1.Oggetto e definizioni

Il presente documento ha la funzione di informare gli incaricati al trattamento dei dati personali in merito alle misure predisposte al fine di garantire la sicurezza degli stessi.

Definizioni:	*Significato*
Dati personali	qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale
Dati sensibili	I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazione a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale, possono essere oggetto di trattamento solo con il consenso scritto dell'interessato
Dati anonimi	il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
Titolare	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza;
Incaricato	la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile
Responsabile	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
Amministratore di sistema	Il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema informativo.
Misure minime	Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza,

	previste nel presente regolamento, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti.
Trattamento	Qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.
Comunicazione	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Password o parole chiave	Codice identificativo personale e segreto per l'accesso agli elaboratori e/o archivi informatici.
Diffusione	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
s.o.	Sistema Operativo.
Firewall	Misura antiintrusione hardware o software per proteggersi da accessi non autorizzati dall'esterno.
Rilevante interesse pubblico	Sono ritenute tali quelle attività che rientrano nella sfera d'azione del ente locale e per il quale è autorizzato il trattamento dei dati sensibili la cui disciplina è demandata all'art. 20 comma 1 del D.Lgs. 196/2003 e più in dettaglio dagli artt. 59 – 73 del citato Decreto.

2.Disposizioni Generali

Titolare dei dati: Comune di Ostiglia.

Cautele generali a cura degli incaricati del trattamento dei dati:

-I dati trattati, riferibili a persone fisiche, sono quelli esclusivamente finalizzati alla propria attività lavorativa.

-Ogni comunicazione o trasmissione esterna all'Ente (non dovuta da obblighi di legge) deve essere preventivamente autorizzata dal responsabile.

-L'incaricato è comunque tenuto alla riservatezza in tutte le fasi del trattamento e della comunicazione dei dati al fine di non incorrere in conseguenze penali e sanzionatorie.

-Anche nel caso di comunicazioni consentite deve essere prestata la massima cautela evitando inutili passaggi dei dati sia in formato informatico che non (documenti, immagini, ecc.)

-Deve garantire la correttezza dei dati trattati.

-I dati personali (sia in formato elettronico che non) non più necessari per l'attività lavorativa devono essere restituiti o eliminati o cancellati.

-Qualora si riscontri che alcuni di questi dati possano dare direttamente o indirettamente indicazioni circa:

- Lo stato di salute
- Le convinzioni politiche, religiose o sanitarie
- Le abitudini sessuali
- L' origine razziale o etnica
- Eventuali situazioni giudiziarie penali dell'interessato

deve essere prontamente contattato il responsabile o titolare del trattamento per ricevere precise istruzioni in merito al loro trattamento

Accesso ai locali:

L'accesso ai locali è consentito solo durante gli orari di lavoro (ordinario e/o straordinario).

Gli edifici interessati dal presente Documento sono gli immobili destinati alle attività dell'Ente ed ubicati:
- Sede Municipale, Via Gnocchi Viani, 16 Ostiglia

I locali i cui archivi contengano dati sensibili devono essere chiusi a chiave e gli accessi controllati.

Durante gli orari di lavoro devono essere costantemente presidiati dall'incaricato e in caso di allontanamento dagli stessi chiusi ed attuate le misure di protezione del caso.

I possessori delle chiavi dei locali i cui archivi contengano dati sensibili o giudiziari devono essere identificati nominalmente (6.2) e le chiavi disposte in posizioni sicure (cassaforte o analoghe).

Ove possibile gli armadi o i contenitori contenenti dati sensibili o giudiziari devono essere chiusi a chiave.

Gli accessi fuori orario devono essere autorizzati per:
- locali appositamente identificati, per gli organi istituzionali
- addetti alle pulizie previo registrazione degli accessi, dei soggetti e della durata (6.1)

Protocollazione
Ciascuno in questa fase deve aver cura di definire l'oggetto della protocollazione in modo che dallo stesso non emergano evidenze di dati o situazioni personali reputate sensibili.

Informazione e formazione:
Il presente documento deve essere reso disponibile a tutti gli incaricati.
I Responsabili devono farsi carico della formazione in materia di privacy, propria e dei collaboratori.

Commissioni ed organismi politico/amministrativi:
Tutti gli organismi che per esplicare la loro attività devono accedere ai dati personali di titolarità dell'ente sono equiparati agli incaricati e devono attenersi alle indicazioni di carattere generale riferibili agli stessi.

Nel caso si trovassero a dover trattare, per motivi attinenti le proprie funzioni, dati configurabili come “sensibili”, devono preventivamente ricevere istruzioni a cura del titolare (nella figura del Sindaco) o del responsabile competente.

Devono in ogni caso esimersi da trattamenti e/o comunicazioni non autorizzate al fine di non incorrere in sanzioni di natura penale.

Professionisti esterni che gestiscono dati personali e sensibili di titolarità del comune
Viene richiesta una dichiarazione circa:

- le modalità di trattamento
- le misure di sicurezza adottate

Obiettori e volontari
Sono considerati incaricati e devono attenersi alle prescrizioni di carattere generale qui riportate.

In nessuna delle mansioni svolte devono aver accesso a dati di natura sensibile, tranne nell’attività di gestione della biblioteca (dati solo potenzialmente sensibili), dove devono aver cura di non comunicare a persone esterne i detentori di testi e di gestire la documentazione e gli archivi in loro possesso con la massima riservatezza.

