PALAU
DE LA
MÚSICA
ORFEÓ
CATALÀ

POLÍTICA D'ÚS D'EINES INFORMÀTIQUES, DISPOSITIUS TECNOLÒGICS I CONFIDENCIALITAT

Document	Política d'ús d'eines informàtiques, dispositius tecnològics i confidencialitat
Descripció	Establiment de normes d'actuació en l'ús d'eines informàtiques, dispositius tecnològics i en la informació confidencial. Complement del sistema de gestió de seguretat de la informació
Data inicial	Setembre 2024
Data revisió	A determinar
Finalitat	Establir normes d'ús de les eines informàtiques, dispositius tecnològics i de la informació confidencial. Complementar el sistema de gestió de seguretat de la informació
Classificació	Document intern

COMISSIÓ DE COMPLIMENT I GOVERNANÇA 2024

1. INTRODUCCIÓ

L'activitat de l'**Associació** de l'Orfeó Català i de la **Fundació** Orfeó Català-Palau de la Música Catalana (en endavant, les Institucions o bé l'Associació o la Fundació), respon a processos i accions a on es fa necessari l'ús d'eines informàtiques, dispositius tecnològics i informació confidencial. Fet aquest últim que impulsa la necessitat d'establir certes normes de d'actuació a totes dues Institucions que assegurin i guiïn el bon ús d'aquestes eines i informació impedint, així, un mal ús de les mateixes que pugui comportar l'assumpció de responsabilitats no només pels seus usuaris sinó també per l'Associació o la Fundació en el normal desenvolupament de les seves activitats.

L'era digital en la que ens trobem fa que cada vegada més ens veiem impulsats a la necessitat d'emprar, en ús propi o bé en col·laboració amb tercers, mitjans tecnològics (ex. Digitalització de processos, softwares o ordinadors) mitjançant estructures de sistemes d'informació, terminals i informació confidencial l'ús correcte dels quals es torna imprescindible. Alguns exemples de conductes que han de ser evitades en l'ús d'aquestes eines poden ser la intrusió i accés a correus electrònics, la vulneració de la llei de protecció de dades personals, el cobrament d'imports indeguts o l'espionatge industrial. Així mateix, resulta imprescindible que els usuaris d'aquests mitjans siguin també conscients dels riscos existents en el seu ús com, per exemple, els derivats dels virus, programaris espies, forats se seguretat etc. que poden posar en risc la informació de les Institucions, la privacitat de les dades i el correcte funcionament dels equips i de les xarxes.

2. OBJECTE

Tant l'Associació com la Fundació són unes Institucions que han de gestionar-se de manera transparent, eficient i honrada d'acord amb les finalitats fundacionals i els valors institucionals que representen. Aquestes finalitats fundacionals són portades a terme, entre d'altres, mitjançant processos a on són necessaris els ordinadors, telèfons mòbils, tablets, sistemes etc. Motiu pel qual es crea aquesta Política a través de la qual s'estableixen normes d'actuació i supervisió la finalitat de les quals és assegurar un bon ús de tots aquests equips. Al propi temps, mitjançant la present Política s'estableixen també les normes a seguir per garantir un ús correcte en el tractament de la informació confidencial de les Institucions o bé de tercers per part de tots els subjectes a qui es dirigeix aquesta Política. Es tracta de transmetre cultura de seguretat i vies d'actuació en ciberseguretat.

A aquests efectes, la present Política estableix deures de diligència que hauran de ser observats pel personal, òrgans directius i demés usuaris de mitjans tecnològics de les Institucions i, segons el cas, per tercers, vetllant, així, per a què ni l'Associació ni la Fundació cometin o bé siguin emprades per a la comissió de conductes que puguin suposar actes contraris a les normes legals o internes d'aplicació a les mateixes.

Així mateix la present Política ha estat redactada amb el propòsit de respectar, entre d'altres, el conveni laboral propi de la Fundació així com els drets laborals i drets fonamentals dels que són titulars els subjectes a qui va dirigida.

3. ÀMBIT SUBJECTIU i OBJECTIU

3.1- Aquesta Política serà d'aplicació a tots els membres de la Junta Directiva de l'Associació, a tots els membres del Patronat de la Fundació així com als seus treballadors durant la relació laboral que ostentin i fins que aquesta finalitzi (sens perjudici de les concrecions exposades més endavant). Serà exigible també, mitjançant compromisos contractuals, als tercers que es puguin veure afectats pel seu contingut així com a aquelles persones que, per la seva vinculació amb les Institucions, també fan ús de les eines informàtiques o dispositius tecnològics de les mateixes (ex. Cantaires o col·laboradors habituals). Tots ells, d'ara en endavant, seran mencionats com els ***usuaris***.

3.2 - El seu àmbit objectiu són tots els processos i activitats, en sentit general, que poden ser desenvolupats per totes dues Institucions, tant en l'àmbit públic com en el privat, així com a qualsevol àmbit geogràfic tant local, com nacional o internacional; quan aquests requereixin l'ús d'eines informàtiques, dispositius tecnològics o sistemes d'informació en un sentit ampli així com informació confidencial tant pròpia com de tercers a la que es pugui tenir accés.

