

Smart working nella fase di emergenza da Coronavirus: linee guida tecniche

Premessa e contesto

Le seguenti indicazioni sono orientate a supportare i lavoratori che utilizzeranno le diverse forme di lavoro agile, mobile o smart working nel periodo di emergenza connesso alla diffusione del Coronavirus.

Dispositivi e dotazioni hardware

I dipendenti autorizzati potranno accedere a forme di lavoro remoto con l'utilizzo di strumentazione propria (notebook, pc desktop), secondo il principio del "bring your own device".

- Sistema operativo windows 7 o superiore
- sistema operativo Mac OS X Yosemite 10.10 o versioni successive
- Computer con installata la versione più recente di Google Chrome con abilitati i cookie e Javascript
[\[https://support.google.com/a/answer/33864?hl=it&ref_topic=9749439\]](https://support.google.com/a/answer/33864?hl=it&ref_topic=9749439)
- Antivirus aggiornato
- Connessione ad Internet su rete fissa o mobile
- Ultima versione del browser Chrome o, in alternativa, di Firefox o Internet Explorer

Per il collegamento alla rete TELPAT:

- FortiClient (vpn) per accedere alla rete provinciale TelPat (fornito da Trentino Digitale)

Nel rispetto dei requisiti individuati sopra è opportuno effettuare un test e quindi segnalare al proprio responsabile l'impossibilità di svolgere determinate attività mettendosi nelle condizioni di svolgere attività differenti o farsi supportare dai colleghi o dall'help desk per gli impedimenti tecnologici del caso.

Gestione della posta elettronica e GSuite

L'utilizzo della posta elettronica e degli strumenti di collaboration offerti da Google Gsuite effettuato dal proprio domicilio non è contraddistinto da alcuna particolarità rispetto alla normali prassi in ufficio: è accessibile attraverso un comune browser (anche se si consiglia di utilizzare Google Chrome), accedendo dal link <https://accounts.google.com>, inserendo il proprio indirizzo email individuale (nome.cognome@scuole.provincia.tn.it) o email Gsuite for Education dell'istituto e la propria password. Si ricorda e si sottolinea, soprattutto in relazione all'utilizzo di dispositivi di proprietà del dipendente:

1. l'utilizzo della suite è rigorosamente da effettuarsi tramite browser senza altre installazioni e/o configurazioni
2. la propria utenza con dominio @scuole.provincia.tn.it, ha spazio illimitato (comprensivi di posta e spazio di archiviazione su GDrive).

Utilizzo dei documenti e delle cartelle GSuite

Ferme restando le disposizioni vigenti in materia di sicurezza, privacy ed utilizzo degli strumenti informatici, gli strumenti della Google Suite possono essere utilizzati anche fuori dalla sede lavorativa, con la strumentazione fornita dall'istituto ovvero con propri strumenti personali. Gli strumenti della Google Suite (Gmail per la posta elettronica, GDrive per l'archiviazione dei file, Google Documenti per la redazione di documenti di testo e Google Fogli per la gestione di dati in fogli di calcolo) sono infatti accessibili da qualsiasi *browser* attraverso la rete internet (anche al di fuori della intranet PAT).

Si sottolinea che l'utilizzo del Drive nelle modalità descritte successivamente è limitato alla situazione di emergenza attuale. Al termine della contingenza sarà fatta esplicita richiesta di spostare nuovamente i documenti dal Drive di Google a favore dei dischi di rete. Si chiede pertanto di trasferire su Drive solamente i documenti necessari e non gli archivi.

Drive personale

E' consigliato (quantomeno in questa situazione contingente) trasferire i file regolarmente utilizzati per lavoro - presenti sui dischi di rete - sul proprio Drive personale.

In particolare i file necessari alle proprie attività attualmente caricati nelle directory di rete vanno copiati nel drive personale, allo scopo di poter essere accessibili ovunque e da qualunque dispositivo ci si colleghi.

Al seguente link una breve spiegazione di come caricare e condividere i file

<https://www.youtube.com/watch?v=-67FCHtWCEQ>

Si evidenzia che Google Drive fornisce la possibilità di editare i file Microsoft Office direttamente (per quanto con funzionalità più limitate), mentre per i file Libreoffice tale possibilità non è disponibile. Si suggerisce quindi di caricare il file Libreoffice e convertirli in formato nativo Google una sola volta. Si ricorda che la conversione da un formato all'altro può comportare una diversa gestione della formattazione. **Si suggerisce quindi di redigere il documento in formato nativo Google.**

Drive di struttura

Il drive di queste caselle (ove esistente) può essere utilizzato come punto di partenza per progetti o iniziative riconducibili alle competenze della struttura.

I referenti delle caselle di struttura creeranno una cartella ad hoc per il progetto/iniziativa e metteranno in condivisione la stessa con i componenti del gruppo di lavoro secondo indicazione del responsabile del progetto/iniziativa.

Tutti i documenti creati dai colleghi per il progetto/iniziativa dovranno essere salvati nella cartella condivisa e, in fase di creazione, la proprietà dovrà essere passata alla casella della struttura. In questo modo ogni documento sarà lavorabile da tutto il gruppo, ma di effettiva proprietà della casella di struttura.

Tutti i documenti, in formato nativo Google, non occupano spazio sul drive.

