ISTITUTO D'ISTRUZIONE SUPERIORE "POMPONIO LETO"
Liceo Artistico: Arti Figurative/Architettura e Ambiente - Liceo Linguistico - Liceo delle Scienze Umane
Liceo delle Scienze Umane "Economico-Sociale" - Liceo Scientifico ordinario - Liceo Scientifico "Scienze Applicate"
Via S. Biagio, 1 - 84039 Teggiano - 0975/79038 - fax 0975/587963 - C.F.:83002490650 Cod. Mecc. SAIS02600Q
www.iisteggiano.edu.it - sais02600q@pec.istruzione.it - sais02600q@istruzione.it

REGOLAMENTO
Utilizzo Piattaforme on-line per la Didattica a Distanza

A.S. 2019/2020

Approvato dal collegio docenti nella seduta del 28 aprile 2020

Approvato dal consiglio d'istituto: DELIBERA N. 14 del 29 aprile 2020

---

1. Contenuto generale

Premessa

L'I.I.S. "*Pomponio Let*o" di Teggiano, in occasione della necessità di introdurre stabilmente la didattica a distanza tra le modalità di offerta formativa, per la tutela dei dati personali e in ottemperanza alla normativa vigente, decide di adottare il seguente regolamento sull' utilizzo delle piattaforme virtuali e dei vari ambienti didattici sul web.

La tecnologia agevola la nostra vita in molti modi. I social network e le piattaforme didattiche in particolare, per la loro natura migliorano le possibilità informative/comunicative tra gruppi di persone, garantendo un miglioramento in termini di velocità ed efficienza dell'attività lavorativa.

Tuttavia l'uso ponderato e consapevole di questi nuovi mezzi ne garantisce un utilizzo più corretto ed efficiente, per questo motivo nel nostro istituto si è ritenuto opportuno adottare una piattaforma ***Microsoft certificata AgiD***, comprensiva di tutte le App necessarie allo *smart working* per le aziende e scuola digitale (*Office 365*), senza ulteriori oneri per l'istituzione scolastica.

Questo regolamento prende in considerazione i principali aspetti basati sulle relazioni presenti tra i principali attori con cui ciascun utente si trova quotidianamente ad interagire.

Art.1 Relazioni tra insegnanti

Le App ufficiali per la condivisione dei materiali tra colleghi sono tutte quelle contenute nel pacchetto *Office 365 Edu*, dal momento che l'Istituto è già accreditato presso *Microsoft*.

La mail ufficiale per la corrispondenza tra colleghi e tra docenti e Istituto è la mail di Istituto generata appunto tramite Microsoft Office 365, ferma restando la possibilità di ognuno di continuare ad utilizzare la mail personale per comunicare tra colleghi.

In caso di gruppi *Whatsapp* (o altre applicazioni di messaggistica) ufficiali legati all'attività scolastica è necessario attenersi al seguente "codice di comportamento":

- ⇒ **postare** solo messaggi attinenti all'attività organizzativa, didattica e progettuale della scuola;
- ⇒ **limitare** il numero di post in modo da non pregiudicare l'efficacia dei messaggi presenti in bacheca;
- ⇒ **evitare** post e commenti personali e/o ridondanti su particolari eventi avvenuti all'interno dell'Istituto;
- ⇒ **utilizzare** un linguaggio semplice, chiaro e che non dia spazio a fraintendimenti;
- ⇒ **evitare** conversazioni che manchino di rispetto o siano ambigue nei confronti degli altri membri del gruppo o di persone assenti.

