No: IT_01

Policy Name: **Email and Instant Messaging**

Objective:

Provide appropriate guidelines for productively utilizing Dasman Bilingual School's email system and instant messaging technology that protects the employee and the school while benefiting our business.

Applies to: *All employees.*

Key guidelines:

The IT Department at Dasman Bilingual School has established this policy about the acceptable use of School provided electronic messaging systems, including but not limited to email and instant messaging.

Email and instant messaging are important and sensitive business tools. This policy applies to all electronic messages composed, sent or received by any employee or by any person using Dasman Bilingual School provided electronic messaging resources.

The IT Department at Dasman Bilingual School sets forth the following policies but reserves the right to modify them at any time to support our School:

General

- *Dasman Bilingual School provides electronic messaging resources for its employees to assist in conducting its business.*
- *E-mail attachments must not exceed 10 megabytes per attachment.*
- *All messages composed and/or sent using School provided electronic messaging resources must comply with Dasman Bilingual School policies regarding acceptable communication.*
- *Dasman Bilingual School prohibits discrimination based on age, race, gender, sexual orientation or religious or political beliefs. Use of electronic messaging resources to discriminate for any or all these reasons is prohibited.*
- *Upon termination or separation from Dasman Bilingual School, the IT Department will deny all access to electronic messaging resources, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.*
- *Each employee will be assigned a unique email address that is to be used while conducting School business via email.*

- *Employees are not authorized to use instant messaging programs (Yahoo messenger, Hotmail Messenger, Skype …etc), in case it is specially required it will be advised specifically on which instant message program(s) are permissible. Employees who will be authorized to use instant messaging programs will be assigned a unique instant messaging identifier, also known as a buddy name, handle or nickname.*
- *Electronic messages are frequently inadequate in conveying mood and context. Carefully consider how the recipient might interpret a message before composing or sending it.*
- *Any employee who discovers a violation of these policies should immediately notify his Principal, Principals are requested to notify the Human Resources Department and the IT Department.*
- *Any employee in violation of these policies is subject to disciplinary action, including but not necessarily limited to, termination.*

Ownership

- *The email/electronic messaging systems are School property. All messages stored in School provided electronic messaging system(s) or composed, sent, or received by any employee or non-employee are the property of DASMAN BILINGUAL SCHOOL*

Electronic messages are NOT the property of any employee.

- *Dasman Bilingual School reserves the right to intercept, monitor, review and/or disclose all messages composed, sent, or received.*
- *Dasman Bilingual School reserves the right to alter, modify, re-route, or block the delivery of messages as appropriate.*
- *The unique email addresses and/or instant messaging identifiers assigned to an employee are the property of Dasman Bilingual School Employees may use these identifiers only while employed by Dasman Bilingual School.*
- *E-mail massages MUST NOT be deleted nor stored in personal folders.*

Confidentiality

- *Messages sent electronically can be intercepted inside or outside Dasman Bilingual School and as such there should never be an expectation of confidentiality. Do not disclose proprietary or confidential information through email or instant messages.*
- *Electronic messages can never be unconditionally and unequivocally deleted. The remote possibility of discovery always exists. Use caution and judgment in determining whether a message should be delivered electronically versus in person.*
- *Electronic messages are legally discoverable and permissible as evidence in a court of law. Messages should not be composed that you would not want to read out loud in a court of law.*
- *Employees are prohibited from unauthorized transmission of School secrets, confidential information, or privileged communications.*
- *Unauthorized copying and distribution of copyrighted materials is prohibited.*

Security

- *Dasman Bilingual School employs sophisticated anti-virus software. Employees are prohibited from disabling anti-virus software running on School provided computer equipment.*
- *Although Dasman Bilingual School employs anti-virus software, some virus infected messages can enter the school messaging systems. Viruses, "worms" and other malicious code can spread quickly if appropriate precautions are not taken. Follow the precautions discussed below:*
    - *Be suspicious of messages sent by people not known by you.*
    - **Do not open attachments** *unless they were anticipated by you. If you are not sure,* **always verify** *the sender is someone you know and that he or she sent you the email attachment.*
    - *Disable features in electronic messaging programs that automatically preview messages before opening them.*
    - *Do not forward chain letters. Simply delete them.*
- *Dasman Bilingual School considers unsolicited commercial email (spam) a nuisance and a potential security threat. Do not attempt to remove yourself from future delivery of a message that you determine is spam. These "Remove Me" links are often used to verify that you exist.*
- *Internet message boards are a fertile source from which mass junk e-mailers harvest email addresses and email domains. Do not use School provided email addresses when posting to message boards.*