4. PRINCIPIS D'ACTUACIÓ GENERALS

Les Institucions i els seus usuaris aplicaran l'observança dels següents principis rectors a fi de realitzar un ús correcte de les eines informàtiques, dispositius tecnològics així com de la informació confidencial que puguin tractar en el desenvolupament de les seves normals activitats:

- Transparència i comunicació: Desenvoluparan tota actuació pròpia de manera transparent i comunicada a l'òrgan que correspongui en el seu cas;
- Ús responsable dels equips: Tots els usuaris dels sistemes d'informació i eines informàtiques i dispositius tecnològics faran un ús responsable i raonable dels mateixos;
- Documentació: Procedimentaran i documentaran tots els processos de les Institucions vinculats amb l'ús d'eines informàtiques i dispositius tecnològics o informació confidencial, de manera que sempre siguin aplicats de la mateixa manera evitant discrecionalitats;
- Respecte dels principis bàsics de seguretat informàtica:
    - Confidencialitat: La informació, dades i documents en qualsevol format titularitat de les Institucions no serà divulgada ni cedida a tercers si no és amb el consentiment d'aquestes;
    - Integritat: La informació, dades i documents en qualsevol format titularitat de les Institucions serà emmagatzemada en sistemes segurs de manera que es pugui garantir la seva integritat i no manipulació;
    - Disponibilitat de la informació: La informació, dades i documents en qualsevol format estaran sempre disponibles per les persones autoritzades al seu ús i/o consulta. Així mateix es procurarà que, en cas d'una pèrdua d'informació, aquesta sigui recuperable.
- Compliment de la Política General de Protecció de Dades Personals de la Fundació (política interna): Sense perjudici de tot l'establert en la present Política, les Institucions i els seus usuaris compliran en tot moment amb la Política General de Protecció de Dades Personals de la Fundació.

- Ús responsable de la informació confidencial: Tots els destinataris d'aquesta Política realitzaran un ús responsable de la informació confidencial, tant pròpia com de tercers de la que puguin tenir coneixement, segons es desenvolupa al present document;
- Respecte dels drets dels usuaris: Les Institucions garantiran, en l'ús de les eines informàtiques i dispositius tecnològics, el respecte als drets fonamentals dels usuaris com, per exemple, el dret a l'honor i a la intimitat, emprant sempre els principis de proporcionalitat i menor intrusió en el seguiment del seu ús;
- Desconnexió digital: Les Institucions garantiran, així mateix, el dret a la desconnexió digital dels usuaris essent només exigible l'ús de les eines o dispositius en horari laboral dels treballadors o en execució de tasques concretes sol·licitades als usuaris, a fi de garantir, fora del temps de treball establert legalment o convencionalment, el respecte del seu temps de descans, permisos i vacances, així com de la seva intimitat personal i familiar;
- Accés de les Institucions al contingut de les eines o dispositius: Les Institucions podran accedir als continguts derivats de l'ús de les eines/dispositius per part del usuaris només a l'efecte de controlar el compliment de les seves obligacions laborals, garantir la integritat de les eines/dispositius i realitzar investigacions internes;
- Inquietuds: Els usuaris consultaran a la Comissió de Compliment i Governança i/o al Departament d'Informàtica en cas de dubtes sobre una norma o instrucció d'aquesta Política.

Aquesta política, a més, podrà ser complementada amb altres normes internes que puguin ser desenvolupades per les Institucions que, així mateix, seran revisades per la Comissió de Compliment i Governança. Així mateix aquesta Política complementa totes aquelles que puguin ser aprovades per les Institucions en matèria del sistema de seguretat de la informació.

5. DEFINICIONS:

5.1 – Eines informàtiques i dispositius tecnològics: Les eines informàtiques que poden fer servir els destinataris d'aquesta Política són, amb caràcter general i no limitatiu, els processadors de textos; fulls de càlcul; bases de dades; agendes; programes de correu electrònic; softwares de programació; la intranet; internet; els servidors etc. i els dispositius són, també amb caràcter general i no limitatiu, els equips de fax; impressores; telèfons fixes i mòbils; ordinadors, tablets, perifèrics externs etc. Tots ells, d'ara en endavant, seran mencionats com les ***eines***.

5.2 - Dades de caràcter personal: Qualsevol informació sobre una persona física identificada o identificable; es considerarà persona física identificable tota persona la identitat de la qual pugui determinar-se, directa o indirectament, mitjançant un identificador, com per exemple un nom, un número d'identificació, dades de localització o un o diversos elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social d'aquesta persona.

5.3 - Informació confidencial: Es considerarà informació confidencial totes aquelles dades o informació, de titularitat pròpia o bé de tercers, en el suport que sigui, que es volen mantenir sota reserva i protegides de l'accés de persones no autoritzades per les Institucions o tercers. En tot cas, les Dades de caràcter personal es consideraran informació confidencial.

6. DRETS I DEURES DELS USUARIS EN L'ÚS D'EINES INFORMÀTIQUES, DISPOSITIUS TECNOLÒGICS I INFORMACIÓ CONFIDENCIAL

Seran normes d'obligada observança per tots els destinataris d'aquesta Política les següents:

6.1 – Abast de les eines i dispositius:

Tots els destinataris d'aquesta Política han de ser coneixedors de que les eines que les Institucions posen a la seva disposició són eines de treball titularitat de les mateixes. La finalitat d'aquestes eines és facilitar les tasques professionals que han de ser desenvolupades en el lloc de treball, en la relació contractual o en el permís d'ús de les eines. Es realitzaran recordatoris periòdics a tots els destinataris de la política sobre aquest punt.