Per qualsiasi informazione/istruzione in merito al trattamento dei dati personali, devono rivolgersi al responsabile di area/servizio al quale sono assegnati.

Comunicazioni agli interessati
La comunicazione dei dati è sempre possibile ai fini di esercitare il diritto all’aggiornamento, conoscenza, correttezza degli stessi all’interessato (art. 7 D.Lgs. 196/2003) e nei casi previsti da legge ai soggetti aventi un interesse legittimo verso i dati stessi.

Accesso ai dati
Come disciplinato dall’art. 60 del D.Lgs. 196/2003, quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

In tutti gli altri casi, con riferimento ai soli atti amministrativi, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241 e successive modificazioni, e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.

Gestione del Sistema Informatico del Comune

Struttura del sistema informatico e protezioni:
Il sistema informatico è strutturato come segue:

- n. 1 Server WINDOW 2000.
- Postazioni Pc per ciascun incaricato, attrezzate con S.O. Windows XP PRO, la maggior parte, Windows 98 e Windows 2000 PRO, il cui elenco e attribuzione viene gestito ed aggiornato a cura dell'amministratore del sistema.
- Le singole postazioni accedono alla rete tramite sistema di autenticazione gestito da entrambi i server e gli archivi contenenti i dati personali sono localizzati sugli stessi server.

Ad ogni utente sono attribuiti quindi 2 livelli di password:
1 – identificativo e password per l'accesso alla rete e quindi al server
2 – identificativo e password per l'accesso ai singoli programmi

Tutti i PC hanno accesso ad internet, mediante linea ADSL a larga banda (Telecom) tramite router Adsl CISCO serie 800. Protezione intrusioni dall'esterno mediante servizio di Firewall hardware installato presso l'ente e gestito da Telecom.
Tutte le postazioni PC utilizzano un antivirus (Norton Antivirus Corporate) in modalità attiva, con aggiornamento quotidiano e con una frequenza di scansione impostata giornalmente.

Tutti gli utenti hanno una propria casella di posta elettronica.

Le diverse postazioni accedono, ciascuna con i propri livelli di autorizzazione, ai diversi programmi utilizzati dall'Ente, che sono:

-Microsoft Office SBE, Professional 97/2000/XP
-Sun StarOffice 6.0
-OpenOffice 1.0.1
-Applicativi software house SinteCop (servizi demografici, area economica finanziaria, inventario)
-Applicativi software house Studio K (gestione delibere e determine, protocollo)
-Applicativo Asi per il protocollo informatico con base dati a Mantova
-Applicativi Maggioli

-Gate 2000 (gestione pratiche edilizie)
-Autodesk Autocad,
Utility varie di masterizzazione, stampa in formato PDF, ecc.

L'amministratore del sistema informatico si avvale di consulenze esterne sia per il profilo hardware sia per quello software.

Amministratore del sistema: Paolo Carpigiani

Soggetto preposto alla custodia delle password e alla loro eventuale disattivazione: Paolo Carpigiani

Salvataggio dei dati:
I supporti di backup del sistema vengono utilizzati con il sistema della rotazione giornaliera, mensile, bisettimanale e bimestrale tramite 10 nastri DAT. I nomi delle cassette sono:
-Lunedi
-Martedi
-Mercoledi
-Giovedi
-Venerdi
-Sabato
-inizio mese pari
-metà mese pari
-inizio mese dispari
-metà mese dispari
I supporti vengono riutilizzati per un anno: trascorso tale periodo i nastri per i backup giornaliere vengono distrutti, mentre quelli per i backup mensili vengono utilizzati come giornalieri per essere rimpiazzati da nuovi nastri.
Verifiche a campione dell'efficienza dei backup con cadenza periodica (settimanale)effettuate dall'amministratore del sistema.
I nastri vengono conservati in una cassettiere in un locale non adiacente al CED presidiata o chiusa a chiave quando non presidiata.

All'interno dell'area economico-finanziaria è stato individuato un responsabile per la sostituzione giornaliera dei nastri (Rosanna Bianconi) il quale è stato istruito sulle modalità per l'inserimento, l'estrazione, la verifica del corretto alloggiamento e per la metologia adottata.

Chiunque utilizzi supporti magnetici per il salvataggio dei dati (dischetti, ecc.), se utilizzati per dati personali, deve trattare i supporti con la stessa cura preposta per i documenti che li hanno originati.

Per ciascun utente vengono predisposte dall'amministratore di sistema specifiche cartelle riservate, su server, su cui archiviare i dati che verranno successivamente salvati mediante backup.

Modalità di gestione delle password:

1. Il responsabile di area deve assicurarsi che ciascun utente (mediante l'ausilio eventuale dell'amministratore di sistema) sia in grado di modificare e proceda nella modifica dei livelli di password previsti.
2. In caso di:
    a. Cambio mansioni
    b. Sostituzione macchina
    c. Dimissioni /nuovi inserimenti

   l'amministratore di sistema deve provvedere all'adeguamento del sistema autorizzativi e l'incaricato deve sostituire la password al primo accesso successivo.
3. L'amministratore di sistema deve assicurarsi che, qualora non gli sia possibile intervenire con le autorizzazioni specifiche di amministratore di dominio, l'incaricato compili l'apposito modulo che gli verrà consegnato ed archiviato in busta chiusa, identificando sulla stessa la data di assegnazione

Ogni incaricato che definisce le proprie password ne è direttamente responsabile e non deve in alcun modo comunicarle a persone diverse od altri incaricati; qualora abbia il timore che la propria password sia divenuta di conoscenza di altri soggetti deve prontamente darne comunicazione al responsabile incaricato al fine di attivare la procedura di sostituzione di cui sopra.