Art. 2 Relazioni con gli studenti

Si ricorda che le uniche piattaforme ed *Apps* autorizzate dalla scuola, ai fini della privacy e della regolamentazione vigente, sono quelle contenute nel pacchetto *Microsoft Office 365 Edu*, pertanto gli insegnanti e gli studenti devono utilizzare esclusivamente le applicazioni contenute in ***Microsoft Office 365 Edu*** e rispettare le seguenti regole:

- ⇒ l'insegnante deve **assumere** il ruolo di "Proprietario" della classe creata;
- ⇒ il **"Proprietario"** ha il compito di **impostare** il nome della classe (seguendo l'apposita sintassi "anno di studi" - "sezione" - "disciplina insegnata"), l'immagine, l'interfaccia, ecc. prima dell'apertura della classe agli studenti;

- ⇒ gli insegnanti devono aver cura di **esplicitare** agli alunni le finalità esclusivamente didattiche della Classe Virtuale;
- ⇒ **utilizzare** unicamente gli indirizzi mail istituzionali sia per i docenti che per gli studenti (nell'attesa dell'implementazione di queste ultime, sono utilizzabili, in forma provvisoria, fino al termine del corrente a.s., le mail personali degli stessi studenti se maggiori di 14 anni);
- ⇒ il "Proprietario" deve **stabilire** ed esplicitare i filtri relativi alle attività che è possibile effettuare con il materiale (visualizzazione, download, modifica, ecc.);
- ⇒ i docenti si fanno carico di **guidare** la comunicazione all'interno della *Piattaforma web* che deve essere sempre semplice, chiara e tale da non dare spazio a fraintendimenti; sono pertanto **vietate** comunicazioni che manchino di rispetto o siano ambigue nei confronti degli altri membri del gruppo o di persone assenti;
- ⇒ tutti i partecipanti devono **rispettare** le regole per l'uso della Classe Virtuale secondo il regolamento e le linee guida DAD già stabilite dalla Dirigenza scolastica e pubblicate sul sito web della scuola (*comunicazione prot.n.0001810 del 14/04/2020*);
- ⇒ **gli alunni**, assumendo autonoma iniziativa, **non possono creare gruppi** se non esplicitamente autorizzati dalla Dirigenza dell'Istituto, previa richiesta effettuata per tramite del Team digitale, e che ogni gruppo deve necessariamente prevedere la presenza di almeno un docente (ogni 25 alunni), in qualità di "Proprietario".

Se un docente decide comunque di creare con gli studenti un gruppo chiuso con altre piattaforme o altri strumenti di messaggistica veloce, quali a titolo indicativo e non esaustivo *WhatsApp, Telegram*, ecc., si assume ogni responsabilità in tal senso, dal momento che, stante la normativa vigente, l'istituzione scolastica non può autorizzare in nessun modo simili iniziative.

Regolamento specifico della Classe Virtuale – TEAMS:

1. Nella Classe Virtuale di TEAMS si possono pubblicare solo post di queste tipologie:
   a) consegna di compiti, elaborati e/o esercizi assegnati;
   b) richiesta di compiti, spiegazioni e/o informazioni relative alle varie discipline scolastiche;
   c) files (documenti di testo, presentazioni, immagini, articoli, fotografie, disegni, ecc.) relativi ad argomenti didattici o agli stessi direttamente riconducibili;
   d) commenti e interazioni con i post dei compagni, e/o altri contenuti comunque attinenti alle attività didattiche.
2. Tutti i post, ed i commenti in particolare, dovranno essere rispettosi e costruttivi, cioè:
   a) non dovranno essere mai, in nessun modo, offensivi nei confronti di chiunque;
   b) dovranno servire sempre come supporto per tutti e aiuto al miglioramento di tutti gli studenti.
3. In occasione delle Video-lezioni i docenti e gli studenti sono tenuti al rispetto di tutte le indicazioni presenti nella circolare "Comunicazione sull'attivazione di ***Microsoft Office 365 Education*** **-** Regole di comportamento alunni durante le lezioni in modalità DAD" (*Comunicazione prot.0001810 del 14/04/2020*), prontamente pubblicata e consultabile sul registro elettronico Argo alla sezione BACHECA.

Art. 3 Obblighi di condotta e sorveglianza delle varie categorie di utenti

Dirigente scolastico

Il Dirigente Scolastico promuove l'uso delle tecnologie e di internet e si impegna a:

- ⇒ **garantire** la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica;
- ⇒ **garantire** che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle piattaforme informatiche messe a disposizione e delle TIC;
- ⇒ **garantire** l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- ⇒ **assicurare** la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- ⇒ **comprendere** e **seguire** le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola e sulla piattaforma virtuale scolastica.