6.2 – Abast de la informació confidencial:

Així mateix, amb caràcter general i excepte que s'indiqui el contrari, totes les dades (incloent, amb caràcter enunciatiu però no limitatiu, les Dades de caràcter personal) i informació tractades a les Institucions tindran la qualitat d'informació confidencial i haurà de ser tractada com a tal segons s'estipula a la present Política. Les Institucions podran classificar les seves dades i informació en aquest sentit.

6.3 – Normes d'ús general:

- Les eines facilitades als destinataris d'aquesta Política hauran d'ésser emprades amb cura i preferentment per a les finalitats que els hi són pròpies, és a dir, el desenvolupament de l'activitat professional o contractual que correspongui. Els seus usuaris seran responsables dels danys que les eines puguin patir com a conseqüència de l'incompliment d'aquesta Política així com dels danys produïts per un mal ús d'aquestes;
- Així mateix es realitzarà un ús sostenible i responsable de les eines com, per exemple, evitant el consum de paper, imprimint per les dues cares, utilitzant impressió en color negre etc.;
- Quan es tracti de dispositius mòbils (ordinador portàtil, telèfons, tablets, USB etc.) els usuaris extremaran les precaucions en el seu ús i risc de pèrdua, establint sempre per l'accés als mateixos l'ús de contrasenyes. En cas de que aquest dispositius puguin ser perduts o furtats, es comunicarà immediatament el fet succeït al Departament d'Informàtica a fi de que adopti les mesures de seguretat necessàries per evitar accessos no consentits als mateixos com, per exemple, el bloqueig del dispositiu. En el cas de patir un furt o robatori, aquest fet serà degudament denunciat a les autoritats competents. Només es faran servir els dispositius mòbils facilitats per les Institucions per a garantir la deguda seguretat dels mateixos;
- En aquells casos en que sigui necessària la utilització de les eines a l'estranger es demanarà autorització pel seu ús així al Departament d'Informàtica per establir els millors usos de les eines (exemple: Utilització de xarxes wifi en destí);
- Cada usuari d'una eina que li hagi estat assignada pel desenvolupament de les seves tasques no podrà permetre l'accés a tercers a les mateixes excepte quan així ho autoritzi el Departament d'Informàtica;
- Les Institucions podran adoptar en qualsevol moment mesures de verificació d'ús de les eines, així com dels continguts derivats del seu ús, que creguin necessàries a fi de comprovar el compliment de les obligacions laborals, estatutàries o contractuals dels usuaris i de poder garantir la integritat de les eines facilitades, així com la seva correcta aplicació i la seva

seguretat o bé per a la realització d'investigacions per determinar el compliment de les normes vigents a les Institucions. En aquest sentit, tractant-se d'eines titularitat de les Institucions facilitades preferentment per finalitats professionals no es podrà entendre que existeix expectativa de privacitat, intimitat ni de confidencialitat sobre les mateixes pels seus usuaris;
- Els usuaris utilitzaran totes les mesures de seguretat que siguin establertes sobre les eines pel Departament d'Informàtica, sense que puguin en cap cas modificar o suprimir les mateixes (codis d'accés, números de desbloqueig etc.).
- Les eines mai no seran utilitzades amb finalitats fraudulentes o delictives, quedant expressament prohibit el seu ús amb finalitats d'assetjament laboral, sexual o per raó de sexe; discriminació en el treball; contra l'honor i la dignitat o qualsevol altre conducta constitutiva de conducta il·lícita o delicte. Tampoc no seran emprades per finalitats que puguin afectar la reputació de les Institucions;
- Estarà autoritzat l'ús d'eines personals pels usuaris (ex: Telèfon mòbil propi i no corporatiu) en el seu horari laboral sempre que no interfereixi en el compliment de les obligacions laborals o contractuals.

6.4 – Normes d'ús particulars:

- Els usuaris de les eines no podran modificar els seus continguts sense l'autorització prèvia del Departament d'Informàtica, com, per exemple, quan sigui necessari instal·lar un nou software a les mateixes;
- El Departament d'Informàtica podrà realitzar revisions de les eines a fi de garantir el millor ús i eficiència de les mateixes o bé amb les finalitats esmentades al punt anterior, pel que també podrà procedir a eliminar aquells softwares o programes que pugui localitzar en la seva activitat de revisió i que no hagin estat autoritzats pel Departament. En aquests casos l'eliminació es comunicarà, amb caràcter previ, a l'usuari afectat;
- Quan els dispositius ho permetin, aquests quedaran bloquejats, com a màxim, cada 10 minuts d'inactivitat, de manera que s'hagi de tornar a introduir la contrasenya d'usuari per continuar amb el seu ús; Serà responsabilitat de cada usuari deixar apagades les eines un cop finalitzin la seva jornada laboral o tasca a desenvolupar (tancar la sessió);
- Serà responsabilitat de cada usuari no deixar en fotocopiadores, faxos o impressores papers amb Dades de caràcter personal o qualsevol altra informació confidencial, així com assegurar-se que no queden documents impresos que continguin Dades personals -o qualsevol altra informació confidencial- en la safata de sortida de la fotocopiadora, impressora o faxos. Els usuaris no compartiran ni escriuran en papers o documents a la vista les contrasenyes que emprin per l'ús de les eines;
- Els usuaris dispensaran a les *eines* un ús raonable acomplint amb les directrius que a aquest efecte estableixin les Institucions. L'anterior no impossibilitarà la tasca de control de les Institucions sobre l'ús de les eines tal i com s'exposa més amunt.

