Sede esami
Centre number: 29114

ISTITUTO COMPRENSIVO "SAN G. BOSCO"
Corso Roma 254 - 74016 MASSAFRA (TA)
Segreteria tel. 099/3313902 – Plessi tel. 099/8801271
Codice Fiscale: 90214650732

e-mail taic851009@istruzione.it PEC taic851009@pec.istruzione.it
www.icsgboscomassafra.edu.it

Massafra, li 30/11/2020

A tutti i docenti

Ai genitori

Agli alunni

Al Direttore dei SS.GG.AA.

Al personale ATA

Al registro elettronico

Alla bacheca scuola digitale

Al Sito Web della Scuola

Comunicazione n. 70

Oggetto: **DISPOSIZIONE ORGANIZZATIVA D.D.I. *(didattica digitale integrata)***
Rimodulazione temporanea dell'orario scolastico delle lezioni dal 02/11/2020 al 24/11/2020 ai sensi della normativa emergenziale, dell'Ordinanza del Presidente della Regione Puglia n. 407 del 27 ottobre 2020 e del chiarimento del Presidente della Regione Puglia prot. 2547 del 29/10/2020.

IL DIRIGENTE SCOLASTICO

VISTO Il D.M. 7 agosto 2020 n. 89 Adozione delle Linee guida sulla Didattica digitale integrata, di cui al Decreto del Ministro dell'Istruzione 26 giugno 2020, n. 39;

VISTE le Linee guida per la Didattica Digitale Integrata che forniscono alle istituzioni scolastiche indicazioni funzionali alla definizione di criteri, modalità e strumenti per la realizzazione

	delle attività didattiche a distanza, da adottare in modalità complementare rispetto a quelle in presenza;
VISTO	il Piano scuola sulla Didattica Digitale Integrata deliberato dal collegio dei docenti
VISTO	il D.P.R. 295/1999 Regolamento recante norme in materia di Autonomia delle istituzioni scolastiche ai sensi dell'art. 21 della L. 15 marzo 1997, n. 59;
VISTA	l'ordinanza regionale n. 407, datata 27.10.2020, avente in oggetto "Misure urgenti per fronteggiare l'emergenza epidemiologica da COVID-19";
TENUTO CONTO	dei chiarimenti prot. 2547 del Presidente della Regione Puglia, inviati al Direttore Regionale in data 29.10.2020
VALUTATI	i bisogni delle singole classi in merito ai casi specifici che necessitano di interventi speciali a tutela dell'offerta formativa e del principio di inclusione
SENTITO	il Presidente del Consiglio d'Istituto
SENTITE	le famiglie degli alunni con bisogni educativi speciali per il tramite dei docenti;

DISPONE CHE

1) dal 02.11.2020 al 24.11.2020 le lezioni si svolgeranno in DDI secondo l'orario di seguito illustrato:

   - Scuola primaria classi SECONDE TERZE QUARTE QUINTE lunedì – martedì – giovedì e venerdì dalle ore 9,00 alle ore 12,45. Il mercoledì dalle ore 9.00 alle ore 10.45 e dalle ore 15.00 alle ore 16.45

   - Tenuto conto della difficoltà oggettiva di seguire la didattica a distanza degli alunni più piccoli e considerata altresì la presenza di bambini con bisogni educativi speciali, tutte le classi PRIME della scuola primaria, divise in gruppi da 5/6 alunni, seguiranno le lezioni in presenza sia pure in modo scaglionato tra le diverse classi come da orario che sarà pubblicato entro domenica 1 novembre c.a.

   - Scuola secondaria di primo grado dal lunedì al venerdì dalle ore 9,00 alle ore 12,45

2) Le classi seguiranno le attività didattiche a distanza, attraverso la piattaforma Google Suite, applicazione Classroom e Meet, nel rispetto del Regolamento DDI d'Istituto citato in premessa e la piattaforma Zoom tenuto conto che i dispositivi TABLET in dotazione al nostro istituto non supportano le applicazioni Classroom e Meet.
3) È a cura della docente Carmela SIMEONE pubblicare l'orario di ogni singola classe, in presenza e in Didattica Digitale Integrata, nel registro elettronico e nella bacheca scuola digitale.
4) Gli alunni con bisogni educativi speciali (sia della primaria che della secondaria di I grado), integrati con alunni della classe, potranno frequentare le lezioni in presenza e quindi saranno supportati dai docenti della classe e di sostegno a cui sono assegnati, salvo diverso accordo con famiglie.
5) Il *sottogruppo classe* in presenza, per favorire l'inclusione, potrà avere un numero massino di 5/6 alunni.
6) Le attività in presenza verranno svolte secondo l'orario scolastico che verrà comunicato entro domenica 1 novembre c.a. I docenti delle classi di riferimento (inclusi i docenti disponibili), presteranno l'orario di servizio in presenza. Con circolare interna saranno indicate le turnazioni degli alunni presenti a scuola.
7) Tutti gli utenti (alunni e docenti) sono tenuti al rispetto delle norme inerenti alla sicurezza informatica e la privacy, ivi allegate.