Team e animatore digitale

All'Animatore e al Team Digitale spettano i compiti di:

- ⇒ **stimolare** la formazione interna in riferimento a quanto contenuto nel PNSD e nel PTOF;
- ⇒ **fornire** consulenza e informazioni al personale in relazione alle modalità di accesso e utilizzo delle piattaforme on-line e alle misure di attuazione della DAD messe in campo dall'istituto scolastico;
- ⇒ **monitorare** e **rilevare** le problematiche emergenti relative all'utilizzo delle tecnologie digitali e delle piattaforme internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- ⇒ **assicurare** che gli utenti possano accedere alle piattaforme digitali della scuola solo tramite password temporanee regolarmente cambiate al primo accesso, a piacimento dell'utente, e curare la manutenzione e lo sviluppo del sito web e delle piattaforme della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- ⇒ **assicurare** la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- ⇒ **coinvolgere** la comunità scolastica nella partecipazione ad attività e progetti attinenti la "scuola digitale".

Direttore dei servizi generali e amministrativi

Il direttore dei servizi generali e amministrativi si impegna ad:

- ⇒ **assicurare**, nei limiti delle risorse finanziarie disponibili e delle possibilità tecniche offerte dalle piattaforme utilizzate, l'intervento di tecnici per garantire che l'infrastruttura informatica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- ⇒ **garantire** il funzionamento dei diversi canali di comunicazione della scuola per la notifica dei documenti e delle informazioni istituzionali.

Docenti

Il personale docente deve:

- ⇒ **informarsi**/**aggiornarsi** sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- ⇒ **garantire** che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- ⇒ **assicurare** che gli alunni seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle piattaforme digitali e degli ambienti di lavoro virtuali (team) di cui sono "proprietari";
- ⇒ **fornire** agli alunni le competenze utili alla comprensione delle opportunità di ricerca e studio offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- ⇒ **garantire** che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con i sistemi scolastici ufficiali (*Portale Argo e Microsoft Office 365*);
- ⇒ **assicurare** la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- ⇒ **controllare** l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le video-lezioni e ogni altra attività scolastica (ove possibile);
- ⇒ nelle lezioni in cui è programmato l'utilizzo di Piattaforme virtuali, motori di ricerca e navigazione web **guidare** gli alunni a siti controllati e verificati come adatti per il loro uso e controllare, per quanto possibile, che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- ⇒ **comunicare** ai genitori difficoltà, bisogni o disagi espressi dagli alunni rilevati a scuola e nella DAD connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- ⇒ **favorire** con tutte le modalità a disposizione l'interazione con gli alunni BES, Disabili e DSA, le loro famiglie e, per quanto è possibile, la relazione con i compagni di classe, rapportandosi, in caso di criticità emergenti, con il docente referente (si ricorda che anche con la didattica a distanza è possibile prevedere l'utilizzo di strumenti compensativi e dispensativi, le piattaforme educative offrono numerose risorse per gli alunni con disturbi specifici di apprendimento, alunni con BES o DSA);
- ⇒ **segnalare** qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo al Team Digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola, anche, se necessario, in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- ⇒ **segnalare** al Dirigente scolastico, al suo staff e ai genitori qualsiasi abuso rilevato a scuola, anche in ambiente virtuale, nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

Alunni

Gli alunni devono:

- ⇒ **essere responsabili**, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;