6.5 – Compte d'usuari:

Cada usuari podrà ser titular d'un compte d'usuari, aquest serà gestionat des dels Departaments de RR.HH. i Informàtica per a la seva creació (alta), cancel·lació (baixa) o modificació. Les Institucions dictaran les instruccions oportunes per documentar aquest procés.

6.6– Correu electrònic:

- Els comptes de correu electrònic seran utilitzats preferentment per a finalitats corporatives, per a la comunicació entre treballadors, clients, proveïdors, socis, mecenes i qualssevol altres contactes professionals. Es tracta de garantir la seguretat dels sistemes de les Institucions evitant l'entrada als mateixos de virus o similars.
- Cada usuari tindrà un correu electrònic d'ús propi subministrat pel Departament d'Informàtica.
- Els usuaris no podran accedir als comptes de correu electrònic d'altres usuaris excepte quan així ho autoritzi el Departament de RR.HH. amb el previ consentiment de l'usuari titular del compte de correu. Aquesta autorització haurà de ser remesa al Departament d'Informàtica per escrit. Aquests casos s'entenen per quan sigui necessari accedir a informació en l'equip d'un usuari per gestionar processos de les Institucions (ex. En situació de baixa laboral d'un usuari). Per casos d'investigació interna se seguirà l'establert per a aquestes en el punt 6.6.1, així com a la Política i Procediment de gestió del Sistema Intern d'Informació de la Fundació;
- Els usuaris faran servir l'opció CCO (còpia oculta) quan remetin correus electrònics a una pluralitat de destinataris (significadament quan es tracti de correus electrònics amb finalitats publicitàries, informatives o similars). L'anterior es podrà excepcionar quan els destinataris ho autoritzin o bé quan tots els destinataris siguin treballadors de la Fundació i sempre que el correu electrònic s'enviï a la seva adreça professional;
- Els usuaris, sempre que rebin correus amb aparença de virus, no els obriran i donaran compte immediat al Departament d'Informàtica sobre els mateixos. No donaran credencials d'accés a tercers ni accediran a enllaços sense verificar l'origen dels mateixos. Alguns exemples són els següents: Correus amb remitents desconeguts, en altres llengües, amb arxius adjunts poc precisos, que ofereixin premis o consells, amb inconsistències tals com errors gramaticals, majúscules, mal ús de l'idioma etc. o amb característiques que hagin estat avisades des del Departament d'Informàtica;
- Així mateix quan els usuaris detectin possibles atacs o incidències sobre les eines de les Institucions donaran compte immediat al Departament d'Informàtica a qui podran dirigir també dubtes o sol·licituds d'ajuda sobre el funcionament dels equips.

6.6.1 - Monitorització dels correus electrònics i altres eines:

Les Institucions podran utilitzar software de control automatitzat o eines similars per monitoritzar el material creat, emmagatzemat, utilitzat, descarregat, enviat o rebut als seus sistemes, així com monitoritzar llocs visitats pels usuaris a internet, espais de xerrada o grups de notícies; revisar historials descarregats de la xarxa d'internet per usuaris de l'Associació o la Fundació, revisar l'ús de telèfons mòbils, historials de missatges, de correu electrònic enviats, rebuts o en esborrany pels usuaris i tant el flux d'aquestes comunicacions com el contingut de les mateixes. És a dir, amb caràcter general, qualsevol eina informàtica o dispositiu tecnològic de les Institucions.

No obstant l'anterior, en l'adopció de les mesures de verificació de les *eines*, **sempre i en tot cas**, haurà de tenir-se en compte la idoneïtat, necessitat i proporcionalitat de les mesures emprades i complir amb el que s'estableix a continuació, significadament, quan s'hagin detectat indicis d'irregularitats:

- L'accés ha de ser necessari i ha d'estar justificat per verificar raonablement les operacions o processos empresarials i, si existeixen mitjans de menor impacte per l'usuari per a aconseguir la finalitat perseguida, les Institucions en faran ús dels mateixos. Les actuacions de verificació seran proporcionals amb els drets dels usuaris essent el menys intromisives possible;
- Les Institucions informaran amb caràcter previ als usuaris/empleats de la monitorització dels correus electrònics corporatius i/o altres eines, tot indicant l'abast i les finalitats d'aquesta vigilància.
- La privacitat i la dignitat de l'usuari estaran sempre garantides;
- En el seu cas, el correu electrònic, els arxius i els fluxos dels mateixos seran inspeccionats en el lloc de treball, durant les hores de treball normals i podrà comptar-se amb l'assistència dels representants legals dels treballadors o en el seu defecte per un altre empleat de les Institucions;
- En el seu cas, el correu electrònic, arxius o els seus fluxos seran inspeccionats en la presència de l'usuari afectat, que serà informat prèviament, i mitjançant la recerca cega per paraules clau, de manera que només s'accedeixi a la informació estrictament necessària per a les finalitats previstes en la revisió;
- Les Institucions podran també generar una còpia mirall de la informació que sigui necessari examinar i realitzar l'estudi en un moment posterior. En aquests casos s'adoptaran les mesures tècniques necessàries per acreditar la integritat de la informació recollida i s'entregarà també una còpia de la còpia mirall a l'usuari afectat;
- L'ús que faran les Institucions sobre la informació obtinguda serà estrictament confidencial i cenyit als usos propis pels quals es va obtenir. Així mateix les Institucions informaran al subjecte afectat pel procés de revisió del resultat del mateix de forma coordinada amb el Procediment de gestió de les comunicacions rebudes de les Institucions (Canal de Denúncies);
- El Departament d'Informàtica podrà monitoritzar les eines de manera periòdica, per verificar el seu correcte funcionament, realitzar tasques de manteniment o comprovació de dades o recolzament en investigacions del Sistema Intern d'Informació (Canal de Denúncies).