Non devono essere utilizzati come password nomi facilmente identificabili ma devono essere utilizzate sequenze alfanumeriche di almeno 8 caratteri nella tipologia riportata:

es.: M1C1S9C2 oppure A333ZXXX..

Qualora ci si assenti per un periodo superiore ai 15 minuti dalla propria postazione è necessario procedere alla chiusura della sessione di lavoro attiva.

Il cambio password è obbligato ogno 3 mesi da procedura automatizzata.

Programmi antivirus e corretta gestione del software:
Gli amministratori di sistema provvederanno con frequenza almeno semestrale (e comunque ad ogni aggiornamento disponibile) a verificare l'attività dell'antivirus installato.

Il pacchetto antivirus installato è Norton AntiVirus Corporate, che si aggiorna giornalmente via Internet sul server che provvede alla distribuzione delle definizioni dei virus ai singoli clients.

Ogni incaricato è tenuto ad utilizzare solo il software autorizzato ed è direttamente responsabile di ogni pregiudizio dei dati causato dall'installazione di software non autorizzato e testato quali virus, danneggiamento di archivi e perdita di dati.

Si deve in ogni modo evitare di:
- -scaricare software non autorizzati da internet,
- -aprire allegati in posta elettronica e/o interna provenienti da fonti non conosciute, senza essersi preventivamente accertati della fonte

e, nel caso ciò si rendesse necessario, averne la preventiva autorizzazione dal responsabile di sistema.

Ogni problema inerente la sicurezza o l'affidabilità del sistema deve essere prontamente segnalato all'amministratore di sistema.

Società esterne di manutenzione ed assistenza:
Le società che effettuino manutenzione dei sistemi hardware o software sono considerate responsabili dei dati e devono a tale scopo rispettare le seguenti cautele:

1. Non effettuare copie o procedere alla eliminazione degli archivi informatici detenuti di titolarità dell'ente.

2.Informare l'amministratore di sistema degli interventi che andranno ad attuare.
3.Eventuali collegamenti in tele assistenza devono essere preventivamente autorizzati dall'amministratore di sistema.

Tutti i fornitori che utilizzino dati dell'ente devono rilasciare dichiarazione circa il rispetto della normativa in materia di privacy e di attuazione delle misure minime di protezione dei dati personali (6.4).

I fornitori di software sono tenuti a:
1 – fornire tutte le indicazioni tecniche circa la protezione delle aree di programma
2 – garantire di non avere copie degli archivi dell'ente o, in caso contrario, indicare quali sono le misure di sicurezza adottate
3 – segnalare prontamente ogni problema che possa pregiudicare la sicurezza dei dati dell'Ente.

3.Analisi dei rischi che incombono sui dati

Codice	*Categorie di rischi*	*Grado di rischio*	*Dettaglio*
R1	Minacce ambientali	Basso	Incendio, caduta tensione
R2	Malfunzionamenti	Medio	Problemi Hardware
R3	Minacce interne	Medio	Disattenzione del personale
R4	Minacce esterne	Basso	Hacker, furto del server
R5	Minacce probabili	Medio	Virus, errori software
R6	Rischio di integrità	Basso	Disattenzione del personale
R7	Rischio di riservatezza	Basso	Disattenzione del personale, Hacker
R8	Rischio di disponibilità	Medio	Per furto, virus, errori Software, Hacker, malfunzionamenti, incendio

LEGENDA:
la descrizione dell'impatto sulla sicurezza (alta/media/bassa) è data da due componenti:
- gravità del danno che si potrebbe verificare,
- stima della probabilità che il danno si verifichi.

4.Elenco misure di sicurezza tecniche e organizzative predisposte

Codice	*Descrizione*	*Rischio Coperto*	*Tipologia*	
			Tecniche	Organizzative
I1	Archivi protetti da codice identificativo e password per utente (vedi punto 3)	R4, R7	X	X
I2	Archivi protetti da password di accesso all'elaboratore	R4, R7	X	
I3	Protezione hardware o software all'accesso esterno	R4	X	
I4	Controllo antivirus periodico	R4, R5, R7	X	
I5	Supporti di memorizzazione da non riutilizzare per archiviazioni aggiuntive, salvo il caso di formattazione per la cancellazione completa dei dati	R1-R8	X	X
I6	Installazione gruppo di continuità per Server ed altri PC che contengono dati personali	R1, R2, R8	X	
O1	Locali muniti di sicurezza (chiusi a chiave in caso di assenza dell'incaricato)	R4, R8		X
O2	Archivi/contenitori muniti di sicurezza (chiusi a chiave in caso di assenza dell'incaricato)	R3, R4, R8		X
O3	Precise istruzioni agli addetti	R1-R8		X
O4	Controllo degli accessi fuori orario	R4, R8		X
O5	Rilascio autorizzazione formale agli incaricati	R3		X

NB: le codifiche di "R" separate da virgole (,) si riferiscono alle singole tipologie di rischio, mentre le codifiche di "R" separate da linee (-) fanno riferimento ad intervalli di rischio (da … a …), così come specificato nella tabella di cui al punto 3.

