhasználói jelszavak legalább 6 karakter hosszúságúak lehetnek,

b) a jelszavak tartalmazzanak legalább egy kis-, és egy nagybetűt, valamint egy számot,

c) a jelszavak nem lehetnek személynevek, szótárban megtalálható szavak, felhasználói azonosítók, nem tartalmazhatnak könnyen kitalálható, ismétlődő karaktersorozatot,

d) nem utalhat a felhasználó személyére,

e) a jelszavakat legalább 90 naponta cserélni kell,

f) nem lehet jelszó az utolsóként használt 12 jelszó egyike sem,

g) maximum 5 téves próbálkozás után a fiókot, munkaállomást zárolni kell 15 perc időtartamra.

A jelszó megváltoztatása kötelező:

a) a felhasználói azonosító informatikai rendszerbe történt felvételét követő első bejelentkezéskor,

b) az informatikai üzemeltető szervezeti egység munkatársa általi újbóli jelszóbeállítást, felülírást követően,

c) ha a jelszó illetéktelen személy tudomására juthatott vagy bármilyen módon nyilvánosságra kerülhetett,

d) az érvényességi idő lejártakor.

A felhasználó köteles a jelszót bizalmasan őrizni, illetéktelenek általi megismerését kizárni.

Tilos a jelszót más által megismerhető módon feljegyezni, azt mással bármilyen formában közölni.

Az Intézményvezető felel azért, hogy a felhasználók kizárólag a vezetőjük által igényelt és megjelölt informatikai jogosultsággal rendelkezzenek. Szükség esetén gondoskodnia kell a jogosultság törléséről.

A felhasználót, annak vezetőjét a felhasználó élesített jogosultságairól, illetve azok részleges vagy teljes megszűnéséről e-mailben tájékoztatni kell. A tájékoztatási kötelezettség a jogosultság technikai beállítóját terheli.

### 5.2. Szoftverek telepítése, internethasználat

A munkaállomás csak a felhasználó hivatali feladatainak ellátása miatt kapcsolható össze az

internettel. Hálózathoz csatlakozó munkaállomásokról csak központilag biztosított vírus- és kártékony kód elleni védelemmel, szűrési és forgalom ellenőrzési eszközzel ellátott rendszeren keresztül érhető el az internet.

A hálózathoz csatlakozó munkaállomásra csak a munkavégzéshez szükséges adatállományok, programok tölthetők le, illetve telepíthetők.

A hálózathoz csatlakozó munkaállomásra nem telepíthető, nem másolható – ideiglenesen sem –, illetve a belső hálózaton nem tehető közzé olyan adatállomány, információ, amely

a) jogszabályt sért, így különösen adatvédelmi, szerzői jogvédelmi, személyiségvédelmi előírásba ütközik,

b) a hálózat rendeltetésszerű működését, biztonságát veszélyezteti vagy veszélyeztetheti, így különösen annak erőforrásait indokolatlanul, vagy szándékosan túlzott mértékben, pazarló módon veszi igénybe.

Az internet felhasználása csak az óvoda ügymenete érdekének megfelelően kialakított és betartott szabályok alapján történhet.

Az internet-szolgáltatás minőségének szinten tartása és az óvoda érdekeinek biztosítása céljából – az elektronikus információs rendszer biztonságáért felelős külső rendszergazda javaslatára vagy engedélyével – korlátozásokkal élhet. A korlátozások a következőkre terjedhetnek ki:

a) bizonyos fájl-típusok letöltésének korlátozása,

b) az alapvető etikai normákat sértő oldalak látogatásának tiltása,

c) a látogatható weboldalak körének behatárolása és a maximális fájl-letöltési méret korlátozása.

Az Intézményvezető – amennyiben ezt indokoltnak tartja – az óvoda munkatársainak, egyes felhasználó(k) internet-hozzáférésének letiltását kezdeményezheti az elektronikus információs rendszer biztonságáért felelős rendszergazdánál. A felhasználók csak az elektronikus információs rendszer biztonságáért felelős külső rendszergazda által ismert és a biztosított internet kijáratokon keresztül csatlakozhatnak az internethez. Bármely egyéb módon történő internetelérés létesítése az azt kialakító felhasználó felelősségre vonását eredményezi.