8) Sicurezza sul lavoro:

- L'Amministrazione garantisce, ai sensi del decreto legislativo 9 aprile 2008, n. 81, la salute e la sicurezza del dipendente in coerenza con l'esercizio flessibile dell'attività di lavoro.
- Ogni dipendente collabora con l'Amministrazione al fine di garantire un adempimento sicuro e corretto della prestazione di lavoro.
- L'Amministrazione non risponde degli infortuni verificatisi a causa della negligenza del dipendente nella scelta di un luogo non compatibile con quanto indicato nell'informativa.
- Informativa INAIL sulla salute e sicurezza nel lavoro agile ai sensi dell'art. 22, comma 1, L. 81/2017 rinvenibile al link https://www.inail.it/cs/internet/docs/avviso-coronavirus-informativa-allegato-1.docx

IL DIRIGENTE SCOLASTICO

Dott. Nicola LATORRATA

Firma omessa ai sensi dell'art. 3 del d.lvo 39/93

LINEE GUIDA PER LO SMART WORKING
IN TEMA DI PRIVACY E SICUREZZA INFORMATICA

Le presenti linee guida forniscono le indicazioni operative per il trattamento di dati personali effettuato al di fuori della sede di lavoro, mediante le modalità di svolgimento agile della prestazione lavorativa.
Le prescrizioni riportate nell'atto di incarico al trattamento (Art. 29 Regolamento UE 679/2016 – GDPR), permangono nella loro validità. Alle stesse, il lavoratore agile dovrà prestare, se possibile, ancora più attenzione per garantire un livello di protezione adeguato delle dotazioni tecnologiche attraverso le quali svolge il lavoro smart e rispettare i principi di integrità, riservatezza e disponibilità dei dati e delle informazioni ivi contenute, al fine di ridurre al minimo i rischi di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità oppure di distruzione o perdita dei dati stessi.

Principali prescrizioni

1. Proteggere l'accesso alla rete (LAN, WiFi) e alle dotazioni tecnologiche (PC, notebook, tablet, smartphone, ecc.) attraverso l'uso di password forti e diverse per ciascun servizio[1]. Allo scopo si prescrive il cambio delle password utilizzate abitualmente per l'accesso alle varie applicazioni in cloud. Si consiglia, inoltre, il cambio della password di accesso della propria linea ADSL. Laddove possibile, utilizzare l'autenticazione a due fattori. Ad esempio, gli applicativi Argo consentono l'attivazione del PIN di autenticazione in aggiunta alla password d'accesso. Medesima possibilità è garantita dagli account Google.
2. Garantire che i sistemi operativi installati sulle workstation (PC, notebook, tablet, smartphone) siano autentici e aggiornati all'ultima versione disponibile. Non è consentito lo smart working attraverso workstation dotate di sistemi operativi privi del supporto (ad esempio Windows 7) o peggio non autentici (privi della licenza d'uso). Le vulnerabilità proprie dei sistemi operativi non autentici o privi del supporto e quindi non aggiornati con le ultime patch di sicurezza è la prima causa di accesso non autorizzato alla rete e alle informazioni.
3. Nel caso di utilizzo di una workstation condivisa (PC, notebook, tablet) è obbligatorio implementare un nuovo account d'accesso al sistema, personale e riservato.
4. Garantire la presenza, sulla propria workstation, di un firewall e di un sistema antivirus. Il sistema antivirus deve essere sempre attivo e aggiornato in real time (va bene, ad esempio, anche Avira nella sua versione non commerciale). Il firewall (va bene anche quello integrato nel sistema operativo Windows) deve sempre essere attivo e non deve prevedere alcuna eccezione.
5. È assolutamente vietata la pratica di memorizzazione delle password dei vari account nel browser. È consigliabile evitare di memorizzare anche le user name. Pertanto, il completamento automatico deve essere disabilitato. Si consiglia di utilizzare, per l'accesso ai vari account in cloud, sempre lo stesso browser. La memorizzazione degli account in cloud può essere consentita solo in presenza di un gestore di password crittografico (ad esempio, l'applicazione "Password Manager" integrata nella suite gratuita di Avira).
6. Nel caso in cui si proceda a memorizzare in locale qualsivoglia tipologia di informazioni contenenti dati personali degli interessati, anche temporaneamente, le stesse non dovranno mai essere memorizzate sull'hard disk della workstation, ma sempre in un dispositivo rimovibile (ad esempio pen drive, hard disk portatile) protetto su base crittografica. A tal proposito è possibile attivare la funzione "Attiva Bitlocker" fornita dal sistema operativo Windows.
7. Non meno importante, nello smart working, attuare una serie di misure organizzative per rendere l'ambiente domestico pari a quello lavorativo al fine di garantire la sicurezza e la riservatezza delle informazioni. Ad esempio, la normale cura della propria postazione di lavoro, non lasciare incustoditi i dispositivi e non condividere informazioni riservate con i propri familiari.
8. L'eventuale collegamento alla LAN (e quindi alla propria workstation) della scuola è consentito solo ed esclusivamente per mezzo di applicazioni conformi al GDPR e agli standar ISO/IEC 27001, ed ISO 9001:2015 (quali, ad esempio, Teamviewer). Ovviamente, in tal caso, valgono le prescrizioni definite ai punti precedenti.

[1] La password deve essere sufficientemente lunga e complessa, ad esempio deve essere composta da almeno 8 caratteri, contenere almeno un carattere appartenente alle lettere maiuscole e almeno un carattere appartenente alle lettere minuscole, contenere almeno un carattere appartenente alle 10 cifre (0-9), contenere almeno un carattere appartenente ai caratteri non alfabetici (ad esempio !,$,#,%), essere diversa dall'ultima utilizzata e mai riconducibile alla propria sfera personale o professionale.