5.Disposizioni specifiche

5.1AREA ECONOMICO FINANZIARIA
Responsabile del trattamento dei dati personali: Responsabile di Area

5.1.1 Area Contabilità - Economato

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Bilanci e rendiconti	No	Cartaceo e informatico	Raccolta, elaborazione, archiviazione, trasmissione	Tipografia	R1 – R8	I1,I2,I3,I4, I6, O3,O5
Richieste contributi associazioni	No	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O3, O5
Pratiche di contributi/assegni -dich. Redditi -assegni famigliari -..	No	Cartaceo	Verifica		R1, R3, R7, R8	O3, O5
Preventivi	No	Cartaceo e informatico	Raccolta, elaborazione, archiviazione		R1 – R8	I1,I2,I3,I4, I6, O3,O5
Determine	No	Cartaceo e informatico	Visto di conformità	Pubblicazione (con allegati)	R1 – R8	I1,I2,I3,I4, I6, O3,O5
Albo dei Beneficiari	No	Cartaceo e informatico	Raccolta, elaborazione, archiviazione, trasmissione	Invio in forma completa al ministero Pubblicazione (con omississ)	R1 – R8	I1,I2,I3,I4, I6, O3,O5

Per quanto riguarda tutti i servizi a domanda individuale, che vengono fatturati dal Comune, il responsabile del servizio finanziario dovrà organizzare l'invio dell'informativa ex art. 13 D. Lgs. 196/2003 a tutti i Clienti e a tutti i Fornitori, con cui il Comune ha avuto rapporti nel 2004 e negli anni successivi.
Il Comune non gestisce direttamente le mense scolastiche ma c'è un apposito capitolato con la …….che gestisce tutta la documentazione.

5.1.2. Area Personale – Organizzazione (gestione giuridico - amministrativa)

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Certificati Medici (buste chiuse)	Si	Cartaceo	Archiviazione	Medico incaricato	R1, R3, R7, R8	O1, O2,O3,O4,O5
Fascicolo personale -stato famiglia -Certificati di malattia -Casellario giudiziale	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Rilevazione Presenze	No	Cartaceo e informatico	Raccolta, elaborazione, archiviazione		R1 – R8	I1,I2,I3,I4, I6, O3,O5
Registro Infortuni e tutti allegati	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Iscrizione a Sindacati	Si	Cartaceo e informatico	Raccolta, elaborazione, archiviazione	Sindacati e banche, per versamento trattenute	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Pratiche Pensioni INPS e Ministero del tesoro	No	Cartaceo e informatico	Raccolta, elaborazione, archiviazione	INPS Minist. Tesoro Altri Enti locali	R1 – R8	I1,I2,I3,I4, I6, O3,O5
Documentazione obiettori -certificati medici -permessi -comunicazioni al distretto	Si	Cartaceo	Raccolta, elaborazione, archiviazione	U.N.S.C. (ufficio nazionale per il servizio civile	R1, R3, R7, R8	O1, O2,O3,O4,O5

Per quanto riguarda le assenze per malattia del personale dipendente, tutti i certificati medici arrivano al Capo Settore, che li esamina e provvede direttamente ad inoltrarli all'Ufficio del Personale, il quale può richiedere la visita fiscale dopo il 3° giorno di assenza.

5.1.3.Tributi

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
ICI: autocertificazione dichiarazioni	No	Cartaceo e informatico	Raccolta, elaborazione, archiviazione		R1 – R8	I1,I2,I3,I4, I6, O3,O5
TARSU: Reddito minimo INPS dichiarazione redditi	No	Cartaceo	Raccolta, elaborazione, archiviazione	Siem	R1, R3, R7, R8	O3, O5
Ruoli ICI e TARSU e plateatici	Potenzialmente	Cartaceo e informatico	Raccolta, elaborazione, archiviazione, trasmissione	Concessionario della riscossione	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Pratiche di accertamento: doc. di supporto (dich. Redd., estratti, ecc.)	No	Cartaceo e informatico	Raccolta, elaborazione, archiviazione		R1 – R8	I1,I2,I3,I4, I6, O3,O5
Occupazione Spazi ed Aree Pubbliche (T.O.S.A.P. e C.O.S.A.P.)	No	Cartaceo e informatico	Raccolta, elaborazione, archiviazione	Promozione iniziative	R1 – R8	I1,I2,I3,I4, I6, O3,O5
Atto di compravendita e successione	No	Cartaceo e informatico	Raccolta, elaborazione, archiviazione		R1 – R8	I1,I2,I3,I4, I6, O3,O5
Banca dati catasto	No	Cartaceo e informatico	Raccolta, elaborazione, archiviazione		R1 – R8	I1,I2,I3,I4, I6, O3,O5

