**Ordine dei Medici Chirurghi e degli Odontoiatri**
**della provincia di Padova**

35139 PADOVA - Via San Prosdocimo, 6/8 – tel 049.8718855
e-mail: info@omco.pd.it mail PEC: info.pd@pec.omceo.it

# DELIBERA N. 191 del 08.10.2024

**Oggetto: Aggiornamento al CODICE DI COMPORTAMENTO DEL PERSONALE DELL'ORDINE DEI MEDICI CHIRURGHI E DEGLI ODONTOIATRI DI PADOVA approvato con delibera n. 14 del 16.01.2024 – inserimento ALLEGATO A2)**

Il Consiglio Direttivo dell'Ordine dei Medici Chirurghi e degli Odontoiatri della Provincia di Padova, riunito in data 08.10.2024,

**VISTI:**

il D.Lgs.C.P.S. n. 233/46 - "*Ricostituzione degli ordini delle professioni sanitarie e per la disciplina dell'esercizio elle professioni stesse*" e ss.mm.ii;

- il D.P.R. n. 221/50 – "*Approvazione del regolamento per la esecuzione del decreto legislativo 13 settembre 1946 n. 233, sulla ricostituzione degli ordini delle professioni sanitarie e per la disciplina dell'esercizio delle professioni stesse";*

- la Legge 241/90 e ss. mm. e ii., recante "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*";

- il D. Lgs. 27/10/2009, n. 150 - "*Attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni*";

- il D. Lgs. 25/05/2017, n. 74 - "*Modifiche al decreto legislativo 27 ottobre 2009, n. 150, in attuazione dell'articolo 17, comma 1, lettera r), della legge 7 agosto 2015, n. 124*";

- il D. Lgs. 179/12, recante "*Ulteriori misure urgenti per la crescita del Paese*";

- la Legge 190/12, "*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione*";

- il D. Lgs. 14 marzo 2013 n. 33, "*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*";

- la Legge 11 gennaio 2018, n. 3, recante "*Delega al Governo in materia di sperimentazione clinica di medicinali nonché disposizioni per il riordino delle professioni sanitarie e per la dirigenza sanitaria del Ministero della salute*";

- il D. Lgs. n. 165/2001 *"Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche";*

**VISTO** in particolare l'art. 54 del D. Lgs.165/2001 rubricato "*Codice di comportamento*";

**VISTO** il D.P.R. n. 62/2013 avente ad oggetto: "*Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165*";

**VISTO** in particolare il D.P.R. n. 81 del 13 giugno 2023 avente ad oggetto: "*Regolamento concernente modifiche al Decreto del Presidente della Repubblica 16 aprile 2013, n. 62, recante: «Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165";*

**VISTO** il Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati" (GDPR) e il Codice Privacy D. Lgs. 196/2003 armonizzato;

**VISTO** il Codice di Comportamento del Personale Dipendente dell'Ordine dei Medici Chirurghi ed Odontoiatri della Provincia di Padova approvato con Delibera del Consiglio Direttivo n. 14 del 16 gennaio 2024;

**DATO ATTO** che le misure di sicurezza poste a tutela dei dati costituiscono un obbligo finalizzato alla protezione dei dati e che il trattamento dei dati personali richiede obbligatoriamente l'adozione di idonee e preventive misure di sicurezza;

**RAVVISATA** pertanto la necessità di completare il Codice di Comportamento del Personale Dipendente dell'Ordine con le "Linee Guida sul corretto utilizzo delle tecnologie informatiche e degli archivi";

**CONSIDERATO** che il Codice di comportamento adottato dall'Ente è attualmente composto di n. 22 articoli e dal documento rubricato "Social media policy" (All. A1);

**RAVVISATA** altresì la necessità di integrare il summenzionato Codice di Comportamento del Personale dipendente dell'Ordine dei Medici con il documento rubricato "Linee Guida sul corretto utilizzo delle tecnologie informatiche e degli archivi" quale allegato A2) del medesimo e che ne costituisce parte integrante e sostanziale;

**DATO ATTO** che mediante la sopra descritta integrazione il Codice di Comportamento dei Dipendenti dell'Ordine (All.A) si compone di due documenti:

- "Social Media policy" (All. A1);
- "Linee Guida sul corretto utilizzo delle tecnologie informatiche e degli archivi" quale (All.A2)

e che i tre documenti sopra menzionati si allegano al presente provvedimento per costituirne parte integrante e sostanziale;

per le motivazioni espresse in premessa che qui si intendono integralmente accolte

su proposta del Presidente

all'unanimità di voti

**DELIBERA**

- di prendere atto della necessità di integrae il Codice di comportamento del Personale Dipendente dell'Ordine con il documento rubricato "Linee Guida sul corretto utilizzo delle tecnologie informatiche e degli archivi" quale allegato A2) del medesimo e che ne costituisce parte integrante e sostanziale;

- di approvare l'Allegato A2 "Linee Guida sul corretto utilizzo delle tecnologie informatiche e degli archivi" quale parte integrante del Codice di Comportamento del Personale dipendente dell'Ordine dei Medici Chirurghi e Odontoiatri di Padova ai sensi del D.P.R. n. 81/2023, già approvato con delibera n. 14 del 16.01.2024;

- di allegare al presente provvedimento il Codice di Comportamento del Personale Dipendente dell'Ordine dei Medici Chirurghi e Odontoiatri di Padova composto da n. 22 articoli (Allegato A), dal documento rubricato "Social media policy" (All. A1), e dalle "Linee Guida sul corretto utilizzo delle tecnologie informatiche e degli archivi" (All. A2), che costituiscono parte integrante e sostanziale del presente provvedimento;

- di trasmettere il Regolamento aggiornato alla Federazione Nazionale degli Ordini dei Medici Chirurghi e Odontoiatri, ai sensi dell'art. 35 del DPR 221/1950;

- di procedere alla pubblicazione del presente provvedimento nella sezione "Amministrazione Trasparente" nel rispetto del D. Lgs n. 33/2013.

IL [redacted] *rà*

A)

*ORDINE PROVINCIALE DEI MEDICI CHIRURGHI E DEGLI ODONTOIATRI DI PADOVA*

# CODICE DI COMPORTAMENTO DEL PERSONALE DELL'ORDINE DEI MEDICI CHIRURGHI E DEGLI ODONTOIATRI DI PADOVA

adottato ai sensi dell'art. 54 del d. lgs. 30 marzo 2001 n. 165 e del d.p.r. 16 aprile 2013 n. 62 - Aggiornato ai sensi del D.P.R. n. 81/2023

**Approvato dal Consiglio Direttivo con Delibera N. 14 del 16 Gennaio 2024 e aggiornato con Delibera N. 191 del 08 Ottobre 2024**

**CODICE DI COMPORTAMENTO E DI TUTELA DELLA DIGNITA' E DELL'ETICA DEI DIPENDENTI DELL'ORDINE DEI MEDICI CHIRURGHI E DEGLI ODONTOIATRI DI PADOVA**

## PREMESSA
## Dichiarazioni di principio a tutela della dignità e dell'etica

1. Le risorse umane sono il più importante patrimonio dell'Ordine dei Medici Chirurghi e degli Odontoiatri di Padova, di seguito denominato Ente, ne costituiscono la forza, l'efficacia, l'intelligenza, la reputazione e la prospettiva e ne condividono gli obiettivi con pieno coinvolgimento, ad ogni livello, nel lavoro di squadra.

2. Tutte le lavoratrici e i lavoratori hanno diritto ad un ambiente di lavoro sicuro e confortevole, sereno e favorevole alle relazioni interpersonali, su un piano di uguaglianza, reciproca correttezza e rispetto delle libertà e della dignità della persona. Hanno diritto a svolgere le proprie funzioni in un ambiente che garantisca il rispetto della dignità umana di ciascuno, evitando ogni tipo di discriminazione, molestia e di comportamento inopportuno e indesiderato.

3. L'Ente garantisce ad ogni dipendente il diritto alla tutela da qualsiasi atto o comportamento che produca un effetto pregiudizievole e discriminazioni, anche in via indiretta. Adotta le iniziative volte a favorire un maggiore rispetto reciproco dell'inviolabilità della persona, attraverso la formazione, l'informazione e la prevenzione. Ciascuna lavoratrice e ciascun lavoratore, nei rapporti interpersonali, è tenuto a contribuire alla promozione e al mantenimento di un ambiente e di una organizzazione del lavoro che siano ispirati e fondati su principi di correttezza, libertà, dignità ed uguaglianza.

4. Il mobbing, le molestie ed ogni altra forma di discriminazione - che tendano ad emarginare la persona per motivi culturali, politici, sindacali, religiosi, etnici, di provenienza territoriale, di orientamento sessuale o di altro genere - sono inammissibili e ledono la dignità di coloro che li subiscono, compromettendone la salute, la fiducia, il morale, la motivazione al lavoro, incidendo inoltre negativamente sulla prestazione di lavoro e sul clima organizzativo.

5. L'Ente riconosce che il benessere psicofisico, la serenità psicologica nei luoghi di lavoro e gli aspetti emotivi e motivazionali delle attività lavorative sono fattori strategici sia per l'organizzazione che per la gestione delle risorse umane, anche per la diretta ricaduta che tali aspetti hanno sulla qualità delle prestazioni e delle relazioni con gli utenti.

6. L'Ente assicura l'adozione di misure diversificate, tempestive e imparziali, volte a garantire alla/al dipendente che sia oggetto di mobbing, di molestie e che sia esposta/o a comportamenti indesiderati, o comunque discriminatori, l'interruzione della condotta molesta.

7. La prevenzione di ogni forma di mobbing, di molestia e di ogni tipo di discriminazione è obiettivo imprescindibile dell'Ente, da perseguirsi anche attraverso l'incentivazione di modelli lavorativi fondati sui principi esposti nel presente codice di comportamento, di seguito denominato Codice.

8. La posizione di superiorità gerarchica non deve legittimare comportamenti o atti discriminatori o molesti nei confronti delle/dei dipendenti. Chi denuncia casi di mobbing o di molestie ha diritto alla riservatezza e a non essere oggetto di ritorsione diretta o indiretta.

9. Ogni accertata violazione della dignità della lavoratrice e del lavoratore costituisce un illecito disciplinare, in quanto l'autrice/autore di tali comportamenti viola un principio etico ed un preciso dovere di ufficio.

10. È inammissibile ogni atto o comportamento che si configuri come molestia sessuale, morale e psicologica.

11. È sancito il diritto delle lavoratrici e dei lavoratori ad essere trattati con dignità e ad essere tutelati nella propria libertà personale.

12. È sancito il diritto delle lavoratrici e dei lavoratori a denunciare le eventuali intimidazioni o ritorsioni subite sul luogo di lavoro derivanti da atti o comportamenti molesti o discriminatori.

12. È garantito l'impegno dell'Ente a sostenere ogni dipendente che sporga denuncia di molestie, fornendo chiare ed esaurienti indicazioni circa la procedura da seguire, mantenendo la riservatezza e prevenendo ogni eventuale ritorsione. Analoghe garanzie sono estese agli eventuali testimoni.

13. È assicurata, nel corso degli accertamenti, l'assoluta riservatezza dei soggetti coinvolti: i dati riservati delle/dei dipendenti coinvolte/i sono trattati nel rispetto di quanto disposto dal Regolamento generale per la protezione dei dati personali n. 2016/679.

14. Nei casi denunciati di molestie o discriminazioni, l'Ente può procedere alla verifica su eventuali azioni moleste o discriminatorie subite dal soggetto interessato, in merito a trasferimenti, percorsi di carriera, riconoscimenti professionali, orari di lavoro, partecipazione ad attività e conferimento di incarichi.

## Art.1

## Valori fondamentali e disposizioni di carattere generale

1. L'Ente assicura il rispetto della persona e della sua dignità, contrasta ogni discriminazione, esalta e promuove l'onestà intellettuale e morale, il decoro, la correttezza e la lealtà nei rapporti personali e professionali di tutte/i le/i dipendenti e collaboratrici/tori a qualunque livello.

2. L'Ente promuove il rispetto di principi, regole, anche morali, e comportamenti coerenti con i suddetti valori fondamentali. I principi e le regole contenute nel presente Codice, oltre a costituire specificazioni esemplificative degli obblighi di diligenza, che qualificano il corretto adempimento della prestazione lavorativa, hanno lo scopo di fornire alle/ai dipendenti dell'Ordine dei modelli comportamentali diretti ad ispirare condotte conformi ai principi di trasparenza, correttezza, imparzialità, efficienza, lealtà e decoro nei rapporti interni ed esterni. La loro osservanza informa l'azione dell'Ente verso l'esterno e delle/dei singole/i dipendenti nei rapporti interni, contribuendo a creare e mantenere un ambiente di lavoro ordinato, positivo e sereno, che valorizzi il benessere di chi lavora, nel rispetto della dignità di ciascuno e contro ogni forma di discriminazione.

3. Il presente Codice integra e specifica, ai sensi dell'articolo 54, comma 5, del decreto legislativo 30 marzo 2001, n. 165, i doveri minimi di lealtà, correttezza e riservatezza già individuati nel Codice di comportamento dei dipendenti pubblici, emanato con Decreto del Presidente della Repubblica 16 aprile 2013, n. 62, di seguito "Codice Generale". Le/I dipendenti dell'Ente, tutte/i le/i collaboratrici/tori e consulenti, con qualsiasi tipologia di contratto o incarico e a qualsiasi titolo e agli affidatari di lavori, servizi e forniture per conto dell'Ente e loro collaboratrici/tori, sono tenute/i ad osservare i principi del precedente comma 3, a tutela del prestigio e del ruolo istituzionale della stessa anche dopo la cessazione del rapporto di lavoro.