Inappropriate use

- *Email or electronic messaging systems may not be used for transmitting messages containing pornography, profanity, derogatory, defamatory, sexual, racist, harassing, or offensive material.*
- *School provided electronic messaging resources may not be used for the promotion or publication of one's political or religious views, the operation of a business or for any undertaking for personal gain.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*

Implementation	*Annually-August to June*
Review date	*1st June Annually*

No: IT_02

Policy Name: Internet usage and Blogging

Objective:

Provide appropriate guidelines for accessing and utilizing the Internet through Dasman Bilingual School's network.

Applies to: *All employees with authorized access to Internet services.*

Key guidelines:

Internet services are authorized to designated employees by their principal to enhance their job responsibility. The Internet is an excellent tool but also creates security implications that Dasman Bilingual School must guard against. For that reason, employees are granted access only as a means of providing support in fulfilling their job responsibility.

General

- *Internet accounts are approved for designated employees by their immediate Principal to provide tools that assist in their work.*
- *Everyone is responsible for the account issued to him/her.*
- *Organizational use of Internet services must reflect the mission of Dasman Bilingual School and support Dasman Bilingual School goals and objectives.*
- *These services must support legitimate, mission related activities of Dasman Bilingual School and be consistent with prudent operational, security, and privacy considerations.*
- *Dasman Bilingual School has no control over the information or content accessed from the Internet and cannot be held responsible for the content.*
- *Any software or files downloaded via the Internet into Dasman Bilingual School network become the property of Dasman Bilingual School Any such files or software may be used only in ways that are consistent with their licenses or copyrights.*

Inappropriate use

The state of Kuwait with coordination of ISP's (Internet service providers) applies special web filtering tools on the Internet communication.

- *The following uses of School provided Internet access are not permitted:*
    - *Use proxy breakers or any proxy than the one supported by the IT department.*
    - *To access, upload, download, or distribute pornographic or sexually explicit material.*

- *Violate and Kuwait, local, or federal law.*
- *Vandalize or damage the property of any other individual or organization.*
- *To invade or abuse the privacy of others.*
- *Violate copyright or use intellectual material without permission.*
- *To use the network for financial or commercial gain*
- *To degrade or disrupt network performance.*

- *No employee may use School facilities knowingly to download or distribute pirated software or data.*
- *The use of file swapping software on School computers and School networks is prohibited.*
- *No employee may use Dasman Bilingual School Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.*

Blogging

- *Blogging by employees, whether using Dasman Bilingual School's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Dasman Bilingual School's systems to engage in blogging is acceptable, if it is done in a professional and responsible manner, does not otherwise violate Dasman Bilingual School's policy, is not detrimental to Dasman Bilingual School's best interests, and does not interfere with an employee's regular work duties. Blogging from Dasman Bilingual School's systems is also subject to monitoring.*

- *Dasman Bilingual School's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by IT policy when engaged in blogging.*

- *Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Dasman Bilingual School and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Dasman Bilingual School.*

- *Employees may also not attribute personal statements, opinions or beliefs to Dasman Bilingual School when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of Dasman Bilingual School. Employees assume all risk associated with blogging.*

- *Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Dasman Bilingual School's trademarks, logos and*

any other Dasman Bilingual School's intellectual property may also not be used in connection with any blogging activity

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No: IT_03

Policy Name: Password security

Objective:

Provide guidelines in appropriate management of business passwords to maintain adequate security and integrity of all Dasman Bilingual School's business systems.

Applies to: *All employees.*

Key guidelines:

Maintaining security of Dasman Bilingual School. Business applications, other software tools, email systems, and network facilities are critical to providing data integrity and stability of our systems. Passwords are provided to limit access to these School assets on an as needed basis.