6.7 – Intranet:

- Els usuaris tindran a la seva disposició, a través de la intranet, informació confidencial necessària pel bon desenvolupament de les seves tasques professionals. Tots aquells autoritzats a accedir a la mateixa hauran de realitzar un ús correcte de la mateixa i tractar la informació allí compresa com a confidencial;
- L'accés a la intranet es realitzarà sempre a través de l'usuari i contrasenya intransferible propi de cada treballador, és a dir, no s'empraran contrasenyes de tercers;
- Aquells usuaris que no disposin d'equips informàtics i necessitin accedir a la intranet podran utilitzar, prèvia autorització del Departament d'Informàtica, els dispositius que aquest els hi faciliti amb dita finalitat o bé sol·licitar la informació necessària al Departament de RR.HH.

6.8 – Ús d'internet i xarxes socials:

- L'ús d'internet facilitat per les Institucions serà emprat preferentment per a finalitats relacionades amb l'activitat professional de les Institucions i de forma raonable;
- Els usuaris realitzaran un ús correcte d'internet i amb les finalitats pròpies per les quals es posa a disposició dels usuaris, és a dir, l'ús professional;

- En cap cas els usuaris utilitzaran internet per accedir a pàgines web amb contingut inapropiat o ofensiu pels diferents col·lectius o il·legal i s'asseguraran sempre de respectar els drets de propietat intel·lectual i industrial dels continguts als que puguin accedir en l'ús d'internet (exemple: Accedint a fotografies o textos);
- Els usuaris no empraran les xarxes socials amb perfils privats amb finalitats professionals, excepte autorització expressa del Departament de Comunicació o Direcció General. Així mateix tindran cura de realitzar un ús adequat de les xarxes socials a fi de no malmetre la reputació de les Institucions a través de les mateixes;
- En cap cas es faran servir xarxes wi-fi públiques excepte que el seu ús sigui autoritzat pel Departament d'Informàtica;

6.9 – Ús de softwares i programes:

- És prohibit utilitzar, descarregar o instal·lar als dispositius de les Institucions qualsevol eina informàtica (softwares, aplicacions, programes etc.) que no hagin estat autoritzades pel Departament d'Informàtica i sobre la que les Institucions no tinguin les corresponents llicències d'ús;
- Totes les *eines* que facin servir les Institucions respectaran sempre els corresponents drets de propietat intel·lectual i industrial, circumstància que serà supervisada pel Departament d'Informàtica. L'anterior resultarà també d'aplicació a les actualitzacions o noves versions dels softwares, aplicacions, programes etc. que puguin ser emprats per les Institucions;
- Els usuaris no faran servir amb finalitats personals aquestes eines de les Institucions excepte autorització expressa del Departament d'Informàtica;
- El Departament d'Informàtica confeccionarà un inventari del programari corporatiu homologat a fi de poder gestionar correctament les llicències d'ús i situacions de crisi.

6.10 – Emmagatzematge:

- Els usuaris no empraran sistemes d'emmagatzematge ni de transmissió de la informació - incloses les Dades de caràcter personal i la informació confidencial- fora dels servidors habilitats per les Institucions a aquests efectes.
- Les Institucions només realitzen còpies de seguretat de la informació emmagatzemada als servidors, no així als fitxers locals i a d'altres eines, pel que el Departament d'Informàtica només podrà oferir seguretat sobre la informació custodiada als servidors.

6.11- Dispositius de videovigilància a les Institucions:

Mitjançant la present Política s'informa a tots els usuaris que les Institucions tenen instal·lades a les seves seus càmeres de seguretat, degudament senyalitzades, per poder garantir la seva seguretat i la del seus usuaris (treballadors, públic, visitants etc.) així com per poder supervisar que no es cometin infraccions pels destinataris d'aquesta Política. L'ús de les mateixes es regirà per les següents normes:

- Les càmeres o dispositius de videovigilància en cap cas seran instal·lats a llocs destinats al descans dels usuaris com, per exemple, vestuaris, camerinos, lavabos, menjadors o anàlegs;

- En qualsevol cas es respectaran els principis de proporcionalitat i d'intervenció mínima en el seu ús;
- Així mateix, en cas de que les Institucions, mitjançant les càmeres de videovigilància, puguin detectar un incompliment laboral o contractual, aquestes podran fer servir els enregistraments obtinguts per motivar les sancions disciplinàries o contractuals que corresponguin;
- La captació d'imatges de la via pública només es realitzarà quan resulti imprescindible per a preservar la seguretat de les persones i béns així com de les seves instal·lacions;
- Les imatges que puguin ser enregistrades seran suprimides en el termini d'un mes a comptar des del dia següent al seu enregistrament. Excepte quan sigui necessari conservar-les per acreditar la comissió d'actes que atemptin contra la integritat de persones, béns o instal·lacions. En aquests supòsits les imatges hauran de ser posades a disposició de les autoritats competents en un màxim de 72 hores des de que es tingui coneixement de la gravació i podran ser custodiades a efectes probatoris. També podran custodiar-se les imatges quan aquestes evidenciïn la infracció d'una norma d'obligat compliment a les Institucions o bé d'un il·lícit;
- Tots els dispositius de videovigilància estaran identificats de forma visible a les instal·lacions i s'identificarà, al menys, l'existència del tractament de les imatges, la identitat del responsable, les finalitats de les gravacions i la possibilitat d'exercitar els drets previstos a la llei.