- ⇒ **avere una buona comprensione** delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- ⇒ **comprendere l'importanza** di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- ⇒ **adottare condotte rispettose** degli altri, anche quando si comunica in rete, evitando prevaricazioni e atteggiamenti scorretti di ogni tipo, ad esempio disattivazioni di audio e/o video in relazione tra pari e con gli insegnanti, condivisioni schermo non richieste dall'insegnante, ecc.;
- ⇒ **esprimere domande o difficoltà** o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori;
- ⇒ **attenersi scrupolosamente ad una condotta** di utilizzo delle piattaforme di classe virtuale strettamente connessa alle attività scolastiche, considerando l'ambiente di apprendimento virtuale quale luogo scolastico vero e proprio: a tal fine qualsiasi gruppo (team) si senta la necessità di creare per condividere interessi, approfondimenti culturali, attività ludico-didattiche e musicali o artistiche, gli alunni promotori dovranno presentarne esplicita richiesta al Dirigente scolastico ed al suo Staff per tramite del Team digitale, responsabile della piattaforma di apprendimento a distanza (Microsoft Office 365);
- ⇒ **prendere visione, leggere attentamente** e rispettare tutte le indicazioni presenti nella circolare "Comunicazione sull'attivazione di Microsoft Office 365 Education - Regole di comportamento alunni durante le lezioni in modalità DAD" (Prot.0001810 del 14/04/2020), consultabili sul registro elettronico Argo alla sezione BACHECA e sul sito Web dell'istituto.

Genitori

Il ruolo dei genitori degli alunni include i seguenti compiti:

- ⇒ **sostenere** la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- ⇒ **seguire gli alunni** nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet;
- ⇒ **concordare con i docenti** linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet.

Art. 4 - Condivisione e comunicazione del Regolamento e della Policy all'intera comunità scolastica.

Condivisione e comunicazione della politica di DAD ed *e-learning* agli alunni

Tutti gli alunni devono essere informati che la rete, l'uso di Internet e di ogni dispositivo digitale di proprietà dell'Istituto e/o la connessione alle Piattaforme ufficiali dell'istituto (*Argo e Microsoft Office 365*) è soggetto a controllo da parte dei fornitori dei servizi e, per quanto riguarda la condivisione di file e contenuti web sulle piattaforme istituzionali, all'intervento dei docenti "Proprietari" dei vari ambienti di lavoro (teams) e del Team Digitale per la più generale amministrazione delle piattaforme. L'istituto si fa carico di istruire gli alunni riguardo l'uso responsabile e sicuro di internet attraverso diversi momenti formativi, anche, se necessario attraverso uno specifico periodo di formazione a distanza nell'ambito dei P.C.T.O., e l'attribuzione di credenziali di accesso

univoche (Username e Password) di proprietà esclusiva del singolo alunno. Sarà posta particolare attenzione all'educazione sulla sicurezza e agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili.

Condivisione e comunicazione della politica di DAD ed *e-learning* a tutto il personale scolastico

La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet, in special modo da quando la DAD ha assunto un ruolo preminente nell'ambiente di apprendimento virtuale, sarà portata all'attenzione degli organi collegiali e comunicata a tutto il personale. Il personale docente sarà reso consapevole del fatto che il traffico in internet è monitorato e si potrà risalire al singolo utente registrato in relazione ad attività messe in atto all'interno degli ambienti virtuali di lavoro. Azioni di informazione/formazione saranno messe in atto dall'Istituto per l'uso sicuro e responsabile di internet, delle attività connesse all'utilizzo delle TIC e di quelle più strettamente legate alla DAD.

Condivisione e comunicazione della politica di DAD ed *e-learning* ai genitori

L'Istituto si impegna a stimolare un approccio di collaborazione nel perseguimento della consapevolezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali. L'Animatore e tutto il Team digitale, con il supporto determinante di tutto il collegio docenti, forniranno ai genitori suggerimenti e indicazioni per l'uso evoluto e consapevole delle tecnologie digitali, di internet e delle piattaforme ufficiali utilizzate dall'istituto scolastico, anche in relazione alle risorse utili per lo studio e a siti idonei ed educativi per gli alunni.

Art. 5 – Relazioni tra persone e condivisione di contenuti in ambiente virtuale

La DAD, il Web 2.0, l'*e-lerning* e, più in generale, l'uso di *social network* hanno permesso l'attivazione di processi di comunicazione e collaborazione tra persone senza vincoli, non solo di luogo e di tempo, ma anche di conoscenza. Si è sviluppato quindi un nuovo sistema di "connessione" nel quale sono state completamente trasformate, o meglio riscritte, le regole di identità, di relazione, di comunicazione, all'interno di luoghi e contesti del tutto nuovi e non sempre conosciuti. Distinti per classi di appartenenza, migranti o nativi, siamo diventati "cittadini digitali", ma le nuove forme di cittadinanza digitale non sono automaticamente garantite a tutti. Non bastano tecnica e destrezza, qualora siano presenti, nell'utilizzo delle nuove tecnologie per essere o diventare cittadini responsabili, attivi e partecipativi nella società della conoscenza.