- *Dasman Bilingual School provides access to network, electronic mail, and business applications resources to its employees in support of Dasman Bilingual School mission. Passwords are assigned for access to each of these resources to authenticate a user's identity, to protect network users, and to provide security.*
- *It is the responsibility of everyone to protect and to keep private all passwords issued to him/her by Dasman Bilingual School*
- *The IT Department will establish guidelines for issuing new passwords, deleting passwords as required, and allowing employees to change their passwords.*
- *Although Dasman Bilingual School strives to manage a secure computing and networking environment, Dasman Bilingual School cannot guarantee the confidentiality or security of network, or e-mail passwords from unauthorized disclosure.*
- *Employee can change passwords. This helps monitor and manage the importance of protecting passwords in their distribution and use in such a way that reinforces the integrity of users accessing School systems.*
- *A System network Principal must approve any password change requested by a user's supervisor. Confirmation will be sent to user when a password change is completed at the request of a supervisor.*

- *IT Helpdesk Support will handle requests made in one of the following ways:*
    - *Requests may be sent by e-mails from the employee's Principal account.*
    - *The IT Department will delete all passwords of exiting employees upon notification from Human Resources.*

- *System Network administrators and users assume the following responsibilities:*
    - *System Network administrators must protect confidentiality of user's password.*
    - *User must manage passwords according to the Password Guidelines.*
    - *User is responsible for all actions and functions performed by his/her account.*
    - *Suspected password compromise must be reported to Helpdesk Support immediately.*

Password Guidelines

Select a Wise Password

To minimize password guessing:

- *Do not use any part of the account identifier (username, login ID, etc.).*
- *Use 8 or more characters.*
- *Use mixed alpha and numeric characters.*
- *Use two or three short words that are unrelated.*

Keep Your Password Safe

- *Do not tell your password to anyone.*
- *Do not let anyone observe you entering your password.*
- *Do not display your password in your work area or any other highly visible place.*
- *Change your password periodically (every 3 months is recommended). The IT Department may force all the employees to change their passwords periodically.*
- *Do not reuse old passwords.*

Additional Security Practices

- *Ensure your workstation is reasonably secure in your absence from your office. Consider using a password-protected screen saver, logging off or turning off your monitor when you leave the room.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_04

Policy Name: **Software usage**

Objective:

Provide guidelines on appropriate use of software products utilizing School equipment.

Applies to: *All employees.*

Key guidelines:

This policy is intended to ensure that all School employees understand that no computer software may be loaded onto or used on any computer owned or leased by Dasman Bilingual School unless the software is the property of or has been licensed by Dasman Bilingual School

General

- *Software purchased by Dasman Bilingual School or residing on School owned computers is to be used only within the terms of the license agreement for that software title.*
- *Unless otherwise specifically provided for in the license agreement, any duplication of copyrighted software, except for archival purposes is a violation of copyright law and contrary to Dasman Bilingual School* **Software Usage Policy**.
- *To purchase software, users must obtain the approval of their department Principal who will follow the same procedures used for acquiring other School assets.*
- *All approved software will be purchased through the IT Department.*
- *The IT Manager and designated members of the IT Department will be the sole governing body for defining appropriate software titles acceptable for use in Dasman Bilingual School*
- *Under no circumstances will third party software applications be loaded onto School owned computer systems without the knowledge of and approval of the IT Department.*
- *Illegal reproduction of software is subject to civil and criminal penalties, including fines and imprisonment. Any School user, who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances and may include termination of employment.*
- *Dasman Bilingual School does not condone the illegal duplication of software in any form.*

Compliance

- *We will use all software in accordance with its license agreements.*

- *Under no circumstances will software be used on School computing resources except as permitted in Dasman Bilingual School* **Software Usage Policy**.
- *Legitimate software will be provided to all users who need it. School users will not make unauthorized copies of software under any circumstances. Anyone found copying software other than for backup purposes is subject to termination.*
- *Each user of software purchased and licensed by Dasman Bilingual School must acquire and use that software only in accordance with Dasman Bilingual School* **Software Usage Policy** *and the applicable Software License Agreement.*
- *All users acknowledge that software and its documentation are not owned by Dasman Bilingual School or an individual but licensed from the software publisher.*
- *Employees of Dasman Bilingual School are prohibited from giving School acquired software to anyone who does not have a valid software license for that software title. This shall include but is not limited to clients, vendors, colleagues, and fellow employees.*

- *All software used by a School entity for School owned computing devices, or purchased with School funds, will be acquired through the appropriate procedures as stated in Dasman Bilingual School* **Software Usage Policy**.
- *Any user who determines that there may be a misuse of software within the organization will notify the software Manager or department Principal.*