6.12 – Informació confidencial:

Sense perjudici de l'establert al punt 6.2 els usuaris, en l'ús de les *eines*, prendran a més les següents mesures de diligència per evitar la pèrdua d'informació confidencial o l'accés no consentit a la mateixa:

- Utilitzaran les contrasenyes i els comptes d'usuari establerts a la present Política;
- No extrauran fora dels sistemes de les Institucions (ex. Mitjançant dispositius externs, com ara USB o discs durs) informació confidencial.
- La informació confidencial no podrà ser facilitada a tercers no autoritzats sense l'exprés consentiment de les Institucions a través del responsables de cada Departament;
- En cas de pèrdua o accés no consentit a informació confidencial per tercers, informaran immediatament al seu superior jeràrquic sobre el fet succeït i s'adoptaran les mesures preventives o correctives que resultin necessàries;
- Quan sigui necessari, destruiran tot suport d'informació confidencial mitjançant els destructors de paper existents a les instal·lacions de les Institucions o bé mitjançant processos de destrucció d'informació confidencial contractats a l'efecte a fi de garantir la confidencialitat de la informació. L'eliminació de la informació que pugui estar custodiada al Centre de Documentació (CEDOC) haurà de comptar amb la deguda autorització del seu responsable tal com i així consta estipulat al Reglament del Sistema de Gestió Documental de les Institucions;
- Quan els usuaris causin baixa a les Institucions restaran obligats a deixar a les mateixes els arxius, documents o qualsevol tipus de suport que contingui informació de les Institucions a disposició de les mateixes sense que quedin autoritzats a continuar accedint a aquells ni a custodiar còpies dels mateixos;

- L'obligació de confidencialitat correspon a tots els usuaris durant la seva relació laboral o contractual amb les Institucions així com també després de la seva finalització. Així, els usuaris mantindran en la més estricta confidencialitat tota la informació de les Institucions que sigui confidencial i, significadament, aquella relativa a processos, vendes, programació, dades financeres, dades personals, contractes, organització, esdeveniments o qualsevol informació que per la seva naturalesa vulgui ser reservada i no comunicada a tercers per les Institucions;
- Els usuaris només podran accedir a la informació de les Institucions que necessitin pel desenvolupament de les seves tasques professionals i mentre duri la seva relació laboral o vinculació amb les Institucions, pel que el Departament d'Informàtica crearà els corresponents perfils d'usuari amb els permisos d'accés que corresponguin tal i com s'indica més amunt;
- Les Institucions, així mateix, adoptaran les mesures tècniques necessàries per impedir els accessos no consentits a la informació confidencial;

- Els usuaris no accediran a informació confidencial de tercers sense haver estat autoritzats, amb caràcter previ i per escrit, al seu accés;
- A fi de salvaguardar la confidencialitat de la informació tots els usuaris compliran amb les normes establertes a la present Política i a totes aquelles que desenvolupin el Sistema de Seguretat de la Informació.

6.13 – Teletreball:
La present Política resultarà també d'aplicació a l'ús que es produeixi de les eines pels usuaris en situació de teletreball. El Departament d'Informàtica serà el responsable de garantir la seguretat del sistema quan es produeixin situacions de teletreball en els usuaris, així com d'auxiliar als mateixos en l'ús de les eines a distància. Així mateix les Institucions vetllaran pel respecte dels drets i obligacions dels usuaris i d'aquestes en les situacions de teletreball mitjançant el Procediment Intern de Teletreball de la Fundació.

6.14 – Gestió de les altes i baixes dels usuaris en l'ús de les eines:
La gestió de les altes i baixes dels usuaris, en l'ús de les eines, serà realitzada pels Departaments de RR.HH. i Informàtica conforme a instruccions que seran desenvolupades.

6.15 - Mesures de seguretat: Les Institucions vetllaran per la implementació als seus processos de les següents mesures de seguretat a través del Departament d'Informàtica sempre que sigui possible:

- **Protecció de la informació** (ex. Control de les aplicacions instal·lades a dispositius mòbils que només podran ser descarregades dels *markets* oficials -Play Store o App Store per exemle-; xifrat de la informació i autenticació de l'usuari; signar acords de servei amb els emmagatzematges al núvol; realitzar còpies se seguretat periòdiques incloent, quan sigui necessari, els dispositius mòbils; filtres que impedeixin l'accés a determinats urls);
- **Correcte configuració dels dispositius** (ex. Sistema de contrasenya sòlid; antivirus; Firewall; actualitzacions dels softwares en ús; xifrar les dades i les comunicacions; bloqueig remot dels terminals o esborrat remot de dades etc.);

- **Protecció de la connexió a xarxes inalàmbriques** (ex. Prohibir la utilització de xarxes wi-fi o gratuïtes; utilitzar canals xifrats segurs de comunicació VPN; donar ús preferent a les xarxes 3G o 4G abans que wi-fi desconegudes etc.);
- **Realització d'auditories de seguretat** i col·laboració en **auditories externes** com per exemple les de softwares en ús.