5.2AREA SERVIZI ALLA PERSONA

Responsabile del trattamento dei dati personali: il Responsabile di Area

5.2.1 Servizi demografici: anagrafe, stato civile, elettorale e leva

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Cartellini anagrafici Schede famiglia	Potenzialmente	Cartaceo Informatico	Aggiornamento, archiviazione		R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Schedario per stranieri – permessi soggiorno – passaporti	Si	Cartaceo Informatico	Aggiornamento, archiviazione	Istat, questura, altri Enti locali (comune di prov./dest.) ASL	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Pratiche immigrazione/emigrazione	Si	Cartaceo	Raccolta, elaborazione, archiviazione	Istat	R1, R3, R7, R8	O1, O2,O3,O4,O5
Pratiche Pensioni INPS e Ministero del tesoro	No	Cartaceo	Raccolta, elaborazione, archiviazione	INPS Minist. Tesoro Altri Enti locali	R1, R3, R7, R8	O3, O5
Atti di nascita	Potenzialmente	Cartaceo Informatico	Raccolta, elaborazione, archiviazione	ASL ISTAT	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Cert. Comulativo di residenza, cittadinanza e stato libero	Potenzialmente	Cartaceo Informatico	Raccolta, elaborazione, archiviazione		R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Atto di morte	No	Cartaceo Informatico	Raccolta, elaborazione, archiviazione	ASL ISTAT Medicina preventiva delle comunità	R1, R3, R7, R8	I1,I2,I3,I4, I6, O3,O5
Gestione dei Loculi	Potenzialmente	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Permessi seppellimento e trasporto salme	Si	Cartaceo	Raccolta ed archiviazione	Comuni di provenienza o destinazione	R1, R3, R7, R8	O1, O2,O3,O4,O5
Pratiche di immigrazione ed emigrazione	Si	Cartaceo	Raccolta, elaborazione, archiviazione	Comune di origine Questura ISTAT	R1, R3, R7, R8	O1, O2,O3,O4,O5

Liste di leva (solo esonero senza motivazioni)	Si	Cartaceo	Raccolta, elaborazione, archiviazione	distretto militare	R1, R3, R7, R8	O1, O2,O3,O4,O5
Liste Elettorali	Si	Cartaceo	Raccolta, elaborazione, archiviazione	C.E.M.	R1, R3, R7, R8	O1, O2,O3,O4,O5
Registro elettori che hanno perso i diritti politici	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Registro elettori all'estero	Si	Cartaceo e informatico	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O3,O4,O5
Fascicolo per ogni elettore: -casellario giudiz. -Cert. Nascita -Residenza -Notifiche	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Stato civile: -copie atto di nascita -cert. Comulativo di residenza, cittadinanza e stato libero -copie atti di matrimonio -atto di morte	Si	Cartaceo	Raccolta, elaborazione, archiviazione (Archiviato per 1 anno)	Procura	R1, R3, R7, R8	O1, O2,O3,O4,O5
Registri stato civile	Si	Cartaceo	Raccolta, elaborazione, archiviazione	Procura Prefettura	R1, R3, R7, R8	O1, O2,O3,O4,O5
Allegati ai Registri di stato civile	Si	Cartaceo	Raccolta e archiviazione (1 anno)	Procura	R1, R3, R7, R8	O1, O2,O3,O4,O5
Autorizzazioni alla cremazione/seppellimento	Si	Cartaceo	Raccolta, elaborazione, archiviazione	Forno crematorio competente	R1, R3, R7, R8	O1, O2,O3,O4,O5
Comunicazione dei decessi (senza indicazione causa di morte)	No	Cartaceo	Elaborazione e trasmissione	ASL INPS Dir. Prov. Tesoro INPDAP Distretto militare	R1, R3, R7, R8	O3, O5
Documentazione per ric. Figli naturali:	Si	Cartaceo	Raccolta, elaborazione, archiviazione	Autorità giudiz.	R1, R3, R7, R8	O1, O2,O3,O4,O5

-atto di nascita -cert. Com. residenza, cittadinanza, stato libero -atto di matrimonio						
Concessone dei Loculi	Potenzialmente	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5

5.2.2. Servizio Assistente Sociale

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Cartelle individuali per ogni singolo assistito: (cartelle sanitarie,verbali, ecc.)	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Relazioni sui minori al tribunale: Decreto del tribunale Parere ASL	Si (Sensibili e Giudiziari)	Cartaceo	Raccolta, elaborazione, archiviazione	Scuola Servizi specialistici ASL	R1, R3, R7, R8	O1, O2,O3,O4,O5
Pratiche ISEE	Potenzialmente	Cartaceo e informatico	Raccolta, elaborazione, archiviazione	CAAF (apposita convenzione)	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Documentazione Trattamenti sanitari obbligatori (TSO)	Si	Cartaceo	Raccolta, elaborazione, archiviazione	Giudice tutelare Istituti Sanitari	R1, R3, R7, R8	O1, O2,O3,O4,O5
Pratiche adozioni e affidi familiari	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Situazioni di handicap	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Pratiche trasporto utenti assistiti in centri di cura	Si	Cartaceo	Visione e restituzione all'assistito		R1, R3, R7, R8	O1, O2,O3,O4,O5

Tutta la documentazione cartacea viene archiviata in cartelle personali intestate al soggetto.

5.2.3. Servizio Assistenza Domiciliare (S.A.D.)

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Utenti in carico al servizio domiciliare: (cartelle sanitarie,verbali, ecc.)	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Elenchi per contributi economici e documentazione di supporto	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Relazioni per ab./Case popolari: . ASL . Uff. igiene . Uff. tecnico	Potenzialmente	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5

5.2.4 INFORMAGIOVANI

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Elenchi utenti	No	Cartaceo e informatico	Raccolta, elaborazione, archiviazione		R1 – R8	I1,I2,I3,I4, I6, O3, O5

AREA AMMINISTRATIVA

Responsabile del trattamento dei dati personali: il Responsabile di Area

5.3.1 Protocollo

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Protocollazione Ordinaria Riservata	 No Si	Informatico	Raccolta e trasmissione agli uffici destinatari		R1 – R8	I1,I2,I3,I4,I5, I6, O3 (vedi Riferimenti Normativi)
Corrispondenza in entrata	Potenzialmente	Cartaceo e informatico	Raccolta e trasmissione		R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Determine	No	Cartaceo e informatico	Archiviazione		R1 – R8	I1,I2,I3,I4, I6, O3,O5
Archivio Delibere	No (possibili in allegati)	Cartaceo e informatico	Archiviazione Consultazione		R1 – R8	I1,I2,I3,I4, I6, O3,O5

Il programma per il protocollo informatico è in fase iniziale e sarà operativo dall'inizio del 2005.
Le Determine e le Delibere sono accessibili a tutti.
Le Delibere consiliari e/o di Giunta sono atti pubblici, liberamente consultabili da chiunque. L'incaricato deve avere l'avvertenza di non rendere pubblici tutti gli allegati alle delibere, soprattutto qualora questi allegati contengano dati sensibili e/o giudiziali.