Registration of software

- *Software licensed by Dasman Bilingual School will not be registered in the name of an individual.*
- *When software is delivered, it must first be properly registered with the software publisher via procedures appropriate to that publisher. Software must be registered in the name of Dasman Bilingual School with the job title or department name in which it is used.*
- *After the registration requirements above have been met, the software may be installed in accordance with the policies and procedures of Dasman Bilingual School A copy of the license agreement will be filed and maintained by the IT Department's Systems Administrators.*
- *Once installed, the original installation media should be kept in a safe storage area designated by the IT Department.*
- *Shareware software is copyrighted software that is distributed freely through bulletin boards, online services, and the Internet. Dasman Bilingual School policy is to pay shareware authors the fee they specify for use of their products if the software will be used at Dasman Bilingual School Installation and registration of shareware products will be handled the same way as for commercial software products.*

Software Audit

- *IT will conduct periodic audits of all School owned PCs, including laptops, to insure Dasman Bilingual School is following all software licenses.*
- *Audits will be conducted using an auditing software product.*

- *Software for which there is no supporting registration, license, and/or original installation media will be removed immediately from the user's computer.*
- *During these audits, the software Manager will search for computer viruses and eliminate any that are found.*
- *The full cooperation of all users is required during software audits.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_05

Policy Name: **PC software standards**

Objective:

Provide guidelines for purchasing and installing software on School PC's

Applies to: *All employees.*

Key guidelines:

The purpose for this policy is to explain School software standards and to identify the levels of technical support available to Dasman Bilingual School employees from the IT Department.

Applicability

1. *This policy applies to all employees of Dasman Bilingual School requesting the purchase of new computer software and who desire computing support for that application from the IT technical support team.*
2. *The following software standards have been established to ensure efficient and cost-effective use of School computing assets:*
    - *To help ensure compatibility between applications and releases.*
    - *To provide more effective system administration*
    - *To assist in the computer planning process and enable the realization of long-term goals and the future computing vision.*
    - *To ensure cost effective purchasing*
    - *To enable effective tracking of software licenses*
    - *To provide cost effective end user software training*
    - *To facilitate efficient and effective technical support effort*

Technical Support

- *Software support is provided at several levels and is based on whether the software is Dasman Bilingual School enterprise standard or department specific.*
- *The IT Department will not provide support for evaluation software, personally purchased software, illegal copies of software, screen savers, shareware, and non-network software that is not included in the standard software list.*
- *Software applications determined by IT technical staff to cause computer problems with Dasman Bilingual School standard network software will be removed.*

IT Department's Role in The Purchase of Hardware And Software

- *Assist departments with evaluating new business software solution.*
- *Act as liaison for departments when dealing with computing vendors.*
- *Recommend and evaluate the tasks/jobs/functions to be accomplished via the new software product.*
- *Assist with hardware and system requirements.*
- *Install the software as needed.*
- *Enforce School hardware and software standards.*

Standard PC Equipment and Software List

- *Standard PC hardware and software configurations will be posted on Dasman Bilingual School Intranet web site in the IT Department section.*
- *Contact the Systems Network Administrator/Manager of the IT Department for questions pertaining to School standards.*

Requesting Standard PC Equipment and Software

- *Equipment and software requests that are covered by Dasman Bilingual School PC Equipment and Software Standards List will be provided quickly if appropriate approvals are granted.*

- *The steps that follow outlines the process for purchasing PC equipment and software:*
  1. *Complete the* **PC Equipment and Software Request** *form. Gain approval of the Department Principal*
  2. *Submit request to IT Department's helpdesk.*
  3. *The IT Department will review the order and forward to Purchasing or will contact Requestor for clarification as needed.*
  4. *The IT Department is available for follow-up questions regarding your order as needed.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_6

Policy Name: **Training on Business Applications and Software.**

Objective:

Provide guidelines regarding Dasman Bilingual School IT related Training policy.

Applies to: *All employees.*

Key guidelines:

Dasman Bilingual School encourages the investment of training and education in all levels of our employee base to increase employee skill, performance, and opportunity. The following guidelines will help manage the use of training and education in Dasman Bilingual School

General

- *Training and education requests should be for training that enhances the skills of the employee to do a better job in his/her position or that positions the employee for a new responsibility within Dasman Bilingual School*
- *Dasman Bilingual School IT Department provides in-house training for selected* **key-users** *in each department, an effective train-the-trainers course will be conducted for each* **key-user** *based on his department needs and the department owned business processes.*
- *Key users are selected from user departments and are not only experts in the school's processes, but also possess domain knowledge of their areas in the industry. Key users specialize in parts of the Business application and act as trainers, help-desk resources, educators, advisors, and change agents for end users, end users have only very specific knowledge of the parts of the system they need for their work.*
- *The training for the key-users may cover the School's Business application Specific Modules Training, Email and Internet usage, Basic network & hardware maintenance knowledge, other software tools.*
- *Key-Users training requests must be approved by the employee's Principal.*
- *Department's key-users will be responsible to train the end users on the parts of the system they need for their work.*
- *Principals are encouraged to include in each employee's annual performance plan specific training and education programs that improve the employee's skill and help the organization achieve more success.*

Dasman Bilingual School's E-Learning & Training Materials

- *All employees are eligible for E-learning materials provided by Dasman Bilingual School IT Department.*
- *Selected access to the e-learning materials should be appropriate in developing skills to improve the employee's skills for current responsibility or that positions him/her for future responsibilities agreed upon by management.*
- *Management approval is required for all e-learning material access.*
- *Available training and e-learning materials are posted on Dasman Bilingual School IT Department Intranet.*

.

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_7

Policy Name: **Inventory and equipment**

Objective:

Provide management guidelines for managing the use and security of School inventory and equipment.

Applies to:

Principals

Key guidelines:

PC's, equipment, and supplies are purchased for School employee use and productivity. It is the responsibility of all employees, Managers, and Principals to manage the security of School equipment and supplies to cost effectively manage Dasman Bilingual School expense in these areas.

Allocating equipment to employees

- *Equipment is assigned to employees based upon their job function.*
- *Principals should maintain a list of equipment allocated to each of his/her employees. (See sample Employee Inventory Allocation log)*
- *Specific equipment should be tracked by employee includes, but is not limited to:*
    - *PC's (both desktop and laptop)*
    - *PC peripherals (scanners, printers, modems, etc.)*
    - *Faxes*
    - *Tablets*
    - *Projector remote and Interactive pens*
    - *Cell phones*
    - *Building access keys and access cards*

Employee termination

- *One of the responsibilities of the principal is to collect all allocated equipment issued to an employee who leaves Dasman Bilingual School Maintaining the Employee Inventory Allocation Log makes it a simple process.*
- *Employees not able to return allocated equipment are responsible for reimbursing Dasman Bilingual School for the fair market value of the item.*

Technology assets

- *The IT Department will maintain an accurate inventory of all networked technology assets, laptops, and tangible technology to include the following information:*
    - *Item*
    - *School ID#*
    - *Serial #*
    - *Basic configuration (i.e., HP PC Desktop -1GB RAM, 100GB HD, CD-RW)*
    - *Physical location*
    - *Operating system release level*
    - *Date placed in service.*
    - *Original cost*
- *Technology equipment will be tagged for easy identification.*
- *Periodic inventory audits will be conducted to validate the inventory and to identify maintenance issues needed for employee productivity.*

Samples:

Department Employee Inventory Allocation log

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_8

Policy Name: **PC standards**

Objective:

Provide guidelines for maintaining a standard PC image for Dasman Bilingual School that addresses the needs of School employees.

Applies to:

All employees

Key guidelines:

Dasman Bilingual School will maintain standard configurations of PC's and laptops to enhance employee productivity and supportability of Dasman Bilingual School network.

General

- *The IT Department will establish the standard configuration of PC hardware and software to be run on School PC's and laptops.*
- *Multiple configurations are maintained to provide stronger capabilities for employees that need more PC capabilities for their work. These users are called "Power users" and are determined to need the more capable PCs by their Principal.*
- *On an exception only basis, a PC may be requested that does not meet the standards configuration. To request a non-standard PC, see* **the PC Software Standards** *policy for the Requesting a Variance from the Standard request form.*

Network access

- *All PCs are network enabled to access Dasman Bilingual School network.*
- *It is the employee's responsibility to maintain appropriate security measures when accessing the network as defined in Dasman Bilingual School* **Password Security** *policy.*

PC Support

- *The IT Department will maintain all PC's of Dasman Bilingual School or will direct you to appropriate measures for maintaining your PC.*
- *Standard configurations are defined to assist in providing responsive support and to assist in troubleshooting your issue or problem. Deviations from the standards are not permitted except in appropriately reviewed and approved situations.*
- *For assistance with your PC or peripheral equipment, contact the IT Help Desk.*