Ecco allora le regole da rispettare:

1. L'utilizzo del pacchetto ***Office 365***, con tutte le numerose App in esso presenti, scelto dalla scuola quale luogo deputato allo svolgimento della DAD, così come di tutti i Social Network e le applicazioni web (Facebook, Twitter, Myspace, Flickr, Linkedin, YouTube, Vimeo, Foursquare, ecc…) richiede una buona conoscenza degli articoli presenti nel regolamento d'uso degli stessi, nonché dei diritti e dei doveri dell'utente.
2. La condivisione di informazioni personali, immagini, contenuti, ecc… deve essere effettuata attraverso una attenta riflessione relativa alla pubblicazione in ambiente pubblico, scegliendo con estrema cura i soggetti cui si è deciso di attribuire la propria "amicizia" e con cui accrescere la propria rete di conoscenze, oltre che i gruppi con cui condividere riflessioni e materiali.

3. Gli ambienti di condivisione virtuale, didattici e non, come i Social Network sopra elencati, permettono lo scambio di file con diversi utenti di cui non necessariamente si conosce l'identità, vengono richiesti nomi e cognomi reali visibili da tutti e come se non bastasse a questi dati si aggiunge un volto con una foto, iscrivendosi in qualche gruppo si forniscono anche altre informazioni come preferenze riguardo hobby, orientamenti politico/religiosi, anche il proprio numero di telefono insieme a molti altri dati sensibili. Per questo bisogna prestare la massima attenzione anche nel gestire ogni singola informazione o materiale didattico personale con cui si dovesse venire in contatto nello svolgimento della DAD. È fatto divieto, quindi, per evidenti motivazioni derivanti dalle leggi che tutelano il copyright, il diritto d'autore e la privacy, diffondere al di fuori dell'ambiente scolastico qualsiasi materiale didattico condiviso all'interno della piattaforma virtuale scolastica.

4. È bene tenere presente, inoltre, che la struttura del *social network* purtroppo è ben indicizzata dai motori di ricerca, come ad esempio *Google*, basta quindi una ricerca di nome e cognome ed ecco che tali strumenti di ricerca forniscono facilmente i commenti personali che un utente ha inviato nei vari gruppi del *social network*, specie se pubblici. Chiunque può quindi conoscere quello che un utente scrive nei vari gruppi di discussione, chiunque può capire le idee, la personalità di un utente, etc. Per questo si invita l'utenza tutta a prestare la massima attenzione a non "contaminare" gli ambienti di condivisione istituzionalizzati con altri *social network* non autorizzati dai luoghi deputati all'apprendimento.

5. Se durante una chat, un forum o in una qualsiasi discussione online, I'interlocutore diviene volgare, offensivo o minaccioso, si deve evitare l'invito a continuare la discussione e abbandonare la conversazione;

7. Quando si riscontra un comportamento riconducibile ad un illecito durante una conversazione privata (tentativi di approccio poco ortodossi, richiesta di foto, *stalking* o *cyber bullismo*) I'utente può sfruttare gli appositi sistemi di reportistica degli abusi predisposti dall'apposita regolamentazione specifica, segnalando tempestivamente il *nickname* che ha perpetrato il comportamento scorretto. In questi casi può essere conveniente, se non indispensabile, abbandonare non soltanto la conversazione ma disconnettersi dalla piattaforma e denunciare immediatamente l'accaduto alla dirigenza scolastica;

8. Nell'uso di sistemi di *file-sharing* P2P (*peer-to-peer*), evitare di scaricare dei file che possono essere considerati illegali e/o protetti dal diritto d'autore, non aprire mai dei file sospetti (la maggior parte dei programmi P2P contiene *spyware* e *malware*). Per motivi di sicurezza la scuola deve necessariamente supervisionare l'utilizzo di tali sistemi.

9. I sistemi di messaggistica dei *social network* hanno le stesse regole della posta elettronica quindi, quando si invia un messaggio a più destinatari che non si conoscono tra loro, è necessario evitare che i destinatari possano vedere e conoscere i propri indirizzi di posta elettronica.

10. Quando si scambiano contenuti multimediali o si pubblicano video con colonna sonora o musica di sottofondo bisogna essere sicuri di averne il diritto d'uso e di non utilizzare impropriamente alcun file coperto da *copyright*.

Art. 6 – Contenuti prodotti dagli utenti

1. I contenuti pubblicati sulle applicazioni web hanno diversi livelli di visibilità (singoli utenti o tutti gli utenti del team o addirittura della piattaforma) che devono sempre essere tenuti a mente, dando a ciascun contributo i corretti livelli di privacy. Pertanto la pubblicazione di materiale all'interno di una *community* richiede l'utilizzo corretto delle funzioni necessarie all'attribuzione dei vari livelli di *privacy*.

2. Dal momento che ciò che viene pubblicato sulla Piattaforma Web ed ancor di più su di un *social network* è persistente e spesso non è facile da cancellare, se non impossibile, bisogna evitare di contribuire con materiale che in futuro non si vorrebbe veder pubblicato.

3. Quando si opera all'interno di un ambiente condiviso, l'utente è tenuto ad essere coerente con il contesto e le regole di fatto della *community*. Inoltre, è necessario conoscere gli strumenti per segnalare materiale e comportamenti non idonei.

4. Se l'ambiente/contesto nel quale si intende pubblicare il proprio contributo prevede l'intervento di un moderatore assicurarsi che i contenuti oggetto di pubblicazione siano rispondenti alle regole richieste. Se non è visibile online, probabilmente non è idoneo.

5. Quando si fa uso di etichette per catalogare il nome di un file oppure un contenuto/utente (TAG), bisogna assicurarsi che sia coerente con il contenuto o che indichi il file e/o la persona corretta. Se il TAG riguarda una persona specifica od un contenuto di sua proprietà, è opportuno contattarla preventivamente per ottenere il consenso a collegare l'identità della persona al contenuto e/o utilizzare lo stesso sulla Piattaforma Web.

Art. 7 – Riferimenti normativi (reati e violazioni della legge)

Spesso il modo di operare in rete nasconde comportamenti che seppur apparentemente innocui possono portare gli autori a commettere veri e propri reati e, di conseguenza, a subire procedimenti penali dalle conseguenze molto serie. Di seguito si ritiene necessario riportare alcuni riferimenti legislativi specifici, solo a carattere indicativo e senza nessuna pretesa di esaustività.

Reati informatici

La legge 23 dicembre 1993 n. 547 (Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica) individua e vieta tutta una serie di comportamenti nell'ambito informatico e che sono stati reputati lesivi per gli interessi non solo di singoli privati cittadini ma anche di persone giuridiche, in particolare per le imprese e gli enti pubblici:

 Accesso abusivo ad un sistema informatico e telematico

Attività di introduzione in un sistema, a prescindere dal superamento di chiavi "fisiche" o logiche poste a protezione di quest'ultimo. L'articolo 615 ter del Codice penale prevede il reato per "chiunque abusivamente si introduce in un sistema informatico o telematico, protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo". Per commettere il reato basta il superamento della barriera di protezione del sistema o accedere e controllare via rete un PC a insaputa del legittimo proprietario, oppure forzare la password di un altro utente e più in generale accedere abusivamente alla posta elettronica, ad un server o ad un sito su cui non siamo autorizzati.

 Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico

L'art. 615 quinquies (codice penale) punisce "chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri creato, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento". - Per commettere questo reato basta, anche solo per scherzo, diffondere un

virus attraverso il *messenger* o la *posta elettronica*, spiegare ad altre persone come si può fare per rimuovere la protezione da un computer, un *software*, una console per giochi oppure anche solo controllare a distanza o spegnere un computer via rete.