5.3.2 Segreteria

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Comunicazioni infortuni sul lavoro	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5

5.3.3 Legale

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Archivio Protesti	Si	Cartaceo	Archiviazione Consultazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Archivio legale storico	SI	Cartaceo	Archiviazione Consultazione		R1, R3, R7, R8	O1, O2,O3,O4,O5

5.3.4.Contratti

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Archivio legale storico e contratti	No	Cartaceo	Archiviazione Consultazione		R1, R3, R7, R8	O3, O5
Pareri legali	Potenzialmente	Cartaceo	Raccolta e trasmissione	Avvocati cui si chiede parere	R1, R3, R7, R8	O1, O2,O3,O4,O5

5.3.5.Commercio

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Richiesta licenze: casellario giudiziale procedimenti in corso antimafia autorizz. ASL cartellino sanitario …	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Elenchi ditte	No	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O3, O5

Cartella ditta e doc. allegata	No	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O3, O5
Censimenti commerciali (agricoltura, ecc.):	No	Cartaceo	Raccolta, elaborazione, archiviazione	ISTAT	R1, R3, R7, R8	O3, O5
Autorizzazioni Produttive o commerciali	No	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O3, O5
Elenco attività agricole	No	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O3, O5

Per l'area Commercio viene utilizzato apposito programma che si trova installato sul PC del Sig. Sanna.

5.3.6.Sportello Unico

Lo sportello unico è ancora in fase di sviluppo e verrà gestito tramite una convezione con altri quattordici comuni denominata "Area Ostigliese Destra Secchia" via internet con apposito programma (Genuit).

5.3.7. Biblioteca

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Elenchi utenti	No	Cartaceo e informatico	Raccolta, elaborazione, archiviazione		R1 – R8	I1,I2,I3,I4, I6, O3, O5

I Personal Computer della Biblioteca costituiscono una rete informatica autonoma, distinta dal sistema informativo comunale, con proprio accesso ad Internet; esiste un collegamento alla rete bibliotecaria della Provincia di Padova, gestito da un server localizzato a Padova.
Il Comune è pur sempre il Titolare del trattamento dei dati, ma occorre indicare nell'informativa che il Comune potrà trasferire i dati degli iscritti al servizio interbibliotecario che diventa così un responsabile esterno del trattamento dei dati.

5.3.8. Cultura

Tipologia di dati	Presenza di dati	Tipologia di Supporto	Principali tipologie di	Comunicazione	Rischi	Principali Misure di

	Sensibili o giudiziari		Trattamento			sicurezza
Elenchi associazioni	No	Cartaceo e informatico	Raccolta, elaborazione, archiviazione	Promozione iniziative	R1 – R8	I1,I2,I3,I4,I5, I6, O3
Comunicazioni di manifestazioni ed iniziative	No	Cartaceo e informatico	Raccolta, elaborazione, archiviazione	Promozione iniziative	R1 – R8	I1,I2,I3,I4,I5, I6, O3

Tutte le iniziative promozionali dovranno prevedere la facoltà per l'interessato di cancellarsi dagli elenchi, per non ricevere più nulla a riguardo.

5.4.AREA URBANISTICA E ECOLOGIA

Responsabile del trattamento dei dati personali: il Responsabile di Area

5.4.1.Urbanistica

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Richieste di varianti al PRG	Potenzialmente	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Osservazioni al PRG	Potenzialmente	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Richiesta per edilizia economica popolare (cond. Igieniche)	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Legge 13/99 (Contributi barriere architettoniche)	No (solo in caso di richiesta contributi, c'è apposita fase istruttoria gestita da Servizi Sociali)	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O3, O5
Richieste PEEP (Verifica requisiti e doc. allegata: dich. Redditi, ..)	No (solo dati economici)	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O3, O5
Destinazione Urbanistica	No	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O3, O5

Le pratiche in merito alla L. 13/99 sono gestite in contemporanea con l'Ufficio dei Servizi alla Persona.

5.4.2.Edilizia privata

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Permessi di Costruzione / autorizzazioni edilizia (documentazione di supporto)	Potenzialmente	Cartaceo e informatico	Raccolta, elaborazione, archiviazione, trasmissione	Ministero Lavori Pubblici; Regione Lombardia	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Sopralluoghi/ verifiche edilizie	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Idoneità al ricongiungimento familiare	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Denunce abusi edilizi	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Denuncia Inizio Attività (D.I.A.)	Potenzialmente	Cartaceo	Raccolta, elaborazione, archiviazione, trasmissione	Uff. Tributi	R1, R3, R7, R8	O1, O2,O3,O4,O5

Gli elenchi delle concessioni edilizie rilasciate nell'anno sono pubblici, si possono consultare dietro apposita richiesta scritta.

Il Comune ha predisposto apposito Regolamento interno per la consultazione degli atti.