  Tot l'anterior serà desenvolupat a través del Sistema de Seguretat de la Informació de les Institucions.

6.16- Protecció de dades personals:

Les Institucions i els usuaris tractaran de manera confidencial les Dades de caràcter personal de les quals tinguin coneixement durant l'ús de les *eines*, complint adequadament les disposicions contingudes a la normativa vigent en cada moment de protecció de dades de caràcter personal i, en particular, amb la Llei Orgànica 3/2018 de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPD-GDD) i el Reglament (UE) 2016/679 relatiu a la protecció de les persones físiques en el que respecta al tractament de les dades personals i a la lliure circulació de les dades.
No es realitzaran transferències de dades personals a tercers, amb excepció de les comunicacions de dades personals als encarregats de tractament de les Institucions amb els quals prèviament s'hagi signat un contracte d'encarregat del tractament que compleixi amb els requisits que s'estableixen en la normativa aplicable.

És responsabilitat de les Institucions assegurar que la recollida de les Dades Personals (*ex*. Dades de clients, candidats, treballadors, etc.) es realitza complint amb el deure d'informació que exigeix la normativa aplicable de protecció de dades personals i, en els casos que així ho exigeixi aquesta normativa, complint també amb el requisit d'obtenció d'un consentiment informat d'aquests subjectes de Dades Personals.

En aquest sentit, les Institucions vetllaran per:

1. Que han informat als subjectes de Dades Personals sobre la recopilació i tractament de les seves dades (finalitats, destinataris, períodes d'emmagatzematge, drets dels subjectes, etc.), d'acord amb les disposicions aplicables en matèria de protecció de dades personals aplicables.
2. Que han obtingut un consentiment informat dels subjectes de Dades Personals quan així ho requereixi la normativa aplicable de protecció de dades personals.
3. Que les Dades Personals recopilades i tractades per les Institucions i el seus usuaris són pertinents, rellevants, no excessives i limitades als fins pels quals s'han recaptat i que la recollida d'aquestes Dades Personals no és il·lícita.
4. Que eliminaran les Dades Personals de totes les Eines -incloent els dispositius- quan ja no siguin necessàries per a les finalitats per a les quals es van recaptar, tret que hi hagi una norma legal que habiliti per a la seva conservació.

De la mateixa manera, els usuaris de les Institucions vetllaran per:

1. Recaptar les Dades Personals utilitzant sempre les pertinents clàusules de protecció de dades proporcionades per les Institucions i complint sempre amb el deure d'informació

i/o l'obtenció del consentiment informat exigit per la normativa aplicable de protecció de dades personals.

2. Tractar les Dades Personals únicament per a les finalitats per les quals es van recaptar.
3. Eliminar les Dades Personals de totes les Eines -incloent els dispositius- quan ja no siguin necessàries per a les finalitats per a les quals es van recaptar, tret que hi hagi una norma legal que habiliti per a la seva conservació.

Amb caràcter enunciatiu, però no limitatiu, les Institucions i els seus usuaris garanteixen el següent:

- Gestió de *currículums vitae*: En la recepció dels mateixos s'informarà al candidat de que el seu CV podrà ser custodiat per les Institucions per a futurs processos de selecció. Els CV's dels candidats que siguin d'interès per la Fundació seran conservats fins que hagin deixat de ser necessaris per a la finalitat per a les quals es va recollir per les Institucions i, en tot cas, no es conservaran durant un període superior a 24 mesos des de que finalitza el procés de selecció que es tracti, tret que hi hagi una norma de rang legal que habiliti la seva conservació.
- Gestió de contractes de laborals: Tots els contractes laborals inclouran, mitjançant annex als mateixos, les pertinents clàusules de protecció de dades personals. Només tindran accés als mateixos el Departament de RR.HH. i Direcció General, havent de ser custodiats degudament als servidors de les Institucions.
- Enviament de correus electrònics amb finalitats publicitàries: Les Institucions i els seus usuaris només podran enviar comunicacions publicitàries als seus clients/proveïdors si tenen el consentiment previ per escrit d'aquests clients/proveïdors.
- Comunicacions col·lectives: Quan es tracti de comunicacions col·lectives (dirigides a un grup de persones), les Institucions i els usuaris, en tot cas, faran servir el mode CCO (còpia oculta).
- Notificacions de violacions de seguretat: Si es donés un incident de seguretat de dades personals, els usuaris hauran de notificar a les Institucions aquest incident sense dilació indeguda i, en tot cas, en les 24 hores següents. Aquesta notificació es farà a través dels canals que designin les Institucions com ara el correu electrònic pd@palaumusica.cat.

En tot cas, les Institucions i els seus usuaris es comprometran a complir amb la Política General de Protecció de Dades de la Fundació.

6.17- Formació: Les Institucions facilitaran formació periòdica a tots els usuaris sobre el contingut de la Política, així com sobre el Sistema de Seguretat de la Informació.

7. ÒRGAN RESPONSABLE:

Seran els departaments afectats per cadascun dels processos aquí establerts així com, en un sentit transversal, el Departament d'Informàtica, Recursos Humans i la Comissió de Compliment i Governança.