4. Il Codice rappresenta misura attuativa delle strategie di prevenzione della corruzione ed è strumento integrativo del Piano triennale di prevenzione della corruzione nell' Ente. Il Codice, assieme alle sottosezioni Anticorruzione e Trasparenza del PIAO, è pubblicato sul sito internet istituzionale nella pagina dell'Amministrazione Trasparente, e viene inoltre consegnato, per via telematica, a tutte/i le/i dipendenti e alle/ai collaboratrici/tori esterni al momento della loro assunzione, all'avvio della attività di collaborazione e a seguito di aggiornamenti. Costoro sottoscrivono, all'atto del loro ingresso nell'Ente, apposita dichiarazione di presa d'atto.

5. Il presente Codice di Comportamento recepisce e fa proprio il Codice di Comportamento Generale approvato con D.P.R. 62/2013, in esecuzione agli obblighi di cui alla L.190/2012.

6. Il presente codice viene aggiornato al D.P.R. n. 81/2023.

7. Il presente Codice sostituisce il precedente, adottato con delibera consiliare del n. 24 del 2 febbraio 2016

## Art. 2
## Ambito di applicazione

1. Il Codice si applica, secondo competenza, alle/ai dipendenti dell'Ordine dei Medici Chirurghi e degli Odontoiatri di Padova (dipendenti a tempo indeterminato e a tempo determinato), nonché a tutte/i le/i collaboratrici/tori e consulenti, con qualsiasi tipologia di contratto o incarico e a qualsiasi titolo e agli affidatari di lavori, servizi e forniture per conto dell'Ente e loro collaboratrici/tori.

2. I/le dipendenti dovranno altresì rispettare le disposizioni, oltre che del presente Codice, anche di ogni altra disposizione organizzativa dell'Ente oltre che delle sottosezioni Anticorruzione e Trasparenza del PIAO.

## Art. 3
## Principi generali

1. I/le dipendenti osservano la Costituzione, servendo la Nazione con disciplina e onore e conformando la propria condotta ai principi di buon andamento e imparzialità dell'azione amministrativa. I/le dipendenti svolgono i propri compiti nel rispetto della legge, perseguendo l'interesse pubblico senza abusare della posizione o dei poteri di cui è titolare.

2. I/le dipendenti rispettano altresì i principi di integrità, correttezza, buona fede, proporzionalità, obiettività, trasparenza, equità e ragionevolezza e agisce in posizione di indipendenza e imparzialità, astenendosi in caso di conflitto di interessi.

3. I/le dipendenti non usano a fini privati le informazioni di cui dispongono per ragioni di ufficio, evitano situazioni e comportamenti che possano ostacolare il corretto adempimento dei compiti o nuocere agli interessi o all'immagine dell'Ente. Prerogative e poteri pubblici sono esercitati unicamente per le finalità di interesse generale per le quali sono stati conferiti.

4. I/le dipendenti esercitano i propri compiti orientando l'azione amministrativa alla massima economicità, efficienza ed efficacia. La gestione di risorse pubbliche ai fini dello svolgimento delle attività amministrative deve seguire una logica di contenimento dei costi, che non

pregiudichi la qualità dei risultati.

5. Nei rapporti con le/i destinatarie/i dell'azione amministrativa, le/i dipendenti assicurano la piena parità di trattamento a parità di condizioni, astenendosi, altresì, da azioni arbitrarie che abbiano effetti negativi sui destinatari dell'azione amministrativa o che comportino discriminazioni basate su sesso, nazionalità, origine etnica, caratteristiche genetiche, lingua, religione o credo, convinzioni personali o politiche, appartenenza a una minoranza nazionale, disabilità, condizioni sociali o di salute, età e orientamento sessuale o su altri diversi fattori anche a mezzo web, social network, blog, forum o altri media.

6. La/il dipendente e i soggetti di cui all'art. 2, comma 1, dimostrano la massima disponibilità e collaborazione nei rapporti con le altre pubbliche amministrazioni, assicurando lo scambio e la trasmissione delle informazioni e dei dati in qualsiasi forma anche telematica, nel rispetto della normativa vigente.

7. La/Il dipendente e i soggetti di cui all'art. 2, comma 1, esercitano la propria attività lavorativa nel rispetto delle leggi istitutive, quale atto normativo fondamentale dell'Ente, e dei Regolamenti vigenti (D. Lgs. C.P.S. 13/09/46 n.233 e s.m.i., D.P.R. 05/04/1950 n.221; L. 24/07/1985 n.409; L. 3/2018).

## Art. 4
## Regali compensi e altre utilità

1. I/le dipendenti e i soggetti di cui di cui all'art. 2, comma 1, non chiedono, né sollecitano, per sé o per altri, regali o altre utilità. Inoltre, non accettano, per sé o per altri, regali o altre utilità, salvo quelli d'uso di modico valore effettuati occasionalmente nell'ambito delle normali relazioni di cortesia e nell'ambito delle consuetudini internazionali. In ogni caso, indipendentemente dalla circostanza che il fatto costituisca reato, i/le dipendenti non chiedono, per sé o per altri, regali o altre utilità, neanche di modico valore a titolo di corrispettivo per compiere o per aver compiuto un atto del proprio ufficio da soggetti che possano trarre benefici da decisioni o attività inerenti all'ufficio, né da soggetti nei cui confronti è o sta per essere chiamato a svolgere o a esercitare attività o potestà proprie dell'ufficio ricoperto.

2. I/le dipendenti e i soggetti di cui di cui all'art. 2, comma 1non accettano, per sé o per altri, da un proprio subordinato, direttamente o indirettamente, regali o altre utilità, salvo quelli d'uso di modico valore. Inoltre, non offrono, direttamente o indirettamente, regali o altre utilità a un proprio sovraordinato, salvo quelli d'uso di modico valore.

3. I regali e le altre utilità comunque ricevuti fuori dai casi consentiti dal presente articolo, a cura dello/a stesso/a dipendente cui siano pervenuti, sono immediatamente messi a disposizione dell'Ente per la restituzione o per essere devoluti a fini istituzionali.

4. Ai fini del presente articolo, per regali o altre utilità di modico valore si intendono quelle di valore non superiore, in via orientativa, a 150 €, anche sotto forma di sconto.

5. La/Il dipendente non accetta incarichi di collaborazione, a qualsiasi titolo giuridico e anche a titolo gratuito, da soggetti privati che abbiano, o abbiano avuto nel biennio precedente, un interesse economico significativo in decisioni o attività inerenti all'ufficio di appartenenza.

6. Ai sensi del comma 6, le categorie di soggetti privati che in genere hanno interessi economici

significativi in decisioni o attività inerenti all'Ente sono quelli operanti nei settori: bancario, informatico-gestionale, legale, assicurativo e formazione-comunicazione

7. Al fine di preservare il prestigio e l'imparzialità dell'Ente, la/il responsabile dell'ufficio interessato e la/il Responsabile Anticorruzione dell'Ente vigilano sulla corretta applicazione del presente articolo.

## Art. 5
## Partecipazione ad associazioni e organizzazioni

1. Nel rispetto della disciplina vigente del diritto di associazione, la/il dipendente comunica tempestivamente al responsabile dell'ufficio di appartenenza la propria adesione o appartenenza ad associazioni o organizzazioni, a prescindere dal loro carattere riservato o meno, i cui ambiti di interessi possano interferire con lo svolgimento dell'attività dell'ufficio. Il presente comma non si applica all'adesione a partiti politici o a sindacati.

2. Ai sensi del comma 1, le associazioni od organizzazioni della cui adesione le/i dipendenti addette/i devono effettuare comunicazione, nel termine di 30 gg. dall'adesione, alla/al propria/o responsabile sono quelle operanti nei settori: medico scientifico, bancario (struttura del credito cooperativo), informatico- gestionale, legale, assicurativo e formazione-comunicazione.

3. La/Il pubblico dipendente non costringe altri dipendenti ad aderire ad associazioni od organizzazioni, né esercita pressioni a tal fine, promettendo vantaggi o prospettando svantaggi di carriera.

## Art. 6

## Comunicazione degli interessi finanziari e conflitti di interesse

1. Fermi restando gli obblighi di trasparenza previsti da leggi o regolamenti, la/il dipendente, all'atto dell'assegnazione all'ufficio, informa per iscritto la/il responsabile dell'ufficio di tutti i rapporti, diretti o indiretti, di collaborazione con soggetti privati in qualunque modo retribuiti che lo stesso abbia o abbia avuto negli ultimi tre anni, precisando:
   - se in prima persona, o suoi parenti o affini entro il secondo grado, il coniuge o il convivente abbiano ancora rapporti finanziari con il soggetto con cui ha avuto i predetti rapporti di collaborazione;
   - se tali rapporti siano intercorsi o intercorrano con soggetti che abbiano interessi in attività o decisioni inerenti all'ufficio, limitatamente alle pratiche a lui affidate.

2. Per soggetti privati di cui al comma 1 si intende i soggetti privati operanti nei settori: medico scientifico, bancario (struttura del credito cooperativo), informatico-gestionale, legale, assicurativo e formazione-comunicazione.

3. Qualora ricorra la condizione di cui al comma 1 in un periodo successivo all'assegnazione alla propria struttura di appartenenza, la/il dipendente interessato deve effettuare le predette comunicazioni nel termine di 30 giorni dal verificarsi della condizione.

4. La/Il dipendente si astiene dal prendere decisioni o svolgere attività inerenti alle sue mansioni in situazioni di conflitto, anche potenziale, di interessi con interessi personali, del coniuge, di conviventi, di parenti, di affini entro il secondo grado. Il conflitto può riguardare interessi di

qualsiasi natura, anche non patrimoniali, come quelli derivanti dall'intento di voler assecondare pressioni politiche, sindacali o dei superiori gerarchici.

## Art. 7
## Obbligo di astensione

1. La/Il dipendente si astiene dal partecipare all'adozione di decisioni o ad attività che possano coinvolgere interessi propri, ovvero di suoi parenti, affini entro il secondo grado, del coniuge o di conviventi, oppure di persone con le quali abbia rapporti di frequentazione abituale, ovvero, di soggetti od organizzazioni con cui ella/egli o il coniuge abbia causa pendente o grave inimicizia o rapporti di credito o debito significativi, ovvero di soggetti od organizzazioni di cui sia tutore, curatore, procuratore o agente, ovvero di enti, associazioni anche non riconosciute, comitati, società o stabilimenti di cui sia amministratore o gerente o dirigente. La/il dipendente si astiene in ogni altro caso in cui esistano gravi ragioni di convenienza dandone comunicazione al Consiglio Direttivo.

2. La/Il dipendente, chiamato a svolgere attività o ad assumere decisioni che coinvolgano gli interessi di cui al comma 1 e 2, è tenuta/o a comunicare tempestivamente al Direttore e al Consiglio Direttivo la sussistenza di tale interesse.

3. Il Direttore dell'Ordine ricevuta la comunicazione, deve disporre con proprio provvedimento l'astensione della/del dipendente dall'attività e/o decisione che dà origine al conflitto o, nel caso in cui ravvisi la non rilevanza dell'interesse del dipendente, l'archiviazione della segnalazione ricevuta. In ogni caso deve informare il Consiglio Direttivo. Il presente procedimento deve concludersi entro il termine di 30 giorni dalla ricezione della comunicazione da parte del dipendente interessato, prorogabili per ulteriori 30 giorni per particolari esigenze legate all'istruttoria dello stesso.

## Art. 8
## Prevenzione della corruzione

1. La/Il dipendente rispetta le misure necessarie alla prevenzione degli illeciti nell'Ente. In particolare, la/il dipendente rispetta le prescrizioni contenute nelle sottosezioni Anticorruzione e Trasparenza del PIAO, presta la sua collaborazione attiva al responsabile della prevenzione della corruzione ai fini della prevenzione dei fenomeni di corruzione e di mala amministrazione e dell'accertamento dei fatti.

2. Fermo restando l'obbligo di denuncia all'autorità giudiziaria, la/il dipendente è tenuta/o a segnalare tramite procedura di Whistleblowing eventuali situazioni di illecito nell'Ente di cui sia venuta/o a conoscenza, ovvero alla/al responsabile della prevenzione della corruzione qualora tali fatti siano direttamente riferibili al proprio superiore gerarchico.

3. Per la tutela del *whistleblowing* si rinvia alla sottosezione Anticorruzione e Trasparenza del PIAO.

## Art. 9
## Trasparenza e tracciabilità

1. La/Il dipendente assicura l'adempimento degli obblighi di trasparenza previsti in capo all'Ente secondo le disposizioni normative vigenti, prestando la massima collaborazione nell'elaborazione, reperimento e trasmissione dei dati sottoposti all'obbligo di pubblicazione sul sito istituzionale.

2. La tracciabilità dei processi decisionali adottati dai dipendenti deve essere, in tutti i casi, garantita attraverso un adeguato supporto documentale, che consenta in ogni momento la replicabilità.

3. Le/I dipendenti sono tenuti a rendere disponibili, tempestivamente ed in modo regolare e completo, le informazioni, i dati e gli atti soggetti per legge a pubblicazione.

4. Le/I dipendenti provvedono alla trasmissione delle informazioni, dei dati e degli atti ricevuti, al soggetto addetto alla loro pubblicazione.

**Art. 10**
**Comportamento nei rapporti privati**

1. Nei rapporti privati, comprese le relazioni extralavorative con pubblici ufficiali nell'esercizio delle loro funzioni, la/il dipendente non sfrutta, né menziona la posizione che ricopre nell'Ente per ottenere utilità che non gli spettino e non assume nessun altro comportamento che possa nuocere all'immagine dell'Ente anche a mezzo web, social network, blog, forum o altri media.

2. La/Il dipendente, ferma la libertà di manifestazione del proprio pensiero, deve sempre puntualizzare che le opinioni espresse pubblicamente o in contesti sociali non pubblici, ma comunque costituiti da un numero apprezzabile di persone, che tali opinioni non rappresentano né impegnano l'Ente di appartenenza, fermo quanto disposto dal comma precedente.

3. Le/I dipendenti sono tenuti al segreto d'ufficio, a non rivelare il contenuto di atti e informazioni di cui siano venuti a conoscenza nell'esercizio delle proprie funzioni, o al fine di conseguire utilità dirette o indirette per sé o per i soggetti di cui all'art. 7 comma 1, ovvero per arrecare danno a soggetti od organizzazioni con cui egli o il coniuge abbia causa pendente o grave inimicizia o rapporti di debito significativi.

**Art.11**
**Comportamento in servizio**

1. Fermo restando il rispetto dei termini del procedimento amministrativo, la/il dipendente, salvo giustificato motivo, non ritarda né adotta comportamenti tali da far ricadere su altri dipendenti il compimento di attività o l'adozione di decisioni di propria spettanza.

   La/Il dipendente utilizza i permessi di astensione dal lavoro, comunque denominati, nel rispetto delle condizioni previste dalla legge, dai regolamenti e dai contratti collettivi.

   La/Il dipendente utilizza il materiale o le attrezzature di cui dispone per ragioni di ufficio e i servizi telematici e telefonici dell'ufficio nel rispetto dei vincoli posti dall'Ente.

2. La/Il Segretaria/o dell'Ordine, coadiuvato dalla/dal Dirigente, è tenuto a garantire l'equa e simmetrica ripartizione dei carichi di lavoro tra i dipendenti e a rilevare e tenere conto, in sede di valutazione, delle eventuali deviazioni dovute a negligenza, fermo restando l'obbligo, nei casi più gravi di avviare il procedimento disciplinare nel rispetto delle disposizioni normative e contrattuali vigenti.

   Nel caso in cui la/il Segretaria/io dell'Ordine non ottemperi a quanto previsto dal comma 4, la/il Responsabile Anticorruzione esercita poteri sostitutivi e ha l'obbligo di avviare il procedimento disciplinare a suo carico.

   La/Il Segretario dell'Ordine, coadiuvato dal Dirigente, vigila sulla corretta fruizione dei permessi di astensione dal lavoro, comunque denominati, da parte dei dipendenti, nonché sul corretto utilizzo della procedura di richiesta e sulla tempestività della stessa, anche in ottemperanza a termini specifici previsti da obblighi di legge, limitando l'uso della modulistica cartacea ad ipotesi residuali giustificate da motivate esigenze di carattere eccezionale o applicativo- informatico.

3. Le/I dipendenti sono tenute/i a rispettare l'orario di lavoro secondo l'articolazione vigente nell'Ente, in relazione al loro profilo professionale e a registrare la propria presenza in servizio, oraria ed extra- orario (lavoro straordinario), attraverso sistemi automatici di rilevamento presenze messi a disposizione dall'Ente.

   La/Il Segretaria dell'Ordine, coadiuvato dalla/ dal Dirigente, vigila sul rispetto dell'orario di lavoro e sulla corretta registrazione delle presenze in servizio dei dipendenti addetti alla propria struttura, invitandoli a regolarizzare tempestivamente eventuali anomalie o debiti orari, nel rispetto della prassi vigente all'interno dell'Ente. Nei casi di reiterata violazione di questi doveri da parte di alcuni dipendenti, la/il Segretaria/o dell'Ordine è tenuto a riferire al Consiglio per l'avvio del procedimento disciplinare a loro carico, nel rispetto delle disposizioni normative e contrattuali vigenti e dei regolamenti interni deliberati.

4. Le/I dipendenti hanno il dovere di comunicare tempestivamente eventuali variazioni delle dichiarazioni, già presentate, di insussistenza di conflitto di interessi.

5. Le/I dipendenti interessati da procedimenti penali per reati contro la Pubblica Amministrazione hanno l'obbligo di segnalare immediatamente l'avvio di tali procedimenti all'Ente.

## Art.12
## Comportamento nello svolgimento della prestazione lavorativa in smart working (lavoro agile)

1. Il/la dipendente si impegna al raggiungimento degli obiettivi concordati con l'Ordine con cadenza annuale ed a quelli mensili condivisi con il Segretario dell'Ordine, al fine di garantire l'efficacia della prestazione e la sua realizzazione in maniera organizzata e condivisa sulla base delle esigenze della Segreteria.

2. Il/la dipendente provvede a rilevare l'attività lavorativa svolta durante le giornate di lavoro agile sulla base di un report giornaliero di attività appositamente predisposto che viene chiuso ogni mese, protocollato e inviato a Presidente e Segretario dell'Ordine.

3. Al/alla dipendente in lavoro agile è richiesto di adottare il principio di ragionevolezza nella scelta

dei luoghi di lavoro per l'esecuzione della prestazione lavorativa (ambienti indoor e outdoor) evitando luoghi, ambienti, situazioni da cui possa derivare un pericolo per la sua salute e sicurezza.

4. Il/la dipendente verifica ed assicura il buon funzionamento della strumentazione tecnologica necessaria allo svolgimento della prestazione lavorativa in modalità agile, anche se trattasi di strumentazione personale.

5. Nelle giornate di svolgimento della prestazione lavorativa in modalità agile il/la dipendente osserva le fasce orarie di reperibilità pattuite con l'Ordine e presenti nell'accordo individuale e nella contrattazione decentrata. In ogni caso, viene riconosciuto e garantito il diritto dei dipendenti alla disconnessione. Tale diritto include, tra l'altro, il venir meno dell'obbligo di rispondere a chiamate telefoniche e ad e-mail durante le fasce orarie nelle quali è riconosciuto il diritto alla disconnessione.

6. In ogni giornata di svolgimento della prestazione lavorativa in modalità agile il/la dipendente attiva il collegamento tra la linea del telefono fisso ubicato presso l'Ufficio ed il proprio cellulare tramite apposita applicazione, al fine di garantire il ricevimento delle chiamate telefoniche destinate all'Ufficio anche nel corso delle giornate di svolgimento della prestazione lavorativa in modalità agile.

## Articolo 13
## Tutela dell'ambiente

1. In un'ottica di perseguimento della sostenibilità ambientale e di contenimento delle spese energetiche, tutti i/le dipendenti esercitano i propri compiti nel rispetto dei principi di efficacia, economicità ed efficienza.

2. I/le dipendenti sono tenuti a partecipare in maniera attiva e costante alla riduzione dei consumi dei materiali, delle risorse energetiche e idriche, impegnandosi ad un comportamento quotidiano rispettoso dell'ambiente e ad un utilizzo scrupoloso e parsimonioso delle risorse a disposizione.

   I/le dipendenti sono inoltre tenuti ad adottare pratiche e comportamenti volti a ridurre gli sprechi, utilizzando in maniera consapevole le risorse dell'Ente e riducendo al minimo l'uso della stampante, il consumo di carta e toner e prediligendo procedura digitali. In caso non sia possibile evitare l'utilizzo della stampante, i dipendenti scelgono di utilizzare modalità di stampa fronte – retro, in bianco e nero e in modalità di risparmio dell'inchiostro, ridimensionando i testi o le immagini per limitare il consumo di carta e toner. Quando possibile, le vecchie stampe o le bozze vengono riutilizzate per prendere appunti o per altri impieghi.

   Al termine del servizio, e quando non necessari, i/le dipendenti provvedono allo spegnimento delle luci, del riscaldamento e del climatizzatore dell'ufficio e all'attivazione della funzione stand-by dei dispositivi elettronici (monitor e stampanti), fatte salve eventuali diverse esigenze tecnologiche.

3. I/le dipendenti sono tenuti ad assicurare la corretta attuazione e il rispetto delle norme sulla raccolta differenziata, utilizzando gli appositi contenitori messi a disposizione dall'Ente.

4. Ai/alle dipendenti è richiesto di assumere comportamenti rispettosi delle normative nazionali e internazionali in materia di tutela ambientale.

## Art. 14
## Prevenzione delle discriminazioni e la tutela della dignità del personale dipendente

1. Tutto il personale dipendente dell'Ordine e i suoi collaboratori/collaboratrici hanno diritto ad essere trattati con pari dignità e rispetto, perseguendo il principio di uguaglianza e parità di trattamento.
2. L'Ente intende garantire e assicurare un ambiente di lavoro ispirato alla tutela della dignità e dell'inviolabilità della persona e a principi di rispetto e correttezza nei rapporti interpersonali. L'Ente non tollera alcuna forma di discriminazione o di molestia.
3. Il presente articolo del Codice ha la finalità di informare i lavoratori e le lavoratrici, i collaboratori e le collaboratrici dei loro diritti e dei loro obblighi in merito alla prevenzione e alla rimozione di ogni comportamento discriminatorio o molesto e al mantenimento di un clima di lavoro che assicuri il rispetto della dignità di ciascuno/a.

   A tal fine viene qui richiamata la normativa vigente in tema di prevenzione delle discriminazioni:

- l'articolo 3 della Costituzione sancisce il principio dell'eguaglianza, che viene suddiviso, nei suoi rispettivi commi, in eguaglianza formale e sostanziale. In particolare, il comma 1 – riferendosi all'eguaglianza in senso formale – stabilisce che tutti i cittadini "hanno pari dignità sociale e sono eguali dinanzi alla legge, senza distinzioni di sesso, di razza religione, di opinioni politiche, di convinzioni personali e sociali". Il comma 2, palesando il concetto di eguaglianza sostanziale, afferma che è compito della Repubblica "rimuovere gli ostacoli che, limitando di fatto la libertà e l'uguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del paese";
- l'articolo 15 della legge 20 maggio 1970 n. 300, rappresenta la norma principale, a carattere generale, della legislazione ordinaria interna;
- l'art. 13 della legge 9.12.1977, n. 300 ha aggiunto, nel novero della discriminazione, quelli riferiti alla razza, alla lingua e al sesso.
- decreto legislativo n. 286 del 1998, il c.d. testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero;
- l'art. 4 del d.lgs. n. 216 del 2003, ha introdotto ulteriori fattori di discriminazione da ricomprendere nell'art. 15 dello statuto dei lavoratori, ovverosia: quelli legati alle convinzioni personali, all'handicap, all'età e all'orientamento sessuale.
- il decreto legislativo n. 215 del 2003 è la norma di attuazione della direttiva 2000/43/CE, in tema di parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica;
- dal 2003 in poi, gli interventi normativi europei sono confluiti nel c.d. codice delle pari opportunità (d.lgs. n. 198 del 2006), tutt'oggi vigente;
- per quanto attiene alle discriminazioni per motivi riconducibili all'appartenenza sessuale, le ipotesi contemplate dal decreto legislativo 25.1.2010 n. 5, ovvero quelle concernenti lo stato di gravidanza, di maternità o paternità, anche adottive, nonché i relativi diritti connessi, devono rientrare nelle fattispecie di discriminazione vietate per legge;
- tali fondamentali diritti sono richiamati anche dall'art. 14 della Convenzione Europea dei diritti dell'uomo e all'art. 21 della Carta dei diritti fondamentali dell'Unione europea.

4. Il presente Codice ha altresì la finalità di prevenire ogni atto discriminatorio, garantendo a ogni lavoratore e della lavoratrice e del collaboratore e della collaboratrice uguali condizioni senza distinzioni di età, etnia, condizione sociale, opinione politica, convinzione religiosa, genere, orientamento sessuale, disabilità e altro.

5. L'Ente non ammette alcuna forma di discriminazione e garantisce pari opportunità ed eguale dignità e imparzialità di trattamento per tutti i soggetti. Ai sensi della normativa nazionale, per principio di parità di trattamento in ambito occupazionale e lavorativo si intende l'assenza di qualsiasi discriminazione diretta o indiretta, così come di seguito definite:

a) discriminazione diretta quando, per religione, per convinzioni personali, per disabilità, per età o per orientamento sessuale, una persona è trattata meno favorevolmente di quanto sia, sia stata o sarebbe trattata un'altra in una situazione analoga;

b) discriminazione indiretta quando una disposizione, un criterio, una prassi, un atto, un patto o un comportamento apparentemente neutri possono mettere le persone che professano una determinata religione o ideologia di altra natura, le persone diversamente abili, le persone di una particolare età o di un orientamento sessuale, in una situazione di particolare svantaggio rispetto ad altre persone.

6. Tutti i lavoratori e le lavoratrici ed i collaboratori e le collaboratrici devono essere trattati esclusivamente in base alle loro capacità e competenze professionali, è proibita ogni forma di discriminazione.

7. Le tipologie di discriminazioni da sanzionare possono essere così individuate:
   - discriminazione sindacale, per l'appartenenza o meno ad un'associazione sindacale, disciplinata dall'art. 15 dello Statuto dei diritti dei lavoratori, secondo il quale è nullo qualsiasi atto o patto diretto a subordinare l'occupazione di un lavoratore alla condizione che aderisca o meno ad un'associazione sindacale, ovvero ne faccia parte. Lo stesso articolo tutela anche la libertà sindacale negativa;
   - la discriminazione di genere, disciplinata dalla Carta Costituzionale all'art. 37, in ragione del quale la donna lavoratrice ha gli stessi diritti e, a parità di lavoro, le stesse retribuzioni che spettano al lavoratore, quella diretta viene specificatamente descritta dall'art. 25 co. 1 del d.lgs. 198 del 2006, secondo cui è discriminatorio "qualsiasi atto, patto o comportamento che produca un effetto pregiudizievole discriminando le lavoratrici o i lavoratori in ragione del loro sesso e, comunque, il trattamento meno favorevole rispetto a quella di un'altra lavoratrice o di un altro lavoratore in situazione analoga". Il divieto di discriminazione indiretta si ha "quando una disposizione, un criterio, una prassi, un atto, un patto o un comportamento apparentemente neutri mettono o possono mettere i lavoratori di un determinato sesso in una posizione di particolare svantaggio rispetto a lavoratori dell'altro sesso, salvo che riguardino requisiti essenziali allo svolgimento dell'attività lavorativa, purché l'obiettivo sia legittimo e i mezzi impiegati per il suo conseguimento siano appropriati e necessari";
   - le discriminazioni per ragioni politiche di cui all'art. 15 della legge n. 300/1970;
   - le discriminazioni razziali e per origine etnica di cui al d.lgs. n. 215/2003
   - le discriminazioni per religione, convinzioni personali, handicap, età, e orientamento sessuale di cui al d.lg.s. n. 216 del 2003;
   - Inoltre, la legge 30 novembre del 2017 n. 179, riferendosi alla possibilità che il lavoratore segnali condotte illecite delle quali è venuto a conoscenza, prevede la nullità di qualsiasi atto pregiudizievole che venga attuato nei confronti del lavoratore segnalante, in quanto discriminatorio e ritorsivo.

8. Le tipologie di molestie da sanzionare, così come definite dalla Legge 15 gennaio 2021, nr. 4, possono essere così individuate:

   a) «molestie» nel mondo del lavoro, ovvero un insieme di pratiche e di comportamenti inaccettabili, o la minaccia di porli in essere, sia in un'unica occasione, sia ripetutamente,

che si prefiggano, causino o possano comportare un danno fisico, psicologico, sessuale o economico, e include la violenza e le molestie di genere;

b) «molestie di genere» ovvero le molestie nei confronti di persone in ragione del loro sesso o genere, o che colpiscano in modo sproporzionato persone di un sesso o genere specifico, ivi comprese le molestie sessuali.

## Art. 14 Bis
## Procedura di trattazione dei casi di discriminazioni o molestie, responsabilità disciplinari e tutele esterne

1. I lavoratori e le lavoratrici ed i collaboratori e le collaboratrici possono inviare segnalazioni di possibili comportamenti o pratiche discriminatorie o moleste e, in ogni caso, non conformi a quanto stabilito nel presente Codice di Comportamento, al/alla Segretario/a dell'Ordine – quale responsabile della segreteria. Coloro che invece abbiano assistito a un comportamento discriminatorio e/o configurabile quale molestia, devono immediatamente segnalarlo alla medesima figura Istituzionale. Spetta al/alla Segretario/a il compito di istruire l'iter per l'accertamento dei fatti e l'eventuale avvio del procedimento disciplinare.
2. Costituisce illecito disciplinare il compimento di atti discriminatori e molestie sul luogo di lavoro, nelle fattispecie indicate all'articolo 14. Costituisce altresì illecito disciplinare il compiere atti di ritorsione contro chi denuncia una discriminazione e/o una molestia o intenda rendere o renda testimonianza.

   Le sanzioni verranno comminate in proporzione alla gravità dell'atto e in funzione della tutela della vittima, a prescindere dalla posizione ricoperta dalla persona coinvolta. Il procedimento disciplinare relativo a fatti e circostanze previsti dal presente Codice come atti di discriminazione e molestie, è condotto ai sensi di quanto previsto dal Regolamento dei procedimenti disciplinari del personale dipendente dell'Ordine dei Medici Chirurghi degli Odontoiatri di Padova, approvato con deliberazione n. 63 del 09.03.2021 e pubblicato nel sito istituzionale dell'Ordine.

## Art. 15
## Rapporti con il pubblico

1. La/Il dipendente nei rapporti con il pubblico, opera con spirito di servizio, correttezza, cortesia e disponibilità e, nel rispondere alla corrispondenza, a chiamate telefoniche e ai messaggi di posta elettronica, opera nella maniera più completa, tempestiva e accurata possibile. Qualora non sia competente per posizione rivestita o per materia, indirizza l'interessato al funzionario competente del medesimo Ente.

2. La/Il dipendente, fatte salve le norme sul segreto d'ufficio, fornisce le spiegazioni che gli siano richieste in ordine al comportamento proprio e di altri dipendenti dell'ufficio dei quali ha la responsabilità o il coordinamento. Nelle operazioni da svolgersi e nella trattazione delle pratiche il dipendente rispetta, salvo diverse esigenze di servizio o diverso ordine di priorità stabilito dall'Ente, l'ordine cronologico e non rifiuta prestazioni a cui sia tenuto con motivazioni generiche. La/Il dipendente rispetta gli appuntamenti con gli utenti e risponde senza ritardo ai loro reclami.

3. Salvo il diritto di esprimere valutazioni e diffondere informazioni a tutela dei diritti sindacali, la/il dipendente si astiene da dichiarazioni pubbliche offensive nei confronti dell'Ente anche a mezzo web, social network, blog, forum o altri media.

4. La/Il dipendente poiché svolge la sua attività lavorativa in un Ente che fornisce servizi al pubblico, cura il rispetto degli standard di qualità e di quantità fissati dall'Ente anche nell'apposita carta dei servizi. Egli opera al fine di assicurare la continuità del servizio, di consentire agli utenti la scelta tra i diversi erogatori e di fornire loro informazioni sulle modalità di prestazione del servizio e sui livelli di qualità. Nel rapportarsi col pubblico la/il dipendente adotta un linguaggio comprensibile e flessibile in ragione dell'interlocutore, avendo cura di assistere i cittadini che, per ragioni di età, salute, o altra condizione, si trovino in oggettiva difficoltà nel rapportarsi con la pubblica amministrazione.

5. La/Il dipendente non assume impegni né anticipa l'esito di decisioni o azioni proprie o altrui inerenti all'ufficio, al di fuori dei casi consentiti. Non fornisce informazioni in merito ad attività o procedimenti in corso presso l'Ente e non rilascia informazioni relative ad atti e provvedimenti prima della loro comunicazione alle parti. Non fa uso delle informazioni non disponibili al pubblico o non rese pubbliche, ottenute anche in via confidenziale nell'attività dell'Ente, a fini privati e deve evitare situazioni e comportamenti che possano ostacolare il corretto adempimento dei compiti o nuocere agli interessi o all'immagine dell'Ente.

6. Fornisce informazioni e notizie relative ad atti od operazioni amministrative, in corso o conclusi, nelle ipotesi previste dalle disposizioni di legge e regolamentari in materia di accesso. Rilascia copia ed estratti di atti o documenti secondo la sua competenza, con le modalità stabilite dalle norme in materia di accesso e dai regolamenti della propria amministrazione.

7. La/Il dipendente osserva il segreto d'ufficio e la normativa in materia di tutela e trattamento dei dati personali e, qualora sia richiesto oralmente di fornire informazioni, atti, documenti non accessibili tutelati dal segreto d'ufficio o dalle disposizioni in materia di dati personali, informa il richiedente dei motivi che ostano all'accoglimento della richiesta. Qualora non sia competente a provvedere in merito alla richiesta cura, sulla base delle disposizioni interne, che la stessa venga inoltrata all'ufficio competente della medesima amministrazione.

8. Nei rapporti con il pubblico, la/il dipendente rispetta i termini relativi alle comunicazioni e al procedimento previsti dalle disposizioni normative e regolamentari vigenti.

9. L'Ente favorisce nei rapporti con il pubblico e con le altre pubbliche amministrazioni, l'uso di strumenti e mezzi di comunicazione e corrispondenza in forma telematica.

10. La/Il dipendente è tenuto a rispondere tempestivamente alle comunicazioni di posta elettronica con lo stesso mezzo, riportando tutti gli elementi idonei alla identificazione della/del responsabile del procedimento e della esaustività della risposta.

11. Il/la dipendente deve osservare scrupolosamente le disposizioni che regolano l'accesso ai locali dell'Ente e non introdurre, salvo che non siano debitamente autorizzate, persone estranee all'Ente stesso in locali non aperti al pubblico.

## Art. 16
## Utilizzo delle tecnologie informatiche e dei mezzi di informazione e social media da parte dei dipendenti pubblici, anche al fine di tutelare l'immagine della pubblica amministrazione (L. 79/2022)

1. L'Ente utilizza i social media e altri mezzi di informazione nell'ambito delle proprie finalità istituzionali, per informare sulle proprie attività e iniziative, segnalare eventi, manifestazioni, iniziative culturali e diffondere notizie di pubblica utilità. L'utilizzo scorretto dei mezzi di informazione e dei social media può danneggiare anche gravemente l'immagine dell'Ente e della pubblica amministrazione e la reputazione degli organi istituzionali e del personale, esponendo l'Ente a richieste risarcitorie nel caso vengano pubblicati contenuti offensivi o lesivi del diritto d'autore o di proprietà intellettuale. Il personale ed i collaboratori che gestiscono le attività connesse ai social media e ai mezzi di informazione devono pertanto avere un comportamento di massima prudenza, mettendo sempre a conoscenza il Presidente del materiale postato o condiviso.

2. L'Ordine si riserva di segnalare eventuali casi di violazione della proprietà intellettuale o di abuso dell'identità e dell'immagine dell'Ente, anche tramite account falsi (cosiddetti fake), ai gestori delle piattaforme e, se necessario, alle autorità giudiziarie competenti.

3. L'Ente, previa verifica dell'attendibilità della fonte, valuta la pubblicazione di contenuti di pubblico interesse prodotti da terzi. Inoltre, l'Ente non è responsabile della condivisione di post dallo stesso pubblicati con contenuti di terzi, la ripubblicazione in altro contesto, eventuali rielaborazioni e altre forme di trattamento.

4. Il personale ed i collaboratori che si occupano della pubblicazione dei messaggi sui social network istituzionali sono responsabili dei contenuti che inviano, del linguaggio che deve essere appropriato e di natura istituzionale, del materiale fotografico e video utilizzato e delle opinioni che esprimono, in particolare:
   - devono evitare litigi e non rispondere mai alle provocazioni e ai contenuti inappropriati o diffamatori, postati da utenti privati sui canali istituzionali;
   - devono astenersi dal pubblicare post o commenti che contengano opinioni personali o in contrasto con l'Ente o che abbiano un contenuto politico o propagandistico;
   - devono mantenere il segreto d'ufficio, astenendosi dal divulgare o dall'agevolare la divulgazione di informazioni su attività, servizi, progetti e documenti non ancora resi pubblici, ovvero su decisioni da assumere e provvedimenti relativi a procedimenti anche di natura disciplinare in corso;
   - non devono utilizzare account istituzionali per fini diversi da quelli connessi all'attività dell'Ente o ad essa riconducibile nel caso in cui l'utilizzo possa compromettere la sicurezza o la reputazione dello stesso.

   Il personale ed i collaboratori che utilizzano gli account dei social media di cui sono titolari possono esprimere la propria opinione attraverso la pubblicazione di commenti e post, astenendosi da dichiarazioni offensive o altri interventi che possano ledere il prestigio o l'immagine dell'Ente di appartenenza, dei colleghi, dei collaboratori e della Pubblica Amministrazione in generale.

5. Il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'Ente di appartenenza o della pubblica amministrazione in generale e non può trattare comunicazioni, afferenti direttamente o indirettamente al servizio, attraverso conversazioni pubbliche svolte su qualsiasi piattaforma digitale. Se poi tali comportamenti sono perpetrati sulle piattaforme social con indicazione dirette o ricavabili della qualifica professionale o di appartenenza del dipendente, costituiscono elementi valutabili ai fini disciplinari. Chi presta la propria attività lavorativa, rappresentativa o funzionale dell'Ente non può prescindere dalla consapevolezza di dover conformare la propria condotta al dovere costituzionale di servire esclusivamente la nazione con disciplina ed onore e di rispettare i principi di buon andamento e imparzialità dell'Ente.

6. Ai dipendenti e collaboratori è pertanto fatto divieto, per ragioni estranee al proprio rapporto con l'Ente, di diffondere informazioni, conversazioni e documenti inerenti direttamente o indirettamente le attività dell'Ente attraverso l'utilizzo di qualsiasi piattaforma digitale. Ai dipendenti e collaboratori è fatto divieto di utilizzare su account personali il logo e le immagini di proprietà dell'Ente.

7. È fatto divieto al/alla dipendente di pubblicare, con qualunque mezzo, immagini ritraenti colleghi/e, collaboratori o utenti salvo il caso in cui sia stato esplicitamente e preventivamente autorizzato per iscritto da ciascun interessato, ovvero di diffondere foto, video e audio che possano ledere l'immagine dell'Ordine o che siano idonee ad arrecare pregiudizio all'onorabilità, alla riservatezza o alla dignità delle persone e degli organi dell'Ente, ovvero che possano suscitare riprovazione o strumentalizzazione; il/la dipendente non può inoltre pubblicare immagini dei locali in cui svolge l'attività lavorativa, salvo che sia stato esplicitamente autorizzato per iscritto dal /dalla Responsabile di riferimento per motivate ragioni di servizio nel rispetto delle norme vigenti.

8. Nell'uso dei social media il/la dipendente si astiene dall'utilizzo di parole o simboli idonei ad istigare l'odio o la discriminazione.

9. Fatto salvo il diritto di esprimere valutazioni e diffondere informazioni nell'esercizio e a tutela dei diritti sindacali e fermo restando il principio costituzionale di libertà di espressione del proprio pensiero fuori dall'esercizio delle funzioni, in considerazione della sua qualità di dipendente pubblico, il/la dipendente si impegna a mantenere un comportamento corretto, ineccepibile ed esemplare anche nella partecipazione a discussioni su chat, blog, social forum on line, ispirato all'equilibrio, alla ponderatezza, al rispetto delle altrui opinioni e ai doveri inerenti alla funzione, mantenendo un atteggiamento responsabile e consapevole di riserbo e cautela nell'esprimere, anche via web, opinioni, valutazioni, critiche su fatti ed argomenti che interessano l'opinione pubblica o che possano coinvolgere la propria attività svolta all'interno dell'Ordine.

10. La segnalazione di problematiche, carenze e di ogni altra disfunzione o anomalia inerente alle attività svolte o ai servizi di appartenenza va fatta dal/dalla dipendente seguendo le procedure previste all'interno dell'Ordine e nel rispetto delle competenze istituzionali assegnate.

11. Il/La dipendente che accede ad un social network con un account personale, mediante dispositivo proprio, per motivi estranei all'attività di servizio, non deve sottrarre in ogni caso tempo allo svolgimento dell'attività lavorativa a cui è tenuto.

12. Le caselle di posta elettronica sono messe a disposizione dall'Ente per usi esclusivamente professionali, l'improprio uso personale, comporta assunzione diretta di responsabilità circa i contenuti dei messaggi da parte di chi li invia.

## Art. 17
## Misurazione della performance

Il Consiglio direttivo, pur non essendo tenuto ad effettuare la valutazione delle performance del personale, al fine della distribuzione del compenso incentivante, definito con la contrattazione decentrata, ha cura di individuare annualmente gli obiettivi generali ed individuali del personale con apposito deliberato. In fase di assegnazione, il raggiungimento degli obiettivi viene sottoposto ad una valutazione.

## Art. 18
## Disposizioni particolari per le/i responsabili di area e le/i titolari di incarichi dirigenziali

1. Ferma restando l'applicazione delle altre disposizioni del Codice, le norme del presente articolo si applicano alle/ai funzionari responsabili di posizione organizzativa.

2. La/Il responsabile svolge con diligenza le funzioni ad esso spettanti in base all'atto di conferimento dell'incarico, persegue gli obiettivi assegnati e adotta un comportamento organizzativo adeguato all'assolvimento dell'incarico. Inoltre, prima di assumere le sue funzioni, comunica all'Ente le partecipazioni azionarie e gli altri interessi finanziari che possano porlo in conflitto di interessi con la funzione pubblica che svolge e dichiara se ha parenti e affini entro il secondo grado, coniuge o convivente che esercitano attività politiche, professionali o economiche che li pongano in contatti frequenti con l'ufficio che dovrà dirigere o che siano coinvolti nelle decisioni o nelle attività inerenti all'ufficio. La/Il responsabile fornisce le informazioni sulla propria situazione patrimoniale e le dichiarazioni annuali dei redditi soggetti all'imposta sui redditi delle persone fisiche previste dalla legge.

   La/Il responsabile fornisce in maniera completa ed esaustiva, tempestivamente e comunque non oltre 30 giorni dall'assunzione dell'incarico le comunicazioni di cui al comma 3 e le informazioni sulla propria situazione patrimoniale. Annualmente si provvede all'aggiornamento delle comunicazioni e delle informazioni di cui sopra.

   La/Il responsabile assume atteggiamenti leali e trasparenti e adotta un comportamento esemplare e imparziale nei rapporti con i colleghi, i collaboratori e i destinatari dell'azione amministrativa. La/Il responsabile cura, altresì, che le risorse assegnate al suo ufficio siano utilizzate per finalità esclusivamente istituzionali e, in nessun caso, per esigenze personali.

   La/Il responsabile cura, compatibilmente con le risorse disponibili, il benessere organizzativo nella struttura a cui è preposto, favorendo l'instaurarsi di rapporti cordiali e rispettosi tra i collaboratori, assume iniziative finalizzate alla circolazione delle informazioni, alla formazione e all'aggiornamento del personale, all'inclusione e alla valorizzazione delle differenze di genere, di età e di condizioni personali.

   La/Il responsabile assegna l'istruttoria delle pratiche sulla base di un'equa ripartizione del carico di lavoro, tenendo conto delle capacità, delle attitudini e delle professionalità del personale a sua disposizione. Il responsabile affida gli incarichi aggiuntivi in base alla professionalità e, per quanto possibile, secondo criteri di rotazione.

   La/Il responsabile svolge la valutazione del personale cui è preposto con imparzialità e rispettando le indicazioni ed i tempi prescritti.

   La/Il responsabile intraprende con tempestività le iniziative necessarie ove venga a conoscenza di un illecito, attiva e conclude, se competente, il procedimento disciplinare, ovvero segnala tempestivamente l'illecito all'autorità disciplinare, prestando ove richiesta la propria collaborazione e provvede ad inoltrare tempestiva denuncia all'autorità giudiziaria penale. Nel caso in cui riceva segnalazione di un illecito da parte di una/un dipendente, adotta ogni cautela di legge affinché sia tutelato la/il segnalante e non sia indebitamente rilevata la sua identità nel procedimento disciplinare, ai sensi dell'articolo 54 bis del decreto legislativo n.165 del 2001.

La/Il responsabile, nei limiti delle sue possibilità, evita che notizie non rispondenti al vero quanto all'organizzazione, all'attività e ai dipendenti pubblici possano diffondersi. Favorisce la diffusione della conoscenza di buone prassi e buoni esempi al fine di rafforzare il senso di fiducia nei confronti dell'Ente.

3. I destinatari possono segnalare per iscritto al responsabile Anticorruzione eventuali disparità nella ripartizione dei carichi di lavoro da parte del responsabile. La/Il Responsabile Anticorruzione accerta l'effettiva sussistenza della disparità nella ripartizione dei carichi di lavoro, sia sotto un profilo qualitativo che quantitativo. Qualora, all'esito di tale accertamento, emerga l'effettiva disparità segnalata la/il Responsabile Anticorruzione adotta i provvedimenti ritenuti opportuni al fine di riequilibrare la distribuzione dei carichi di lavoro, ovvero dispone l'archiviazione della segnalazione, non dando luogo a procedere.

4. La/Il responsabile è tenuto ad osservare e vigilare sul rispetto da parte dei dipendenti addetti alla propria struttura delle regole in materia di incompatibilità, cumulo di impieghi e incarichi di lavoro, al fine di evitare pratiche illecite. Qualora la/il responsabile dell'area accerti la violazione di tali regole, la segnala tempestivamente e per iscritto all'ufficio competente per i procedimenti disciplinari, al fine dell'adozione dei consequenziali provvedimenti, ovvero dell'archiviazione.

## Art. 19
## Contratti ed altri atti negoziali

1. Nella conclusione di accordi e negozi e nella stipulazione di contratti per conto dell'Ente, nonché nella fase di esecuzione degli stessi, la/il dipendente non ricorre a mediazione di terzi, né corrisponde o promette ad alcuna utilità a titolo di intermediazione, né per facilitare o aver facilitato la conclusione o l'esecuzione del contratto. Il presente comma non si applica ai casi in cui l'Ente abbia deciso di ricorrere all'attività di intermediazione professionale.

2. La/Il dipendente non conclude, per conto dell'Ente, contratti d'appalto, fornitura, servizio, finanziamento o assicurazione con imprese con le quali abbia stipulato contratti a titolo privato o ricevuto altre utilità nel biennio precedente, ad eccezione di quelli conclusi ai sensi dell'art.1342 del Codice civile. Nel caso in cui l'Ente concluda contratto d'appalto, fornitura, servizio, finanziamento o assicurazione, con imprese con le quali la/il dipendente abbia concluso contratti a titolo privato o ricevuto altre utilità nel biennio precedente, questi si astiene dal partecipare all'adozione delle decisioni ed alle attività relative all'esecuzione del contratto, redigendo verbale scritto di tale astensione da conservare agli atti dell'ufficio.

3. La/Il dipendente che conclude accordi o negozi ovvero stipula contratti a titolo privato, ad eccezione di quelli conclusi ai sensi dell'articolo 1342 del Codice civile, con persone fisiche o giuridiche private con le quali abbia concluso, nel biennio precedente, contratti di appalto, fornitura, servizio, finanziamento ed assicurazione, per conto dell'Ente, ne informa per iscritto il responsabile dell'ufficio.

4. Se nelle situazioni di cui ai commi 2 e 3 si trova la/il responsabile, questi informa per iscritto la/il Segretaria/o dell'Ordine, responsabile della organizzazione e gestione della Segreteria dell'Ordine.

5. La/Il dipendente che riceva, da persone fisiche o giuridiche partecipanti a procedure negoziali nelle quali sia parte l'Ente, rimostranze orali o scritte sull'operato dell'ufficio o su quello dei

propri collaboratori, ne informa immediatamente, di regola per iscritto, la/il Segretaria/o dell'Ordine.

## Art. 20

## Vigilanza, monitoraggio e attività formative

1. Ai sensi dell'art. 54, comma 6, del decreto legislativo 30 marzo 2001, n. 165, la/il Presidente, la/il Segretaria/o dell'Ordine, la/il dipendente in posizione di elevata professionalità e la/il RPCT
   - vigilano sull'applicazione del codice di comportamento generale e del presente codice speciale;
   - curano l'aggiornamento del codice di comportamento dell'Ente, l'esame delle segnalazioni di violazione dei codici di comportamento, la raccolta delle condotte illecite accertate e sanzionate, assicurando le garanzie di cui all'articolo 54-bis del decreto legislativo n. 165 del 2001.
2. La/Il responsabile della prevenzione della corruzione cura la diffusione della conoscenza dei codici di comportamento all'interno dell'Ente, il monitoraggio annuale sulla loro attuazione, ai sensi dell'articolo 54, comma 7, del decreto legislativo n.165 del 2001, la pubblicazione sul sito istituzionale e della comunicazione all'Autorità nazionale anticorruzione, di cui all'articolo 1, comma 2, della legge 6 novembre 2012, n.190, dei risultati del monitoraggio.
3. Ai fini dell'attivazione del procedimento disciplinare per violazione dei codici di comportamento, l'ufficio procedimenti disciplinari può chiedere all'Autorità nazionale anticorruzione parere facoltativo secondo quanto stabilito dall'articolo 1, comma 2, lettera d), della legge n.190 del 2012.
4. Al personale dipendente e ai titolari di incarichi politici sono rivolte attività formative in materia di trasparenza e integrità, che consentano di conseguire una piena conoscenza dei contenuti del codice di comportamento, nonché un aggiornamento annuale e sistematico sulle misure e sulle disposizioni applicabili in tali ambiti.
5. In accordo con quanto previsto dalla lg. 79/2022 i/le dipendenti dell'OMCeO di Padova ed i titolari di incarichi politici si impegnano a partecipare attivamente ai corsi che verranno organizzati o proposti dall'Ente sui temi dell'etica pubblica e sul comportamento etico.

## Art. 21
## Responsabilità conseguente alla violazione dei doveri del codice

1. La violazione degli obblighi previsti dal presente codice rappresenta violazione di un principio etico ed integra comportamenti contrari ai doveri d'ufficio.
2. Per i/le dipendenti dell'Ordine essa è fonte di responsabilità disciplinare accertata all'esito del procedimento disciplinare, nel rispetto dei principi di gradualità e proporzionalità delle sanzioni. Ai fini della determinazione del tipo e dell'entità della sanzione disciplinare concretamente applicabile, la violazione è valutata in ogni singolo caso con riguardo alla gravità del comportamento ed all'entità del pregiudizio, anche morale, derivatone al decoro o al prestigio dell'Ente di appartenenza. Per quanto concerne il procedimento disciplinare nei confronti dei dipendenti dell'Ordine si richiama la Convenzione stipulata con la Federazione Nazionale, approvata con deliberazione n. 63 del 09.03.2021, e si applica il relativo Regolamento pubblicato sul sito istituzionale dell'Ente. L'accertamento della violazione del codice di comportamento incide negativamente sulla valutazione relativa al raggiungimento degli obiettivi incentivanti individuali a prescindere dal livello di raggiungimento degli altri risultati.
3. Gli obblighi di condotta previsti dal presente codice si estendono a tutti i collaboratori o

consulenti, con qualsiasi tipologia di contratto o incarico e a qualsiasi titolo e nei confronti dei collaboratori a qualsiasi titolo di imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione. A tale fine, negli atti di incarico o nei contratti di acquisizioni delle collaborazioni, delle consulenze o dei servizi, le amministrazioni inseriscono apposite disposizioni o clausole di risoluzione o decadenza del rapporto in caso di violazione degli obblighi derivanti dal presente codice.

4. Restano ferme le ipotesi in cui la violazione delle disposizioni contenute nel presente codice, nonché dei doveri e degli obblighi previsti dalla sottosezione Anticorruzione e Trasparenza del PIAO, dà luogo anche a responsabilità penale, civile, amministrativa o contabile del destinatario.

## Art. 22

## Disposizioni finali e abrogazioni

1. L'Ente dà la più ampia diffusione al presente codice, pubblicandolo sul proprio sito internet istituzionale, nella sezione denominata "Amministrazione trasparente", nonché con invio tramite e-mail a tutti la/i proprie/i dipendenti e alle/ai titolari di contratti di consulenza o collaborazione a qualsiasi titolo, anche professionale, alle/ai titolari di organi e di incarichi negli uffici di diretta collaborazione dei vertici politici dell'Ente, nonché alle/ai collaboratrici/tori a qualsiasi titolo, anche professionale, di imprese fornitrici di servizi in favore dell'Ente.

2. L'Ente, contestualmente alla sottoscrizione del contratto di lavoro o, in mancanza, all'atto di conferimento dell'incarico, consegna e fa sottoscrivere ai nuovi assunti, con rapporti comunque denominati, copia del codice di comportamento.

3. Costituisce parte integrante del presente regolamento il documento "Social media policy interna sull'uso dei social da parte dei dipendenti dell'Ordine.

4. Si intendono e restano ferme l disposizioni contenute nel DGPR 679/2016 *"Regolamento generale sulla protezione dei dati"*.

(A1

# SOCIAL MEDIA POLICY- ALLEGATO AL REGOLAMENTO DI COMPORTAMENTO DEI DIPENDENTI DELL'ORDINE –

Sommario



## PREMESSA

La presente "Social Media Policy" ha l'obiettivo di specificare le regole di utilizzo dei social network da parte del personale operante presso l'Ordine dei Medici Chirurghi e Odontoiatri di Padova.
Essa costituisce parte integrante del Codice di Comportamento dell'Ordine.
Dando seguito a quanto già disciplinato attraverso il Regolamento approvato con deliberazione **n. 14 del 16.01.2024** pur sostenendo come principio quello di favorire le attività di condivisione delle informazioni da parte dei propri dipendenti, ritiene tuttavia indispensabile informarli delle possibili ricadute negative che un uso improprio dei social, sia pure involontario, può determinare sia per l'immagine dell'Ordine, sia per gli altri operatori, sia infine per l'autore stesso.
Si rammenta che gli obblighi di condotta previsti dal "Codice" si estendono, per quanto compatibili, anche a tutti coloro che, direttamente o indirettamente, stabilmente o temporaneamente, instaurano rapporti o relazioni con l'Ordine ed operano e concorrono a perseguirne gli obiettivi.
Questo documento in particolare indica:

- i soggetti incaricati di gestire i suddetti profili social dell'Ordine;
- le regole di comportamento che dipendenti e collaboratori devono osservare nell'uso dei siti di social networking.

## 1. USO DEI SOCIAL IN RAPPRESENTANZA DELL'ORDINE

La pubblicazione sui profili social dell'Ordine spetta all'Ufficio Stampa che la presidia in via diretta ovvero per il tramite dei servizi addetti alla comunicazione ordinistica.
In particolare, questi hanno la funzione di gestire gli interventi sulle pagine aziendali in nome e per conto dell'Ordine. Esclusivamente i soggetti in questione, sulla base delle indicazioni del Consiglio Direttivo, definisce quali contenuti è opportuno e utile condividere in rete, nei profili istituzionali dell'Ordine.
Su espressa autorizzazione del Presidente o del Consiglio Direttivo, potranno essere autorizzati profili social istituzionali specifici di determinate strutture e/o servizi. In questo caso la funzione di amministrazione sarà a carico di una figura esponente della struttura/servizio interessata, ferma restando l'opportunità di condividere con i servizi designati dalla direzione le pubblicazioni da fare a valenza generale e/o istituzionale.
Periodicamente l'Ente predispone delle verifiche che permettano di controllare che non siano stati creati profili social dell'Ordine non "ufficiali" e che il logo aziendale non sia usato impropriamente.
Nella gestione dei profili dell'Ente si provvede inoltre ad eliminare commenti/contenuti non appropriati, quali frasi ingiuriose e offensive, commenti osceni, contenuti illegali o classificabili come spam.
In accordo e con il supporto dell'ufficio affari generali, ove ritenuto necessario, ogni volta che si intercetteranno situazioni che possano anche solo ingenerare confusione rispetto alla titolarità di un profilo e di altri contenuti, si interverrà per eliminare messaggi che a vario titolo possono ledere gli interessi o, più genericamente, l'immagine e la reputazione dell'Ordine.

## 2. USO PRIVATO DEI SOCIAL

Il dipendente che accede ai social network con il proprio profilo personale deve ricordare che si tratta di spazi potenzialmente pubblici e come tali vanno dunque considerati: anche nel caso in cui l'utilizzo avvenga per interessi personali (ad esempio per condividere contenuti, immagini, video, informazioni o per stabilire relazioni di tipo personale e/o lavorativo con i propri "amici" o contatti), dovrà pertanto impegnarsi a mantenere un comportamento corretto ed eticamente in linea con il ruolo di dipendente pubblico.

### COMMENTI IN NOME E PER CONTO DELL'ORDINE

Salvo le figure autorizzate – i servizi addetti alla comunicazione o chi, di volta in volta riceverà specifico mandato – il dipendente non è autorizzato a parlare in nome e per conto dell'Ordine.

Tuttavia, allorquando il dipendente risultasse coinvolto in una discussione che interessi l'Ordine stesso, è opportuno che sia reso esplicito il suo ruolo nella consapevolezza che gli utenti dei social– soprattutto in discussioni su temi attinenti l'attività dell'Ordine e, in generale, del comparto sanitario e socio-sanitario nonché delle istituzioni pubbliche – identificano il dipendente dell'Ordine come tale e ne interpretano commenti e opinioni anche in relazione al suo ruolo di dipendente pubblico e dell'Ordine dei Medici.

**ATTENDIBILITÀ DELLE FONTI**

Occorre verificare sempre la attendibilità delle fonti delle informazioni che si decide di postare sui propri profili social, che riguardino l'Ordine, ma non provengano dallo stesso.

**CREAZIONE PROFILI**

Non è consentito istituire profili sui social utilizzando il nome e/o il logo dell'Ordine dei Medici, inducendo erroneamente gli utenti a ritenere di interagire con la stessa. Gli unici profili ufficiali sono quelli gestiti e autorizzati dall'Ordine stesso

**USO DEL LOGO DELL'ORDINE**

Anche sui social, l'utilizzo dei caratteri distintivi dell'Ente (logo, ragione sociale) potrà avvenire esclusivamente su specifica autorizzazione secondo i criteri ordinariamente ammessi per la Concessione del patrocinio e l'uso del logo.

## 3. REGOLE MINIME DI COMPORTAMENTO

Nell'affacciarsi in rete vi sono regole di comportamento al cui rispetto sono chiamati tutti i dipendenti/collaboratori dell'Ordine.
In generale, è indispensabile osservare sempre un atteggiamento rispettoso della organizzazione presso cui si lavora, anche al fine di evitare situazioni di conflitto con l'Ente, sia in contesti pubblici che privati, anche in coerenza con gli obblighi enunciati dal Codice di comportamento di cui questa policy rappresenta una specificazione.

**ESERCIZIO DEL DIRITTO DI CRITICA**

Fermi restando il legittimo esercizio delle libertà sindacali e del diritto di critica, occorre evitare di esprimere giudizi personali, commenti o dichiarazioni pubbliche lesive dell'immagine relativa alle attività istituzionali della amministrazione pubblica e dell'Ordine, tali da contribuire a minare il rapporto di fiducia fra il cittadino ed i servizi pubblici, oppure offensive nei confronti di singoli o gruppi di dipendenti.

**RISPETTO DEL SEGRETO D'UFFICIO**

Occorre tenere sempre presente che l'attività lavorativa è soggetta ad una serie di vincoli quali il segreto d'ufficio o quello professionale, nonché alla tutela della riservatezza rispetto ai dati conosciuti in ambito lavorativo: è dunque indispensabile astenersi dall'affrontare sui social
questioni lavorative specifiche o tematiche legate alla attività, che rischino di violare tali doveri.
Analogamente è vietato divulgare in rete informazioni riservate, come la corrispondenza interna, informazioni di terze parti o relative ad attività lavorative, servizi, progetti e documenti non ancora resi pubblici.

**RISPETTO DELLE MISURE DI SICUREZZA INFORMATICA**

Si ricorda la necessità del rispetto della normativa in materia di protezione dei dati personali, necessaria a garantire la sicurezza, l 'integrità, la disponibilità e l'efficienza dei sistemi informativi dell'Ordine.

**IMMAGINI AMBIENTE DI LAVORO**

Non è consentito diffondere immagini legate all'ambiente di lavoro, che possano configurare violazione della privacy di utenti e dipendenti o contribuiscano a ledere decoro e professionalità dei contesti lavorativi, contribuendo cosi' a minare il rapporto di fiducia che dovrebbe sempre legare i professionisti ai propri assistiti.

Un comportamento pubblico o privato non corretto potrebbe dare origine, a seconda della gravità, alla attivazione di procedimenti disciplinari o addirittura alla segnalazione all'autorità giudiziaria competente nelle ipotesi in cui la violazione delle regole sopraelencate sia fonte di responsabilità penale, civile, amministrativa o contabile.

## 4. L'USO DEI SISTEMI DI MESSAGGISTICA ISTANTANEA

I sistemi di messaggistica (WhatsApp, Telegram, Google chat, Facebook Messenger solo per citare quelli attualmente più utilizzati) possono essere utilizzati come strumenti di lavoro, avvalendosi di tutte le cautele previste dalla normativa vigente in materia di trattamento di dati personali e seguendo le disposizioni contenute nel presente regolamento.

(A 2

# LINEE GUIDA SUL CORRETTO UTILIZZO DELLE TECNOLOGIE INFORMATICHE E DEGLI ARCHIVI

# LINEE GUIDA SUL CORRETTO UTILIZZO DELLE TECNOLOGIE INFORMATICHE E DEGLI ARCHIVI

**PREMESSA**

Le presenti Linee Guida sono emanate dall'Ordine dei Medici Chirurghi e degli Odontoiatri di Padova (" di seguito denominato Ente") ai sensi della vigente normativa in materia di protezione dei dati personali delle persone fisiche, nazionale ed europea, con particolare riferimento al Regolamento Europeo 2016/679 in materia di protezione dei dati personali (nel seguito "Regolamento UE") – e completano ogni altra procedura interna dell'Ente a protezione dei dati personali, con particolare riferimento alle misure di sicurezza poste a tutela dei trattamenti effettuati con strumenti elettronici di qualunque natura e tipologia a tutela dei dati personali disposti in archivi informatici dell'Ente o di fornitori terzi di servizi in cloud.

L'Ente nell'espletamento della sua attività istituzionale opera prestando attenzione alla sicurezza delle informazioni e dei dati, perseguendo adeguati livelli di sicurezza del proprio sistema informativo e adottando idonee misure organizzative e tecnologiche, volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni sia per proteggere i dati personali detenuti, sia per difendere tutte le informazioni presenti nelle banche dati informatiche (di seguito denominati "Database").

**A chi si rivolge questo documento e la portata dello stesso**

Il presente documento definisce le regole e le condizioni per l'utilizzo degli strumenti informatici, da parte dei dipendenti e dei componenti gli Organi Istituzionali e Commissioni dell'Ente e per quanto compatibili a tutti coloro che, in virtù di un incarico qualsiasi titolo (collaboratori, consulenti, stagisti, fornitori, etc.), utilizzano o forniscono strumenti informatici o servizi in favore dell'Ente ("Destinatari").

Le presenti linee guida integrano il Codice di Comportamento comportamentale dell'Ente emanato con Deliberazione N° 14 del 16.01.2024 e sono inserite in una sezione dedicata dello stesso, ai sensi ai sensi dell'art. 54 co. 1 bis del D.Lgs. 30 marzo 2001 n. 165.

Scopo di questo documento è anche quello di essere un valido supporto alle funzioni e alle attribuzioni della funzione di Responsabile della Transizione Digitale dell'Ente il quale deve operare in piena autonomia col supporto del Responsabile della protezione dei dati ("DPO") e dell'Amministratore di sistema ("ADS").

Tali prescrizioni integrano le specifiche istruzioni fornite a tutti gli Autorizzati art. 29 Regolamento UE, in attuazione della normativa in materia di protezione dei dati personali.

Le informazioni contenute nelle presenti Linee Guida vengono rilasciate, pera quanto compatibili, anche ai sensi dell'art. 13 del GDPR e costituiscono, quindi, parte integrante dell'informativa rilasciata a tutti i soggetti interessati e dell'art. 4 dello Statuto dei Lavoratori Legge n. 300/1970.

**Finalità del documento**

Il presente documento definisce e detta ai Destinatari specifiche regole di comportamento e condizioni di utilizzo degli strumenti informatici attraverso:

- la definizione di regole e procedure uniformi da applicarsi all'interno dell'Ente;
- l'osservanza dei doveri minimi di diligenza, lealtà, imparzialità e buona condotta;
- indicazione delle principali disposizioni normative in materia di utilizzo dei sistemi informativi e di protezione dei dati personali;

# LINEE GUIDA SUL CORRETTO UTILIZZO DELLE TECNOLOGIE INFORMATICHE E DEGLI ARCHIVI

- definizione dell'ambito, delle modalità e dei limiti del monitoraggio e dei controlli attuabili nel rispetto della normativa vigente;
- individuazione delle responsabilità dei Destinatari in caso di inosservanza di regole e prescrizioni.

**Fonti**

Le presenti Linee Guida e sono redatte in conformità alle seguenti fonti normative, regolamentari, linee guida e strumenti di soft law:

- Codice di comportamento dei dipendenti pubblici approvato con DPR 16 aprile2013 n. 62;
- Provvedimento del Garante per la protezione dei dati personali (Deliberazione n. 13 del 1/3/2007 - pubblicata sulla GU n. 58 del 10 marzo 2007);
- Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 recepito nella GU n. 300 del 24 dicembre 2008;
- Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati" (GDPR) e il Codice Privacy D. Lgs. 196/2003 armonizzato;
- Piani Triennali per l'informatica della PA;
- Standard ISO/IEC 27001 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti).

## 1 INFORMAZIONI GENERALI SULLA PROTEZIONE DEI DATI PERSONALI

Il diritto alla protezione dei dati è un diritto fondamentale dell'uomo, previsto all'art.1 del Regolamento UE e al Considerando (1) ed all'art. 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea come all'art. 16, paragrafo 1, del Trattato sul funzionamento dell'UE stabiliscono che "*ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano*".

Si ricorda preliminarmente che la normativa attuale, introduce il principio di responsabilizzazione e rendicontazione del Titolare il quale in maniera proattiva sceglie autonomamente le misure di sicurezza adeguate, per la protezione dei dati personali trattati all'interno della propria organizzazione, le quali devono essere periodicamente aggiornate dallo stesso anche in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

Le misure di sicurezza poste a tutela dei dati costituiscono un obbligo finalizzato alla protezione dei dati.

Il trattamento dei dati personali richiede obbligatoriamente l'adozione di idonee e preventive misure di sicurezza. Chiunque essendovi tenuto, omette di adottarle, è suscettibile di sanzioni amministrative, civili e penali.

Le misure di sicurezza che sono prescritte dal Titolare **riguardano il complesso delle misure tecniche, informatiche, organizzative, fisiche, logistiche e procedurali** che configurano i livelli di protezione necessari a ridurre o mitigare i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

# LINEE GUIDA SUL CORRETTO UTILIZZO DELLE TECNOLOGIE INFORMATICHE E DEGLI ARCHIVI

Di seguito sono riportati i principali concetti e definizioni che il Regolamento UE elenca all'art. 4.

## 2 PRINCIPALI CONCETTI E DEFINIZIONI

Si intende per:
"**DATO PERSONALE**" qualunque informazione relativa a persona fisica, identificata o identificabile ("interessato"), anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. I dati personali come ad esempio: il nome, il cognome, il codice fiscale, la residenza, il numero di cellulare, la casella di posta, l'indirizzo Internet, l'indirizzo IP, il saldo del conto corrente, le credenziali di accesso al sito, ecc. sono considerati "dati comuni". Tra i dati personali sono definiti "**dati particolari** "quei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

"**TRATTAMENTO**" qualunque operazione o complesso di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai dati personali, concernenti la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, la selezione, l'estrazione, l'utilizzo, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il blocco, la comunicazione, la diffusione, il raffronto o l'interconnessione, la limitazione, cancellazione o la distruzione.

"**TITOLARE DEL TRATTAMENTO**" la persona fisica, la persona giuridica, la pubblica amministrazione, l'ente o altro organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità e i mezzi del trattamento di dati personali.

"**RESPONSABILE**" la persona fisica o la persona giuridica, l'autorità pubblica, l'ente o altro organismo che tratta dati personali per conto del titolare al trattamento.

"**AUTORIZZATI**" le persone fisiche autorizzate a compiere operazioni di trattamento del dato dal titolare o dal responsabile.

"**INTERESSATO**" la persona fisica a cui si riferiscono i dati personali.

"**DESTINATARIO**" la persona fisica o la persona giuridica, l'autorità pubblica, l'ente o altro organismo che riceve comunicazione di dati personali.

"**GARANTE** "l'autorità di controllo disciplinata all'articolo 51 del Regolamento UE.

"**MISURE ADEGUATE**" il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello adeguato di protezione richiesto in relazione ai rischi previsti nell'articolo 32.

"**STRUMENTI ELETTRONICI**" gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

"**AUTENTICAZIONE INFORMATICA**" l'autenticazione è il processo attraverso il quale viene verificata l'identità di un utente che vuole accedere ad un computer o ad una rete. È il sistema che verifica, effettivamente, che un individuo è chi sostiene di essere. L'autenticazione è diversa dall'identificazione (la determinazione che un individuo sia conosciuto o meno dal sistema) e dall'autorizzazione (il conferimento ad un utente del diritto ad accedere a specifiche risorse del sistema, sulla base della sua identità).

"**CREDENZIALI DI AUTENTICAZIONE**" i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica. Le credenziali di autenticazione, consistono in un sistema per l'identificazione dell'autorizzato (User-

ID / login / user name / utente) associato ad una parola chiave (Password / parola d'ordine) riservata, conosciuta solamente dal medesimo.

**"PAROLA CHIAVE"**, componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

**"PROFILO DI AUTORIZZAZIONE"**, l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

**"SISTEMA DI AUTORIZZAZIONE"** l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

**"RESPONSABILE PROTEZIONE DATI"** o data Protection Officer (di seguito DPO) è una figura introdotta dal Regolamento europeo, è un professionista con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.

**"AMMINISTRATORE DI SISTEMA"** soggetto designato a sovraintendere il funzionamento del sistema informatico dell'Ente. L'attribuzione delle funzioni di amministratore di sistema avviene previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, che deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. La designazione quale amministratore di sistema è individuale e reca l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni loro attribuite, sono riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante per la Protezione dei Dati Personali. L'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, di verifica da parte dell'Ente, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

## 3 AUTORIZZATI DEL TRATTAMENTO

Ai sensi dell'art. 32 comma quarto, e dell'art. 29 del Regolamento UE, il personale dipendente in servizio presso l'Ente nonché tutti i componenti gli Organi Istituzionali e delle Commissioni e i collaboratori a vario titolo (es. stagisti o somministrati) sono nominati con apposito atto scritto, autorizzati a trattare i dati personali necessari per lo svolgimento delle attività e delle funzioni ad essi affidate in funzione del proprio incarico e di compiere le operazioni di trattamento a ciò strumentali, attenendosi anche alle ulteriori istruzioni contenute nel presente documento, o impartite nel corso dell'attività e rispettando le pertinenti disposizioni contenute in specifiche comunicazioni interne indirizzate alle categorie di autorizzati interessati.

Gli autorizzati di norma, possono trattare i soli dati inerenti alle attività del settore organizzativo a cui sono assegnati e non devono eseguire operazioni di trattamento per finalità non previste dall' Ente.

L'Ente conserva la lista degli autorizzati, comprendente l'ambito del trattamento riservato a ciascun autorizzato e la natura dei dati trattati dallo stesso (dati comuni, particolari, giudiziari), aggiornata e verificata periodicamente (comunque almeno una volta l'anno) con il supporto responsabile della protezione dei dati (DPO) e dell'amministratore di sistema (ADS), il quale aggiorna i singoli profili di accesso alle reti informatiche seguendo il principio che gli autorizzati

hanno accesso ai soli dati necessari per lo svolgimento delle loro attività. I profili di accesso assegnati ai singoli autorizzati sono registrati e conservati in un Database informatico costantemente aggiornato e disponibile in caso di verifiche.

### 3.1 ISTRUZIONI GENERALI PER TUTTI GLI AUTORIZZATI

Gli autorizzati, nel trattare i dati personali e, dovranno operare garantendo la massima riservatezza ed integrità delle informazioni.

In particolare il dipendente, nell'ambito del suo rapporto di lavoro pubblico, nonché i Componenti gli Organi Istituzionali e le Commissioni dell'Ente, rispettano il segreto d'ufficio nei casi e nei modi previsti dalle norme dell'ordinamento e un particolare dall'art. 24 della legge n. 241/1990 e mantengono riservate le notizie e le informazioni apprese nell'esercizio delle proprie funzioni e che non siano oggetto di trasparenza in conformità alla legge e ai regolamenti. Osservano inoltre il dovere di riservatezza anche dopo la cessazione dal servizio e alla scadenza della carica. Non forniscono informazioni in merito ad attività istruttorie, ispettive o di indagine in corso presso l'Ufficio e non rilasciano informazioni relative ad atti e provvedimenti prima della loro comunicazione alle parti. Non fanno uso delle informazioni non disponibili al pubblico o non rese pubbliche, ottenute anche in via confidenziale nell'attività d'ufficio, a fini privati e deve evitare situazioni e comportamenti che possano ostacolare il corretto adempimento dei compiti o nuocere agli interessi o all'immagine dell'Ente.

L'autorizzato al trattamento deve osservare scrupolosamente le disposizioni che regolano l'accesso ai locali dell'amministrazione da parte del personale e non introdurre, salvo che non siano debitamente autorizzate, persone estranee all'Ente stesso in locali non aperti al pubblico.

Gli autorizzati dovranno perciò operare con la massima diligenza ed attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, all'eventuale loro aggiornamento, così per la conservazione ed eventuale cancellazione o distruzione.

La procedura di lavoro e la condotta tenuta nello svolgimento delle operazioni di trattamento, dovranno essere orientate a prevenire i rischi che potrebbero incombere sui dati, in particolare evitando che:

- i dati personali siano soggetti a distruzione e perdita anche accidentale;
- ai dati possano accedere persone non autorizzate;
- vengano svolte operazioni per fini diverse da quelli per i quali i dati sono stati raccolti.

Taluni autorizzati di trattamenti di dati particolari e giudiziari sono destinatari di ulteriori specifiche indicazioni che integrano quelle generali di cui al presente documento. Le ulteriori disposizioni sono indicate nei singoli atti di nomina.

## 4 USO DEGLI STRUMENTI E RELATIVE ISTRUZIONI

Gli autorizzati sono tenuti ad operare e custodire i beni e gli strumenti (Banche dati, applicativi ecc.) a loro affidati adottando le cautele necessarie al mantenimento della loro efficienza ed integrità adottando tutte le misure di sicurezza messe a disposizione dall'Ente anche qualora effettuino la prestazione in modalità agile o da remoto.

Gli strumenti affidati sono nella disponibilità del soggetto autorizzato primariamente per un fine di carattere istituzionale e/o lavorativo.

### 4.1 REGOLE PER LA GESTIONE DELLE PASSWORD

Gli autorizzati devono accedere alla rete, ai sistemi di file sharing utilizzati e quindi alle varie attività di trattamento dei dati, utilizzando metodi di autenticazione per garantire l'accesso protetto secondo il livello di protezione scelto e deciso dall'Ente. Le credenziali di autenticazione

per l'accesso ai sistemi, assegnate agli autorizzati, possono consistere in: parole chiavi dette "password", codici per l'accesso, eventuali certificati digitali, i token per la generazione automatica di codici, ecc..

Nell'utilizzo delle parole chiave, ogni autorizzato deve attenersi, anche, alle seguenti norme di sicurezza:

- al momento dell'inserimento in una unità organizzativa dell'Ente e/o alla presa in carico di un personal computer, deve sostituire immediatamente la parola chiave iniziale/transitoria comunicata, con una parola chiave personale secondo le specifiche sotto indicate;
- non deve divulgare la parola chiave personale o comunicarla o trasmetterla ad altri, possibilmente non deve conservarla scritta e comunque deve evitare che sia conosciuta, anche accidentalmente, da altre persone;
- deve sostituire la parola chiave, in modo autonomo, con cadenza almeno trimestrale o quando ritenga che, per qualunque motivo, abbia perso le caratteristiche di segretezza;
- La parola chiave viene scelta liberamente dai singoli autorizzati, ma per garantirne l'affidabilità, deve avere le seguenti caratteristiche definite nei requisiti minimi di complessità definiti dall'Ente:
  - lunghezza non inferiore a quanto richiesto dall'amministratore di sistema;
  - utilizzo misto di caratteri numerici e alfabetici, possibilmente non a scansione fissa scegliendo tra maiuscole e minuscole;
  - non utilizzo contemporaneo o ripetitivo di password uguali o complementari o frazionate;
- La parola chiave, non potrà essere attribuito, nemmeno in tempi diversi, a persone diverse. Salvo casi eccezionali, con lo stesso Codice Identificativo Personale, non si possono attivare o utilizzare più personal computer contemporaneamente.
- In caso di dimissioni o cessazione dalla, carica il Codice Identificativo Personale del dimissionario viene reso inutilizzabile.
- In caso di non utilizzo del Codice Identificativo Personale per un periodo consecutivo di sei mesi, il Codice Identificativo Personale viene disattivato.

### 4.2 DISPONIBILITÀ DI DATI O STRUMENTI ELETTRONICI IN CASO DI ASSENZA

In caso di assenza o impedimento dell'autorizzato, l'Ente potrebbe trovarsi nella circostanza di dover accedere allo strumento o ai dati trattati dalla persona assente.

La modalità di custodia informatica - che riguarda la totalità degli Autorizzati - prevede che tutte le parole chiave per l'accesso alla rete siano create, registrate e gestire su database del sistema di autorizzazione informatico adottato dall'Ente, accessibile attraverso il relativo meccanismo di sicurezza.

Ove per ragioni organizzative sia necessaria la conoscenza della parola chiave, l'amministratore di sistema provvederà al reset della password per poter accedere ai dati ed alle attività in rete di un autorizzato.

Questa procedura dovrà essere supervisionata dal Direttore dell'Ente che ne avrà autorizzato l'esecuzione e che darà immediata notizia all'autorizzato al suo rientro.

### 4.3 PROTEZIONE DELLA SESSIONE DI TRATTAMENTO

È fatto obbligo di non lasciare incustodito ed accessibile lo strumento elettronico (generalmente il personal computer) durante una sessione di trattamento. Allo scopo gli autorizzati nel caso di

abbandono temporaneo della postazione di lavoro, proteggono la sessione di lavoro adottando una delle seguenti misure:

- premere contemporaneamente i tasti Ctrl + Alt + Canc e quindi INVIO oppure tramite il tasto di scelta rapida "Logo Windows" + L;
- effettuare un "log off" della stazione di lavoro utilizzata; (tale operazione è comunque fatta al termine delle attività salvo diversi accordi);
- impostare il sistema in modo che si blocchi automaticamente nel momento in cui l'operatore si allontana dalla postazione.

## 4.4 MISURE DI SICUREZZA

### 4.4.1 ANTIVIRUS E PROTEZIONE DA PROGRAMMI PERICOLOSI

L'uso di programmi antivirus è obbligatorio per tutti i dispositivi (PC, Notebook, tablet e smartphone) collegati, anche temporaneamente in rete.
Tutti i PC, Notebook o altri dispositivi, collegati alla rete e/o ai sistemi di file sharing, sono controllati in modo automatico da un software antivirus gestito centralmente e aggiornato costantemente che, di norma, viene attivato all'accensione del computer e rimane residente in memoria fino allo spegnimento dello stesso.
Tutti gli autorizzati devono controllare che l'operazione di verifica con i programmi antivirus sia correttamente e completamente eseguita, segnalando qualsiasi anomalia e, in tal caso, spegnendo il proprio personal computer.
Tutti gli autorizzati che devono trattare, anche solo in lettura, supporti che non siano già stati testati, devono controllare gli stessi con il programma antivirus.
Ciascun autorizzato che riceva programmi e/o dati da destinatari esterni all'ente deve controllarli (con antivirus) prima di attivarli o aprirli. Non sono consentiti l'apertura, il salvataggio, la registrazione, l'apertura o l'esecuzione di file "allegati" ricevuti in e-mail da mittenti sconosciuti o sospetti.

### 4.4.2 PROTEZIONE DALLE INTRUSIONI E DAGLI ACCESSI ABUSIVI

I servizi di collegamento ad Internet e di posta elettronica sono gestiti e protetti nell'architettura globale del sistema informatico dell'Ente. L'accesso alla rete pubblica (internet), effettuato con tali servizi, è protetto da sistemi attivi e da apposito dispositivo detto "firewall" in cui sono attivi servizi di protezione che sono costantemente aggiornati.

Alcuni di questi servizi permettono:

- individuazione delle attività dannose e di registrarne le informazioni tentando di bloccarle e segnalarle (IPS)
- può limitare l'uso di applicazioni improduttive, inappropriate e pericolose
- controlla l'attività web
- protezione in tempo reale, continua e affidabile contro spam e tentativi di phishing
- prevenzione dalla violazione dei dati (DLS)
- difesa contro malware (TDR e APT blocker)

La rete Wi-Fi è disponibile sia agli operatori dell'Ente che ai visitatori esterni e permette l'esclusivo accesso alla rete pubblica (internet). Anche tale rete è protetta dal sistema di protezione perimetrale dell'Ente sopra definito (*"firewall"*).

#### 4.4.3 MEMORIZZAZIONE DEI LOG DI SISTEMA

Tutti i dispositivi, o quasi, ormai sono in grado di generare dei log e di memorizzarli localmente o su un server di log.

La memorizzazione dei log per un determinato periodo di tempo è necessaria per poter consultare in caso di una violazione di dati e per avere degli avvertimenti in caso comportamenti anomali rispetto alla normale attività.

#### 4.4.4 PROCEDURE DI AGGIORNAMENTO DEI PROGRAMMI PER ELABORATORE PER PREVENIRE VULNERABILITÀ E CORREGGERE DIFETTI

I gestori del sistema curano l'aggiornamento periodico, finalizzato alla prevenzione delle vulnerabilità e alla correzione dei difetti, dei programmi e dei sistemi sulla base dei rilasci effettuati dai fornitori (software-house). La periodicità di tale aggiornamento è almeno semestrale e per i trattamenti di dati particolari o giudiziari trimestrale.

Sono attivi sui personal computer, con sistema operativo Windows, aggiornamenti periodici automatizzati al fine di prevenire vulnerabilità e correggere difetti.

#### 4.4.5 PROCEDURA PER LA CUSTODIA DI COPIE DI SICUREZZA

Si provvede alla generazione delle copie di sicurezza (backup) dei dati trattati dall'Ente secondo gli standard stabiliti, avendo cura della conservazione in sicurezza delle copie di backup in via prioritaria nel cloud e su supporti rimovibili (NAS). La frequenza delle copie è giornaliera, anche su dispositivi diversi e con modalità diverse.

#### 4.4.6 PC PORTATILI

In caso di assegnazione di PC portatili, devono essere adottate le seguenti misure di sicurezza oltre alle misure di sicurezza sopra descritte.
Premesso che non è consentita di norma la memorizzazione di dati personali, qualora ciò sia indispensabile per fini connessi alle attività lavorative svolte:

- Il computer dovrà essere protetto anche con una parola chiave all'accensione dello strumento;

La password sarà assegnata dall'amministratore di sistema in accordo con il funzionario preposto dell'Ente e dovrà essere conservata secondo la procedura già in atto per le password.
Ove necessario periodicamente l'amministratore di sistema provvede alla sostituzione della password comunicandola all'utente autorizzato all'uso.
L'aggiornamento del software antivirus e dei programmi per elaboratore, finalizzato alla prevenzione delle vulnerabilità e alla correzione dei difetti, viene effettuato automaticamente all'atto del collegamento alla LAN. Si raccomanda agli assegnatari di PC portatili di effettuare periodicamente il collegamento alla rete e/o ai sistemi di file sharing per garantire l'aggiornamento dei prodotti. I dati trattati dall' Ente eventualmente contenuti sui PC portatili, nel caso non siano già stati registrati su sistema centrale o su dischi rete o dipartimentali, con cadenza periodica almeno settimanale, devono essere trasferiti sul disco di rete assegnato allo scopo di evitarne la perdita anche se accidentale.
Per tutti i dispositivi portatili considerati ad uso comune (per esempio pc sala congressi/conferenze) verrà predisposto un utente per autenticazione comune la cui password sarà variata regolarmente almeno ogni sei mesi. In tali pc non devono essere conservati dati personali particolarmente riservati. Questi portatili con le autenticazioni assegnate a uso comune

non potranno accedere alla rete LAN dell'ordine ma avranno accesso solo alla navigazione Internet.

#### 4.4.7 LICENZE D'USO DEI PROGRAMMI SOFTWARE

È fatto divieto, per la normativa sul diritto di autore, di copiare, installare o utilizzare programmi software non rilasciati ufficialmente dall'Ente e preventivamente testati circa la loro liceità, integrità e compatibilità con gli standard dell'Ente.

Pertanto ogni necessità di installazione di prodotti cosiddetti "in demo" o "trial", dovrà essere comunicata ed autorizzata dall'Ente sentito l'RTD e l'ADS.

#### 4.4.8 INTERNET E POSTA ELETTRONICA

Per il personale in servizio la navigazione in Internet è inerente a scopi strettamente legati all'attività lavorativa, fatto l'utilizzo eccezionale e limitato nel tempo per necessità personali che non vadano e ledere l'efficacia dell'attività amministrativa dell'Ente.

È vietato:

-accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, che siano in qualche modo discriminatori;

- scaricare software (anche gratuito) da siti internet;

-effettuare transazioni finanziarie, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo per attività lavorative;

-effettuare qualsiasi registrazione a siti internet i cui contenuti non siano riconducibili all'attività lavorativa;

-archiviare documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria

Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di internet, nonché un possibile illecito trattamento di dati personali, è ricondotta nella responsabilità personale del soggetto inadempiente.

Le caselle di posta elettronica sono messe a disposizione dall'Ente per usi esclusivamente professionali, l'improprio uso personale, comporta assunzione diretta di responsabilità circa i contenuti dei messaggi da parte di chi li invia. La casella di posta deve essere mantenuta in ordine, cancellando documenti in eccesso. Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoghe diciture, deve essere visionata od autorizzata dal responsabile dell'ufficio, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

È obbligatorio controllare i file attachment di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Responsabile del trattamento. Non si devono in alcun caso attivare gli allegati di tali messaggi.

Il personale in servizio è responsabile del contenuto delle proprie comunicazioni ed è tenuto ad utilizzare un linguaggio rispettoso della propria posizione istituzionale degli organi politici e dei colleghi anche per quanto riguarda la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare la violazione dell'obbligo di fedeltà, del segreto d'ufficio e della normativa per la tutela dei dati personali.

#### 4.4.9 CONVERSAZIONI TELEFONICHE

Non è consentito fornire informazioni riservate sugli iscritti dell'Ordine, fornitori ed altri enti che intrattengono rapporti con l'Ente, o sulle attività svolte dall'Ente stessa ovvero sul proprio personale, se non si è certi di chi sia l'interlocutore e, comunque, al di fuori dell'ambiente di lavoro, senza autorizzazione.

È fatto divieto, quindi, di fornire telefonicamente informazioni sull'organizzazione interna e/o codici identificativi, password, assenze a sconosciuti.

Nell'effettuare una telefonata riguardante la propria attività, assicurarsi che la persona contattata sia esattamente quella desiderata ed evitare il rischio che persone estranee possano volontariamente o involontariamente ascoltare il contenuto della telefonata. Evitando le conversazioni a viva-voce.

#### 4.4.10 AUTORIZZAZIONI ALL'INGRESSO NEI LOCALI E CONTROLLO ACCESSO AI LOCALI

L'ingresso nei locali dove sono presenti le apparecchiature di gestione della rete dell'Ente dei personal computer e nei locali dove sono presenti le apparecchiature di gestione del sistema informativo dell'Ente (Server) è riservato solo alle persone appositamente autorizzate.

#### 4.4.11 CIFRATURA

Per tutti i dispositivi in cui è possibile attivare la cifratura a livello di volume questa deve essere attiva, mentre per gli altri si predispongono dei contenitori cifrati sono per dati particolari.

#### 4.4.12 CUSTODIA E RIUTILIZZO DEI SUPPORTI RIMOVIBILI

È tendenzialmente sconsigliato l'uso di supporti rimovibili (es. chiavette usb, hard disk, smart card o altri sistemi di memorizzazione o di gestione dei dati) per l'attività dell'Ente in quanto le difficoltà di gestire efficacemente l'importazione e l'esportazione di dati potrebbe esporre l'Ente a svariati rischi di perdite di dati o di introduzione nel sistema informatico di attacchi informatici.

Gli autorizzati, ai quali è stato permesso il trattamento del dato tramite l'utilizzo di supporti rimovibili (forniti esclusivamente dall'Ente e dei quali si prevede la registrazione del soggetto cui vengono affidati in segno di assunzione di responsabilità), debbono custodirli e controllarli in modo tale che soggetti non autorizzati non possano venire a conoscenza, nemmeno accidentalmente, del contenuto di tali supporti. I supporti devono essere protetti da cifratura e al termine di ogni lavorazione dovranno essere custoditi e riposti in contenitori, armadi o cassetti muniti di serratura.

In caso di cattivo funzionamento del supporto, che ne determini l'impossibilità della lettura dei dati registrati, i supporti dovranno essere distrutti.

Nel caso di supporti contenenti dati personali, si precisa che la formattazione di un disco o di una "*chiavetta USB*" non costituisce norma di sicurezza poiché i dati formattati possono essere recuperati e letti attraverso apposite "utility"; pertanto i supporti devono essere trattati per

permettere una distruzione completa e definitiva del dato in esso contenuto, arrivando in taluni casi anche alla distruzione materiale del supporto (ad es. i DVD).

#### 4.4.13 USO STAMPANTI

L'Ente mette a disposizione di dipendenti e collaboratori unità periferiche di stampa ad uso esclusivamente istituzionale e lavorativo. I dipendenti e collaboratori sono tenuti ad effettuare la stampa dei dati solo se necessaria all'attività lavorativa e a ritirarla prontamente dai vassoi delle stampanti comuni, in modo da evitare che sia visibile o possa essere raccolta da terzi.

#### 4.4.14 CLOUD COMPUTING

Con il termine cloud computing si indica uno strumento di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on-demand attraverso Internet a partire da un insieme di risorse/dati preesistenti e configurabili. Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, espone l'Ente a potenziali rischi di violazione della privacy. I dati personali vengono memorizzati nelle server farm di aziende che spesso risiedono in uno stato extraeuropeo, configurando un trasferimento dei dati all'estero.

È perciò vietato l'utilizzo di sistemi Cloud non espressamente approvati dall'Ente se possibile, previo parere del DPO, nel rispettivo di specifiche procedure di controllo che verifichino i requisiti di affidabilità sicurezza informatica e di protezione dei dati personali.

## 5 ARCHIVI CARTACEI

Gli autorizzati sono tenuti a garantire sempre la corretta custodia dei documenti dell'Ente a loro affidati adottando le cautele necessarie al mantenimento della loro integrità adottando tutte le misure di sicurezza messe a disposizione dall'Ente assicurando:

- che i documenti non vengano lasciati incustoditi sulle scrivanie e/o in luoghi aperti al pubblico in assenza di altri autorizzati medesimo trattamento; i documenti non possono essere riprodotti o fotocopiati, se non per esigenze connesse alle finalità del trattamento; i documenti non devono essere consultati da persone non autorizzate al trattamento;
- di conservare i documenti o gli atti, che contengono dati particolari e/o giudiziari, in archivi ad accesso controllato, come ad es. armadi/schedari/contenitori muniti di serratura oppure soggetti a sorveglianza da parte di autorizzati;
- restituire tempestivamente la documentazione prelevata dagli archivi, al termine delle operazioni di trattamento;
- in caso di utilizzo di stampanti, fotocopiatrici o fax, condivisi da vari utenti e collocati al di fuori dei locali ove è posta la propria postazione di lavoro, raccogliere e custodire immediatamente, con le modalità sopra descritte, tutte le stampe prodotte;
- distruggere opportunamente le copie cartacee non più utili di documenti contenenti dati personali, evitando di gettarli via così come sono;
- adottare misure che siano idonee a limitare la conoscenza dei dati particolari e/o giudiziari qualora essi siano presenti nei flussi documentali dell'Amministrazione, garantendo il rispetto della riservatezza dei dati degli interessati.

# LINEE GUIDA SUL CORRETTO UTILIZZO DELLE TECNOLOGIE INFORMATICHE E DEGLI ARCHIVI

## 6 DISPOSIZIONI FINALI

Le presenti Linee Guida costituiscono la disciplina dell'Ente per i trattamenti dei dati personali, con particolare riferimento alle misure di sicurezza poste a tutela dei trattamenti effettuati con strumenti elettronici ma tenendo in debito conto che l'Ente nell'ambito della sua attività tratta anche dati cartacei che possono essere memorizzati o transitare per apparecchiature digitali.

Tutto il personale dipendente, le persone in *stage* o somministrazione, i Componenti degli Organi Istituzionali e delle Commissioni dell'Ente, i consulenti, i collaboratori esterni, gli addetti alla manutenzione e alla gestione di strumenti elettronici, sono tenuti a rispettare le presenti Linee Guida scrupolosamente, nell'ambito delle proprie competenze ed attività e nei rapporti anche con soggetti terzi.

La violazione parziale o totale delle presenti Linee Guida potrà essere suscettibile di provvedimenti disciplinari commisurati alla gravità della violazione, oltre che alle sanzioni civili, penali nonché disciplinari previste dalla vigente normativa e declinate all'interno del Codice di Comportamento dell'Ente.

Anche ai sensi dell'art. 32, primo comma, lettera d) del Regolamento UE sono previste verifiche e controlli periodici circa la puntuale osservanza delle disposizioni di cui al presente documento.