 Danneggiamento informatico

L' art. 635 codice penale vieta di danneggiare un sistema informatico. Per danneggiamento informatico si intende un comportamento diretto a cancellare o distruggere o deteriorare sistemi, programmi o dati. L'oggetto del reato, in questo caso, sono i sistemi informatici o telematici, i programmi, i dati o le informazioni altrui.

 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Questo particolare reato viene disciplinato dall'art.615 quater del codice penale e si presenta spesso come complementare rispetto al delitto di frode informatica. << è considerato reato anche quando l'informazione viene fraudolentemente carpita con "inganni" verbali e quando si prende conoscenza diretta di documenti cartacei ove tali dati sono stati riportati o osservando e memorizzando la "digitazione" di tali codici. >> Si commette questo reato quando si carpiscono, anche involontariamente, i codici di accesso alla posta elettronica, al *messenger* o al profilo di amici e compagni.

 Frode informatica

Questo reato discende da quello di truffa e viene identificato come soggetto del reato "chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità sui dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno". Secondo l'art. 640 ter c.p., che disciplina questo reato, il profitto può anche non avere carattere economico, potendo consistere anche nel soddisfacimento di qualsiasi interesse, sia pure soltanto "psicologico o morale".

Il delitto di frode informatica molto sovente viene a manifestarsi unitamente ad altri delitti informatici, quali l'Accesso informatico abusivo e danneggiamento informatico in conseguenza di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.

Reati non informatici

Sono da considerare reati non informatici tutti quei reati o violazioni del codice civile o penale in cui il ricorso alla tecnologia informatica non sia stato un fattore determinante per il compimento dell'atto:

 Ingiuria (ex art. 594 c.p. – abrogato dal decreto legislativo n.7/2016)

Chiunque offende l'onore o il decoro di una persona presente commette l'illecito di ingiuria. Incorre in quello che prima del 2016 era un vero e proprio reato penale chi commette il fatto mediante comunicazione telegrafica o telefonica o con scritti, o disegni, diretti alla persona offesa. L'art. 594 del codice penale che puniva l'ingiuria è stato abrogato dal decreto legislativo n. 7 del 15 gennaio 2016. Ne risulta quindi la depenalizzazione del reato. Lo stesso decreto legislativo ha fatto divenire l'ingiuria un "illecito civile". In altre parole, un illecito cui corrisponde una sanzione pecuniaria civile, di competenza del giudice civile. Nello specifico l'art.4 del decreto legislativo n. 7/2016 dispone, in riguardo alla sanzione, che: << Soggiace alla sanzione pecuniaria civile da euro cento a euro

ottomila […] chi offende l'onore o il decoro di una persona presente, ovvero mediante comunicazione telegrafica, telefonica, informatica o telematica, o con scritti o disegni, diretti alla persona offesa >>.

Il significato dell'illecito rimane sostanzialmente lo stesso: l'offesa all'onore e al decoro di una persona presente. Quando viene commessa in modo non verbale o con mezzi di comunicazione a distanza (anche informatici o telematici), essa deve consistere in una comunicazione diretta alla persona offesa.

 Diffamazione (art. 595 c.p.)

Chiunque offende la reputazione di qualcun altro, quando all'interno di una comunicazione con più persone si diffondono notizie o commenti volti a denigrare una persona. Aggravante nel caso in cui l'offesa sia recata con un "mezzo di pubblicità" come l'inserimento, ad esempio, in un *sito Web* o *social network* di una informazione o un giudizio su un soggetto. La pubblicazione *on-line* dà origine ad un elevatissimo numero di "contatti" di utenti della Rete, generando una incontrollabile e inarrestabile diffusione della notizia.