Aquests definiran els protocols i els controls adequats en matèria de diligència deguda segons les exigències establertes a les normes aquí citades.

El règim sancionador aplicable per l'incompliment de les mateixes serà l'establert al Conveni Col·lectiu de Treball de la Fundació així com a les normes legals aplicables.

8. EXEMPLES:

Es ressenyen en aquest apartat, a títol d'exemple, supòsits susceptibles d'estar relacionats amb actes d'un ús incorrecte, impropi o maliciós de les eines informàtiques, dispositius tecnològics o sistemes a disposició de les Institucions a fi de facilitar la comprensió del contingut de la present Política:

a) Accedir al correu electrònic professional d'un treballador sense complir les garanties exigides per la llei i la jurisprudència;
b) Accedir de manera no consentida a la base de dades de clients d'un competidor -custodiada al seu sistema- amb independència de que després se'n faci ús o no de la mateixa;
c) Utilitzar els sistemes d'informació de les Institucions per impedir el normal funcionament del sistema d'un competidor i guanyar, així, un major número de venda d'entrades;
d) Enviar un correu electrònic a un col·lectiu de persones sense utilitzar la còpia oculta excepte que es faci únicament amb el correu corporatiu;
e) Accedir a pàgines web de contingut il·legal;
f) Accedir al correu electrònic d'un company de feina sense el seu consentiment;
g) Utilitzar el correu electrònic de les Institucions per a finalitats il·lícites com ara compartir fotografies, gravacions o dades personals sense el consentiment del seu titular;
h) Realitzar pagaments autoritzats per correu electrònic amb suplantació d'identitat i en perjudici de les Institucions (phishing o estafa del CEO).

9. COMUNICACIÓ DE LA PRESENT POLÍTICA

Les disposicions recollides a aquesta Política han de ser conegudes per tots els subjectes als quals va dirigida.

Així mateix, es lliurarà, per mitjans telemàtics o bé en paper, un exemplar de la mateixa a tots els seus destinataris.

Les Institucions conservaran evidències suficients respecte de l'efectiu lliurament de la Política a tots els subjectes apuntats així com del seu compromís per respectar-la.

10.HISTÒRIC, APROVACIÓ I ENTRADA EN VIGOR

Històric:

El següent quadre reflecteix les diferents versions de la Política que han estat confeccionades, així com la seva data i modificacions ulteriors que cadascuna de les versions del document hagi pogut patir:

VERSIÓ	DATA	AUTORS	CANVIS
0.0	Novembre 2018	Carles Ucher	Millora sobre els Protocols de Sistema de Gestió de Seguretat de la Informació i del Protocol de Gestió d'Usuaris

1.0	Setembre 2024	Dpt. Informàtica, Dpt. RR.HH. i Comissió de Compliment i Governança	Versió inicial integrada
2.0	A determinar	A determinar	A determinar

Aprovació i entrada en vigor:

Aquesta Política serà aprovada pels òrgans de govern de les Institucions essent la data de la seva aprovació la data a partir de la qual el document tindrà vigència a les mateixes.

Així mateix aquesta Política substitueix qualsevol altre norma interna existent a les Institucions amb anterioritat a la seva aprovació en matèria d'ús d'eines informàtiques, dispositius tecnològics i confidencialitat.

11. SEGUIMENT, ADEQUACIÓ CONTÍNUA I REFORMA DE LA POLÍTICA

Seguiment i adequació contínua:

S'establiran revisions periòdiques del contingut de la Política per tal de garantir la seva contínua adequació a la realitat de les Institucions, canvis legislatius o jurisprudencials etc.

Reforma:

Les Institucions podran reformar la Política per iniciativa pròpia i/o a proposta que faci al respecte qualsevol destinatari de la mateixa essent sempre revisada per la Comissió de Bones Pràctiques.

12. COMPROMÍS I ACCEPTACIÓ DELS DESTINATARIS DE LA POLÍTICA

Tots els destinataris de la present Política l'han de conèixer, contribuir activament al seu respecte i valorar els incompliments que coneguin així com les deficiències que puguin observar en el seu contingut o desenvolupament.

En el cas d'observar-se el seu incompliment, o bé indicis o proves de la materialització d'un fet que podria constituir un incompliment o bé un il·lícit en matèria d'ús d'eines informàtiques o dispositius tecnològics en sentit ampli, aquesta circumstància haurà de ser posada en coneixement de la Comissió de Compliment i Governança de les Institucions a través de qualsevol dels canals establerts al Sistema Intern d'Informació (Canal de Denúncies) o bé de RR.HH.

Aprovada pel Patronat de la Fundació en sessió de data 19 de setembre de 2024.

ANNEX I

Recepció interna de la Política

La signatura del present document certifica que he rebut, llegit i entès la Política d'ús d'eines informàtiques i dispositius tecnològics i confidencialitat. Comprometent-me, al mateix temps, a respectar-la i a complir-la.
Així mateix, entenc que en cas de que pugui incomplir el seu contingut, aquesta circumstància podria comportar una sanció disciplinària per part de les Institucions o contractual.

Per mitjà del present accepto també estar al dia sobre canvis sobre la Política així com llegir futures revisions que es puguin fer al respecte de la mateixa.

DATA:

NOM/DNI:

SIGNATURA: