ALLEGATO AL DECRETO
PRESIDENZIALE
N. 28 DEL 12 MAR. 2024

All. 1)

Articolo 10 bis - Rapporti con i mezzi di informazione e utilizzo dei social network

1. I rapporti con i mezzi di informazione, sugli argomenti istituzionali, sono tenuti dai soggetti istituzionalmente individuati, nonché dai dirigenti responsabili di struttura. Fatti salvi i principi costituzionali posti a tutela della libertà di espressione, i dirigenti, prima di rilasciare interviste, dichiarazioni o giudizi di valore su attività dell'Amministrazione rivolti alla generalità dei cittadini, ne danno preventiva informazione al Presidente della Provincia.

2. Nel rapporto con terzi, tutto il personale si astiene da dichiarazioni pubbliche che vadano a detrimento del prestigio, del decoro o dell'immagine dell'Amministrazione o della pubblica amministrazione in generale e adotta tutte le possibili cautele per assicurare che ogni commento sia inteso come frutto delle proprie opinioni personali e non di quelle dell'Ente.

3. Il dipendente, nell'utilizzo dei social network, non può pubblicare immagini che lo ritraggano con simboli o fregi riconducibili all'Amministrazione, o in divisa per coloro che la indossino, se non previa autorizzazione scritta del responsabile della struttura di appartenenza.

4. Il dipendente si astiene dal diffondere con qualunque mezzo, compreso il web o i social network, i blog o i forum, commenti o informazioni, compresi foto, video, audio, che possano ledere l'immagine dell'Amministrazione e dei suoi rappresentanti, l'onorabilità di colleghi, nonché la riservatezza o la dignità delle persone. Si impegna inoltre a mantenere un comportamento corretto, ineccepibile ed esemplare anche nella partecipazione a discussioni su chat, blog, social forum online, ispirato all'equilibrio, alla ponderatezza, al rispetto delle altrui opinioni.

5. Al fine del rispetto delle prescrizioni del presente articolo si intendono come equivalenti anche tutte le azioni di condivisione o interazione con terzi.

Art. 10 ter - Utilizzo delle tecnologie informatiche.

1. L'Amministrazione, attraverso i propri responsabili di struttura e con l'ausilio del Servizio E Government, svolge gli accertamenti necessari e adotta ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati. Le modalità di svolgimento di tali accertamenti sono stabilite mediante linee guida adottate dall'Agenzia per l'Italia Digitale. In caso di uso di dispositivi elettronici personali, trova applicazione l'articolo 12, comma 3-bis del decreto legislativo 7 marzo 2005, n. 82.

2. L'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'Amministrazione. L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti il servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale.

3. Il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'Amministrazione. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.

4. Al dipendente è consentito l'utilizzo degli strumenti informatici forniti dall'Amministrazione per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.

5. È vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'Amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'Amministrazione.

6. In particolare, nell'utilizzo delle tecnologie informatiche messe a disposizione dal datore di lavoro per lo svolgimento dell'attività di servizio, il dipendente è tenuto a:

   - utilizzare le risorse hardware e software secondo diligenza in modo appropriato e responsabile;
   - non memorizzare file estranei all'attività di lavoro su hard disk o altri supporti di archiviazione forniti dall'Amministrazione;
   - non utilizzare le risorse per scopi estranei all'attività di servizio e non modificare le configurazioni preimpostate, né installare software o dispositivi che possano compromettano l'integrità, l'operatività e la sicurezza delle risorse hardware e software;
   - adottare ogni utile misura di sicurezza atta ad evitare che le credenziali di autenticazione, connesse all'utilizzo delle risorse del sistema informativo dell'Amministrazione associate al singolo dipendente, vengano a conoscenza di altri soggetti, anche lasciando incustodita l'attrezzatura informatica.

Art. 10- quater - Utilizzo dei mezzi di informazione e dei social media.

1. Nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente all'Amministrazione.

2. In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'Amministrazione o della pubblica amministrazione in generale.

3. Al fine di garantirne i necessari profili di riservatezza le comunicazioni, afferenti direttamente o indirettamente il servizio non si svolgono attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.

4. L'Amministrazione si doterà, con specifico atto, di una "social media policy" per ciascuna tipologia di piattaforma digitale, al fine di adeguare alle proprie specificità le disposizioni di cui al presente articolo. In particolare, la "social media policy" deve individuare, graduandole in base al livello gerarchico e di responsabilità del dipendente, le condotte che possono danneggiare la reputazione dell'Amministrazione.

5. Fermi restando i casi di divieto previsti dalla legge, i dipendenti non possono divulgare o diffondere per ragioni estranee al loro rapporto di lavoro con l'Amministrazione e in difformità alle disposizioni di cui al decreto legislativo 14 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità.

Agli artt. 11 comma 5 e 13 comma 3 del vigente Codice di Comportamento aziendale, dopo le parole "Direttore Generale", si aggiungono le parole "o, in mancanza, al Segretario Generale".