 Minacce e molestie

Il reato di minaccia (art. 612 c.p.) consiste nell'indirizzare ad una persona scritti o disegni a contenuto intimidatorio per via telematica. Può capitare che alcune minacce vengano diffuse per via telematica anche per finalità illecite ben più gravi: come ad esempio obbligare qualcuno a "fare, tollerare o omettere qualche cosa" (Violenza privata: art. 610 c.p.) o per ottenere un ingiusto profitto (Estorsione: art. 629 c.p.). Sull'onda di questa tipologia di reati è utile descrivere anche quello di Molestie e disturbo alle persone, disciplinato dall'art. 660 c.p., che si fonda sul contattare, da parte di terzi, per finalità pretestuose, il soggetto i cui dati sono stati "diffusi" per via telematica. Ad esempio la pubblicazione del nominativo e del cellulare di una persona *on-line*, accompagnato da informazioni non veritiere o ingiuriose: ciò potrebbe indurre altre persone a contattare la persona per le ragioni legate alle informazioni su questa fornite.

 Violazione dei diritti d'autore

Nel nostro ordinamento il diritto d'autore è regolato dal Codice Civile, libro quinto, titolo IX, capo I, agli articoli 2575-2583 c.c. e dalla Legge n. 633, del 22 aprile 1941, che all'articolo 1, definisce quali siano le opere sottoposte a tale tutela: "Sono protette ai sensi di questa legge le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione". Ricadono nell'ambito di tale tutela anche i programmi per computer (*software*) e le banche dati.

La legge 159/93 sottolinea all'art. 1 che chiunque abusivamente riproduce a fini di lucro, con qualsiasi procedimento, la composizione grafica di opere o parti di opere letterarie, drammatiche, scientifiche, didattiche e musicali, che siano protette dalla legge 22 aprile 1941, n. 633 e successive modificazioni, ovvero, pone in commercio, detiene per la vendita o introduce a fini di lucro le copie viola i diritti d'autore. Un primo caso di violazione del diritto d'autore si può verificare quando una copia non autorizzata di un'opera digitale è caricata su un *server* e messa a disposizione degli utenti. In questo caso, colui che riproduce e fornisce l'opera senza l'autorizzazione da parte del suo autore è considerato soggetto responsabile. Per commettere questo reato basta pubblicare su *YouTube* un video con una qualsiasi musica di sottofondo senza le dovute autorizzazioni. Un ulteriore possibile violazione del diritto d'autore si verifica quando I'utente ottiene il documento, il *software* o il brano mp3 messo a disposizione in rete o acquistato e ne fa un uso illegittimo, come ad esempio, rivenderlo a terzi o distribuirlo

sulla Rete facendone più copie non autorizzate. La legge italiana sul diritto d'autore consente all'utilizzatore di un *software* o di un'opera multimediale o musicale di effettuare un'unica copia di sicurezza ad uso personale, utile nei casi di malfunzionamento del programma, smarrimento della copia originale etc. Tale copia, salvo autorizzazione della casa di produzione, non può essere ceduta ad altre persone. La duplicazione abusiva (senza autorizzazione) è sanzionata penalmente e colpisce ugualmente anche chi duplica abusivamente non a scopo di lucro, bensì per un semplice fine di risparmio personale.

Principali riferimenti normativi:

- ⇒ Legge del 23 dicembre 1993, N. 547 (integra e modifica il c.p. e il c.p.p.)
- ⇒ Decreto Legislativo N. 196 del 2003 (tutela dei dati personali)
- ⇒ Decreto Legislativo N. 518 del 29 dicembre 1992 e Decreto Legislativo N. 205 del 15 marzo 1996 (tutela dei diritti sul software)
- ⇒ Decreto Legislativo N. 169 del 6 maggio 1999 (tutela del costitutore di database)
- ⇒ Decreto Legislativo N. 7 del 15 gennaio 2016
- ⇒ Codice Civile e Codice Penale.

PER CHIARIMENTI DI CARATTERE INFORMATICO

Riferirsi direttamente al Team Digitale (prof.ri Giuseppe Aumenta, Bruno Starace e Annamaria Totaro) e all'animatore che ne è responsabile (prof. Andrea D'Arienzo), in special modo per Microsoft Office 365 e al collaboratore del D.S. prof. Manzolillo, quale referente del Portale Argo, nonché a tutto lo staff della dirigenza, per qualsiasi problematica dovesse emergere in corso d'uso delle suindicate piattaforme virtuali.