Felhasználók internethasználatára vonatkozó általános szabályok:

a) csak a munkavégzéshez, szakmai tájékozottság bővítéséhez szükséges vagy általános tájékozottságot biztosító információt, segítséget nyújtó oldalak látogathatók,

b) tilos a jó ízlést, közerkölcsöt sértő, rasszista, uszító és más, a véleménynyilvánítás kereteit meghaladó oldalak szándékos látogatása, online játékok, fogadási oldalak felkeresése, bármely tartalommal kapcsolatos magánvélemény kinyilvánítása (pl. privát blog és chat),

c) a felhasználók nem tölthetnek fel egyénileg – a felelős jóváhagyása nélkül – az óvodai kapcsolatos adatot az internetre,

d) az internetről csak a munkavégzéshez szükséges adatállományok, táblázatok, tölthetők le, alkalmazások, programok nem,

e) a látogatott oldal nem szokványos működése (pl.: folyamatos újratöltődés, kilépés megtagadása, ismeretlen oldalak látogatására történő kényszerítés, ismeretlen program futásának észlelése, stb.) esetén a külső rendszergazda segítségét kell kérni.

### 5.3. Elektronikus levelezőrendszer használata

Az Óvoda feladatainak végrehajtásához alkalmazott elektronikus levelezésben kizárólag a óvodai levelezési cím használható.

Az Óvodai egyházi szolgálati jogviszonyban vagy munkaviszonyban álló személy kaphat levelezési címet, személyes postafiókot. Külsős munkavállaló esetén az Intézményvezetője egyedi elbírálás alapján postafiók beállítást igényelhet.

A levelezőrendszerek használata során a vírusvédelmi előírásokat folyamatosan érvényesíteni kell.

A levelezőrendszeren kizárólag munkacélú üzenetek továbbíthatók. Magáncélú üzenetet nem nevesített felhasználóknak (pl. csoport, mindenki) küldeni tilos! Magáncélú levelezés tilos!

Az elektronikus levelezés biztonságának, működőképességének, stabilitásának és rendelkezésre állásának biztosítása a Fenntartó által biztosított külső rendszergazda feladata.

### 5.4. Az adathordozók kezelése és biztonsága

Az adatok sérülésének elkerülése és a működésfolytonosság fenntartása érdekében az Intézményvezető és az információbiztonsági felelős külső rendszergazda, eljárásokat hoz létre, az elektronikus dokumentumokhoz, számítógép médiumokhoz, adathordozókhoz történő jogosulatlan hozzáférés, módosítás, ellopás megakadályozása érdekében.

### 5.5. Az eltávolítható adathordozók kezelése

A hordozható adathordozók – más terminológia szerint eltávolítható adathordozók – jellegükből adódóan jelentős információbiztonsági kockázatot hordoznak.
Az eltávolítható adathordozók közé tartoznak az adatkazetták, CD-k, DVD-k, külső merevlemezek, pendrive-ok, de ebbe a kategóriába kell sorolni hozzáférhetőségük és felépítésük miatt a mobiltelefonok és fényképezőgépek memóriáját is. (Általában használatos még az „USB mass storage" elnevezés is.)
A legnagyobb veszélyt az eltávolítható adathordozók jogosulatlan használata jelenti. Az óvoda hálózatához ilyen eszközt kapcsolva fennáll a rosszindulatú kódok (vírusok) bejutásának veszélye, másrészről pedig fennáll az adatok jogosulatlan elvitelének veszélye, ezért az egyházi szolgálati jogviszonyba dolgozók saját **eltávolítható adathordozóikat külön feljogosítás nélkül a hálózathoz nem csatlakoztathatják!**

### 5.6. Az eltávolítható adathordozókkal kapcsolatos irányelvek

Az eltávolítható adathordozókkal kapcsolatos irányelvek a következők:

a) bizalmas információ, személyes vagy különleges adatok csak titkosítva írható fel rájuk;
b) biztosítani kell hardver titkosítással ellátott pendrive-okat azon munkatársak számára, akiknek munkájához indokolt;
c) a titkosítatlan optikai adathordozókat, amennyiben már nem szükségesek, helyreállíthatatlanul fizikailag meg kell semmisíteni;
d) a megőrzendő adatok esetében figyelembe kell venni az eszköz várható élettartamát és ennek megfelelően időközönként át kell másolni az adatokat vagy több helyen kell azokat tárolni.

### 5.7. Adathordozók újrahasznosítása és selejtezése

Az adathordozók újrahasznosítása és selejtezése során, az adatok kiszivárgásának megakadályozására, a Gazdasági vezető/Óvodatitkár az alábbi utasításokat betartva jár el:

a) A már szükségtelenné vált adatot tartalmazó, de újrafelhasználható adathordozókat – tipikusan munkaállomások, laptopok merevlemezei, új felhasználóhoz történő kiadásuk előtt –szokásos formázási vagy törlési eljárással törli, majd az eszközt újra használatba adja. Ez kizárólag a szervezeten belül történő újrafelhasználás esetén érvényes,

b) A használaton kívüli adathordozókat osztályozza aszerint, hogy tartalmaznak-e érzékeny adatot. Amennyiben ez nem megállapítható, akkor az adathordozót úgy kezeli, mint ami érzékeny adatot tartalmaz,
c) Az érzékeny adatokat tartalmazó mágneses adathordozókat (merevlemezeket) le-mágnesezéssel vagy speciális felülírással törölteti a külső rendszergazdával,
d) Azokat az adathordozókat, amelyek már további használatra nem alkalmasak, selejtezi. A selejtezésre szánt adathordozókról jegyzőkönyvet vesz fel,
e) Valamennyi adathordozó típus esetén igénybe veheti a speciális, adatmegsemmisítéssel foglalkozó cégek szolgáltatását, amelyek bezúzással, vagy égetéssel, jegyzőkönyvezés mellett végzik a megsemmisítést,
f) A nem elektronikus – jellemzően papír alapú – adathordozók esetében is hasonlóan kell eljárni, a használatból kivont adathordozókat első sorban fizikailag kell megsemmisíteni a Szervezeti és Működési szabályzat 1. számú melléklet szerinti Egységes Iratkezelési Szabályzatban foglaltak szerint.

### 5.8. Az adathordozók tárolása és védelme

Az adathordozók tárolása és védelme érdekében az alábbi utasításokat kell követni:

a) Az adathordozókat a rajtuk lévő adatok érzékenységének megfelelően védeni kell, használaton kívül el kell zárni,
b) Adathordozó (adat) az óvoda területéről csak az Intézményvezető engedélyével lehetséges kivenni. Ez vonatkozik az adathordozókon történő kivitelre, vagy az egyéb, elektronikus úton történő továbbításra, mint az Internet vagy a (mobil)telefonos adattovábbítás.
c) Az óvodai infrastruktúrán (kiszolgálók, csoportkönyvtárak, fájl szerverek stb.) kívül például felhasználói munkaállomásokon, laptopokon csak olyan adatot szabad tárolni, melyek sérülése, elvesztése vagy illetéktelenek kezébe történő kerülése nem okozhat az óvoda számára kárt vagy bizalomvesztést. Az ilyen adatok nem kerülnek központi mentésre, ezért a mentési igényt minden esetben az Intézményvezető felé kell jelezni.
d) A személyi használatra kiadott laptopokon bizalmas információt csak titkosítva szabad tárolni.

## 6. Záró rendelkezések

E Szabályzat 2021.január 14. napján lép hatályba.

A Szabályzat elkészítésért és végrehajtásáért az Adatkezelő szerv Intézményvezetője a felelős.

Balatonfüred, 2021.január 11.

……
Szabadi Edit
Csillagkert Balatonarácsi Református Óvoda
Intézményvezetője

**Határozat**

1. A nevelőtestület az Adatbiztonsági Szabályzatot megismerte, az abban foglaltakkal egyetért.
2. Az alkalmazotti közösség többi tagjainak bevonásával jóváhagyta.

3. Határozat száma: 5 /2021. ( I.13.) Nevelőtestületi határozat.

Balatonfüred, 2021. január 13.

…….

Szabadi Edit
. intézményvezető

1. Jegyzőkönyv
2. Jelenléti ív