Connessioni di rete per le attività lavorative

Connessione personale ad internet dal domicilio

Non ci sono preclusioni alla tipologia di connessione alla rete internet che, per le attività di lavoro, potrà essere di tipo fisso (ADSL, Fibra), Wireless (antenna WiFi) o mobile (3G, 4G, 5G).

La velocità della connessione internet dipende poi da tanti fattori. E' opportuno effettuare un test di utilizzo degli strumenti di lavoro individuati e quindi segnalare al proprio responsabile l'impossibilità di svolgere determinate attività mettendosi nelle condizioni di svolgere attività differenti o farsi supportare dai colleghi o dal servizio di Help Desk per gli impedimenti tecnologici del caso.

Applicazioni accessibili senza VPN

SAA Anagrafe Studenti

SOD Sistema Organico Docenti

RAV Sistema Autovalutazione

accessibili all'indirizzo <https://www.istruzione.provincia.tn.it/>

ISI nuovo sistema istruzione

accessibile all'indirizzo <https://bit.ly/33hcmdh>

REL registro elettronico

accessibile all'indirizzo <https://bit.ly/2wN6PPJ>

Applicazioni accessibili solo con VPN

PiTre Protocollo

accessibile al link <https://www.pitre.tn.it/>

SAP Contabilità

accesso tramite client (*richiede installazione client SapGui*)

S1P Sistema del personale (citrix)

Accesso tramite client scaricabile da <http://gestione.scuole.provincia.tn.it/>

Procedura di installazione del Client VPN per le applicazioni di Trentino Digitale (Pitre,SAP, Citrix)

Se per l'utilizzo delle G-Suite, descritta precedentemente, e degli applicativi indicati nel paragrafo "Applicazioni accessibili senza VPN" non è necessario il collegamento diretto alla rete TELPAT, **per fruire di alcuni sistemi applicativi PAT (es: Pitre, Sap, c.d. Citrix) e del collegamento tramite il PC di casa**, è necessaria la connettività "privata" verso la rete TELPAT. Per poter attivare il collegamento alla rete dell'ufficio è necessario compilare l'**allegato 3** e inviarlo a Trentino Digitale S.p.A.

E' comunque possibile installare in autonomia il software denominato "client VPN" seguendo le istruzioni operative in **Allegato 4**. Al riguardo, preme evidenziare che l'accesso alla Telpat tramite VPN è comunque subordinato alla attribuzione delle credenziali da parte di Trentino Digitale.

Servizio di assistenza e call center

Per facilitare l'avvio delle disposizioni e dell'assetto tecnico e organizzativo del presente documento è attivo un servizio dedicato svolto da Trentino Digitale spa.

Coordinate di contatto

telefonico : 0461 800200

e_mail: csd.assistenza@tndigit.it

oppure

Ufficio Innovazione e Informatica

telefonico: 0461497272

e_mail: informatica.scuola@provincia.tn.it

Problematiche per le quali è possibile contattare il servizio di assistenza

- prima configurazione dispositivo personale per accesso VPN
- utilizzo di particolari applicativi da remoto
- malfunzionamenti di Gsuite (con dominio @scuole.provincia.tn.it)

Orari di apertura

Il servizio CSD è operativo telefonicamente dalle ore 8:00 alle ore 17:00.
Eventuali mail inviate dopo le ore 17:00 saranno prese in carico il giorno successivo

Servizio di recall

Nel caso di richiesta di supporto che non evasa al primo contatto, sarà cura delle strutture tecniche di Trentino Digitale richiamare. E' per questo necessario venga sempre lasciato un eventuale recapito telefonico piuttosto che una mail a cui indirizzare le risposte.

Disclaimer: l'assistenza è svolta senza un processo definito e una gestione strutturata delle problematiche, è presumibile infatti che ogni contatto ponga al reparto tecnico problematiche specifiche tipiche del contesto BYOD. Si raccomanda quindi la massima attenzione a esporre in modo dettagliato il problema e nel contempo massima disponibilità per tempi e modi di soluzione del problema.

Glossario

Termine	Definizione
BYOD	Acronimo di "Bring Your Own Device" porta e utilizza il tuo dispositivo, principio che consente di utilizzare il proprio computer o device in un contesto lavorativo o scolastico
CSD	Acronimo di Customer Service Desk, servizio di assistenza utenti gestito da Trentino Digitale
Device	Dispositivo, usato in senso generale quando ci si riferisce a computer fissi o mobili o a telefoni cellulari e tablet
Drive (Gdrive)	Il disco virtuale all'interno della soluzione Google Gsuite sul quale sono depositato i documenti e i file che vengono prodotti sia all'interno della Gsuite che all'esterno. Il disco utilizza tecnologie Cloud e in questo contesto sostituisce i dischi di rete abitualmente utilizzati.
Recall	Modalità di contatto secondo la quale il call center richiama l'utente in modo proattivo
Snom	Azienda produttrice dei telefoni utilizzati in PAT
Voip	Acronimo Voice Over IP: tecnologia che consente la comunicazione voce su rete Internet
VPN	Acronimo di: "Virtual Private Network", Rete Privata Virtuale, crea un "tunnel" tra la propria postazione e i servizi applicativi PAT che consente il rispetto di tutte le policy di sicurezza per l'accesso ai sistemi.