5.4.3.Ecologia, tutela dell'ambiente

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Pratiche relative ad abusi ambientali	Potenzialmente	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Allacciamenti fognatura	No	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O3, O5
Registro reflui (verifica e autorizzazione scarichi)	No	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O3, O5
Controllo spandimento liquami	No	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O3, O5

Piazzole ecologiche sono gestite dalla società che coordina la raccolta dei rifiuti, la SIEM s.p.a.

5.5. AREA LAVORI PUBBLICI

Responsabile del trattamento dei dati personali: il Responsabile di Area

5.5.1. Lavori Pubblici

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Software Osservatorio Lavori Pubblici	No	Informatico	Raccolta, elaborazione, archiviazione		R1 – R8	I1,I2,I3,I4, I6, O3, O5
Documentazione tecnica relativa ai LL.PP. e urbanistica	No	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O3, O5
Documentazione di gara nuova normativa appalti (casellario giudiziale, dichiarazione antimafia)	Si	Cartaceo	Raccolta, elaborazione, archiviazione		R1, R3, R7, R8	O1, O2,O3,O4,O5
Dati tecnici inerenti il patrimonio, Documentazione tecnica PL, appalti	No	Cartaceo	Produzione, elaborazione, aggiornamento	Enti preposti ed interessati	R1, R3, R7, R8	O3, O5

5.6. POLIZIA LOCALE

Responsabile del trattamento dei dati personali: il Responsabile di Area
L'ufficio presenta n°4 Agenti di Polizia Locale, oltre al comandante e a n°2 impiegati amministrativi .

Tipologia di dati	Presenza di dati Sensibili o giudiziari	Tipologia di Supporto	Principali tipologie di Trattamento	Comunicazione	Rischi	Principali Misure di sicurezza
Atti e documentazione inerente il codice della strada	Si	Cartaceo e informatico	Raccolta, Elaborazione, archiviazione, trasmissione	Autorità giudiziaria (Giudice di Pace, Tribunale) Prefettura	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Ricorsi a Giudice di Pace e/o Prefetto	Si	Cartaceo e informatico	Raccolta, elaborazione, archiviazione, trasmissione	Giudice di Pace, Tribunale Soggetto Interessato	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Atti e documentazione inerente l'attività di vigilanza edilizia	Si	Cartaceo e informatico	Raccolta, Elaborazione, archiviazione, trasmissione	Autorità Giudiziaria e Autorità Amministrativa	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Atti e documentazione inerente l'attività di vigilanza commerciale e attività produttive (Testo Unico Legge Pubblica Sicurezza)	Si	Cartaceo e informatico	Raccolta, Elaborazione, archiviazione, trasmissione	Autorità Giudiziaria e Autorità Amministrativa Sanitarie	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Atti e documentazione per rilascio pass disabili (certificati medici, ecc.)	Si	Cartaceo e informatico	Raccolta, Elaborazione, archiviazione, trasmissione	Soggetti interessati, enti amministrativi	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Documentazione Trattamenti sanitari obbligatori (TSO)	Si	Cartaceo e informatico	Raccolta, Elaborazione, archiviazione, trasmissione	Giudice tutelare Istituti Sanitari F.O.	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Documentazione per Mercatino Antiquariato	Si	Cartaceo e informatico	Raccolta, Elaborazione, archiviazione, trasmissione	Soggetti interessati, enti amministrativi	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Ricorsi vari	Si	Cartaceo e informatico	Raccolta, Elaborazione, archiviazione, trasmissione	Autorità Amministrativa Soggetti interessati	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Denunce Autorità Giudiziaria	Si	Cartaceo e informatico	Raccolta, Elaborazione, archiviazione, trasmissione	Autorità Giudiziaria	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5

Verbali infrazioni Nas Carabinieri	Si	Cartaceo	Raccolta, Elaborazione, archiviazione, trasmissione	Autorità Giudiziaria	R1, R3, R7, R8	O1, O2,O3,O4,O5
Notifiche di Reato	Si	Cartaceo e informatico	Raccolta, elaborazione, archiviazione	Autorità Giudiziaria	R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Altra documentazione prodotta internamente (lettere, occupazione spazi aree pubbliche, infortuni sul lavoro, notifiche altri enti, antimafia, fiere, ecc)	Si	Cartaceo e informatico	Elaborazione, archiviazione		R1 – R8	I1,I2,I3,I4,I5, I6, O1,O2,O3,O4,O5
Infortunistica stradale	Sì	Cartaceo e informatico	Raccolta, elaborazione, archiviazione	Autorità Giudiziaria, Enti Privati (Assicurazioni, Agenzie investigative)		

I Personal Computer, oltre ad avere il pacchetto Office, hanno anche un programma appositamente sviluppato per la gestione dei verbali.
Un PC ha accesso ad Internet, tramite la rete comunale, ed è utilizzato solo per consultare gli archivi ACI, MTCC e PRA.
PC degli Uffici della Polizia Locale sono collegati al server SRV, con apposite cartelle e appositi livelli di accesso.
Negli Uffici della Polizia Locale c'è una centrale radio per il coordinamento di una zona di competenza che si estende, oltre al Comune di Ostiglia, ai Comuni di Revere, Serravalle e Sustinente.

6. Documentazione di Supporto

Elenco accessi fuori orario (6.1)
Dotazione Chiavi (6.2)
Lettera di incarico (6.3)
Richiesta misure di sicurezza enti esterni (6.4)
Modello d' informativa (6.5)
Consenso informato (6.6)
Lettera d'incarico volontari e obiettori (6.7)
Elenco incaricati e autorizzazione (6.8)

Principali riferimenti normativi:

D. Lgs. 196/2003 Codice in materia di protezione dei dati personali

7. Piano di attività per la sicurezza dei dati personali

		2007												
Attività			G	F	M	A	M	G	L	A	S	O	N	D
Verifica password PC e aggiornamento archivio password	Tutti i responsabili e amministratore di sistema				X									
Elenco distribuzione chiavi e eventuale sistemazione serrature di cui non si sia certi sulla distribuzione chiavi o non esista la possibilità di chiusura	Tutti i Responsabili												X	
Controllo accessi fuori orario (sono 7 accessi): •Commissioni e organi politici •Associazione •Pulizia	Responsabile Area, Segretario, Sindaco e Assessori												X	
Remissione del presente documento	Tutti i Responsabili e Giunta Comunale					X								
Salvataggio su archivi server di tutti i dati personali trattati dall'Ente	Amministratore di sistema				X	X	X							
Implementazione di un sistema di Backup su cassetta o altro supporto magnetico removibile	Amministratore di sistema				X	X	X							
Verifica Backup ed effettiva possibilità di Restore	Amministratore di sistema				X	X	X							
Mantenimento del Firewall					X	X								
Archiviare correttamente, in cassetti chiusi a chiave, i certificati medici dei dipendenti assenti, custoditi in ciascun ufficio durante il mese	Tutti i responsabili				X	X	X	X	X	X	X	X	X	X
Biblioteca: le cartelle cartacee degli utenti/libri devono essere chiuse in armadio	Responsabile Area Cultura				X	X	X	X	X	X	X	X	X	X
Biblioteca: una volta completata l'attivazione del sistema	Responsabile Area Cultura					X	X							

bibliotecario interprovinciale, predisporre adeguata informativa da consegnare a tutti gli iscritti, all'atto dell'iscrizione.														
Protocollo Informatico: predisposizione di apposito regolamento	Responsabile Area Amministrativa							X						
Rivisitazione documentazione interna (autocertificazioni, richieste biblioteca, ecc.) con autorizzazione al trattamento dei dati ai sensi D.Lgs. 196/2003. In particolare:	Tutti i responsabili											X	X	X
1. Cedolini: Predisporre informativa e consenso per comunicazione dei dati all'esterno dell'ente per la elaborazione delle buste paga	Responsabile Area											X	X	X
2. Enti esterni che vengono a contatto dei dati dell'ente: predisporre informativa e/o fare riferimento sul contratto, la responsabilità al trattamento dei dati.	Responsabile Area												X	

N.B. L=Luglio; A: Agosto, e così di seguito

8. Descrizione trattamenti affidati all'esterno

Descrizione attività	Natura del dato	Soggetto delegato	Impegni contrattuali assunti	Date e n°verifiche
Elaborazione paghe	Personali e sensibili	CDA – STUDIO LEGALE TRIBUTARIO	Richiesta informativa e dichiarazione impegno adozione misure minime	
Consulenza fiscale	Personali	CDA – STUDIO LEGALE TRIBUTARIO	Richiesta informativa e dichiarazione impegno adozione misure minime	
Assistenza informatica (hardware e software)	Personali e sensibili	-Studio Tecnico – Carpigiani Paolo -Sintecop SPA -Mainoldi & Turcato -ASI S.P.A.	Richiesta informativa e dichiarazione impegno adozione misure minime	
Consulenza legale	Giudiziale	-E&Y - Studio Legale. Tributario -Frangipane Avv. Ginetta -Studio Legale Cabianca -Giannone Avv. Antonietta -Orrick, Herrington & Sutcliffe -Studio Legale Associato (brescia)	Richiesta informativa e dichiarazione impegno adozione misure minime	

		-Orecchia Avv. Paolo -Russo Anna -Nicolini Avv. Cesare, -Gianoglio Avv. Alberto -Avv. Rigobello -Avv.Parente -Avv.Genovesi -Studio Ruggerini -Canteri Avv. Stefania -Studio Magnani Marongiu & Associati		
Consulenza sulla sicurezza nei posti di lavoro -consulenti -medico competente	Personali e sensibili	–Tassini Massimo –Dr.Sleiman Camillo	Richiesta informativa e dichiarazione impegno adozione misure minime	

9. Modalità di approvazione/revisione del presente documento

Il presente documento viene rivisto con frequenza almeno annuale, entro il 31 marzo di ogni anno, ed ogni qualvolta se ne evidenzi la necessità.

L'approvazione compete alla Giunta Comunale

Ogni nuova emissione comporta l'avanzamento del numero di revisione e l'indicazione della data.

Preventivamente alla remissione devono essere consultati i Responsabili al fine di effettuare una valutazione interna di efficacia delle misure predisposte.

10. Osservazioni di natura generale

10.1 Le disposizioni specifiche si applicano per analogia a nuove tipologie di dati non eventualmente considerate o che dovessero sorgere in seguito che in ogni caso devono sottoposte all'attenzione del responsabile.

L'amministrazione ritiene di fondamentale importanza che il personale, i collaboratori esterni, i fornitori e gli organi politici dimostrino e favoriscano una crescente "Cultura della riservatezza" che non deve interessare i soli dati di natura personale e la loro protezione ma tutti i comportamenti sia durante l'attività svolta sia all'esterno dell'Ente.