Employee training

- *Basic training for new employees on the use of PC's, accessing the network, and using applications software will be conducted by the department's key-users.*

Backup procedures

- *Network data and programs are backed up daily and archived off site in case of emergency.*

Data and software on your PC is <u>NOT</u> backed up. *If you want to protect data and files used on your PC, you should copy the data to the appropriate network server and store it within your personal file folder specifically set up for this purpose. This will ensure your important data is saved and archived daily in our normal backup process.*

- *Large amounts of data (over 50 MB) should be discussed with the IT Department before uploading to a network server.*

Virus software

- *Dasman Bilingual School maintains network virus software that will automatically scan your PC for possible viruses each time you log onto the network.*
- *Downloading or copying data files from external systems and the Internet are prohibited without the IT Department's review and approval to protect the integrity of Dasman Bilingual School network.*

Applications software

- *Standard software is maintained on all PC's and laptops. See the* **PC Software Standards** *policy for more information.*
- *Under no circumstances are additional software programs allowed to be loaded onto a PC without the review and approval of the IT Department. This is a protective measure to avoid network problems due to viruses and incompatibility issues.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_9

Policy Name: **Software and Hardware Requests**

(New, Upgrade, relocation …)

Objective:

Provide management guidelines on the proper steps and requirements for requesting a Software, PC, Laptop, and Hardware….

Applies to:

Principals

Key guidelines:

Guidelines for ordering new technology equipment or making changes to existing equipment are provided to streamline the order process and to assist the IT Department in fulfilling the request.

General

- *Capital equipment items must be budgeted and approved for purchase.*
- *All technology capital requests are reviewed and approved by the IT Department and Accounting Departments for appropriate need even when budgeted in Dasman Bilingual School annual Capital Budget.*
- *Only Department Principals may submit equipment requests.*
- *Published response times for various equipment requests are posted on the IT Department's Intranet site as follows:*

The table below considers appropriate approval is received and the requested equipment's are available in stock or at the local market.

Equipment Type	**Purchase New**	**Install**	**Move within same location**	**Move to Other Location**
PC	*3-5 Days*	*1 Day*	*1 Day*	*2 Days*
Laptop	*7 Days*	*1 Day*	*1 Day*	*2 Days*
Pinter	*3-5 Days*	*1 Day*	*1 Day*	*2 Days*

RAM	*1 Day*	*1 Day*	*-*	*-*
Internal Hard Drive	*1 Day*	*1 Day*	*-*	*-*
External Hard Drive	*1 Day*	*1 Day*	*-*	*-*
CD-ROM	*1 Day*	*1 Day*	*1 Day*	*2 Days*
Monitor	*2 Days*	*1 Day*	*1 Day*	*2 Days*
Mouse	*1 Day*	*-*	*-*	*-*
Camera	*1 Day*	*1 Day*	*-*	*-*
Scanner	*1 Day*	*1 Day*	*-*	*-*
USP Flash	*1 Day*	*1 Day*		
Head set and Microphones	*1 Day*	*-*		
Mouse	*1 Day*	*-*	*-*	*-*
Keyboard	*1 Day*	*-*	*-*	*-*
Printer toners	*1 Day*	*-*	*-*	*-*
New-Upgrade, Software, applications, and operating systems	*Will be advised on the time of the request.*			

- *Lead times should be taken into consideration when ordering new equipment, upgrades, equipment relocations, etc.*
- *The IT Department will maintain a small inventory of standard PC's, Printer Toners, Mouse, Keyboards, and other heavily used equipment to minimize the delay in fulfilling critical orders.*
- *It is the principal's responsibility to provide enough lead time for new orders and change requests in managing his/her department effectively.*

Procedures

1. *Complete the* **Equipment request form** *for the equipment you need.*
2. *Have the Department Principal review and approve the request.*
3. *Submit the request to the IT Helpdesk and Support e-mail for review and*

Follow-up.

4. *The IT Systems and network Support administrators will review the request for appropriateness based upon standards and capital equipment purchasing guidelines of Dasman Bilingual School the IT organization will follow-up in one of the following ways:*
    A. *Forward the request to the Purchasing Department to order the equipment.*
    B. *Fill the order if equipment is available in inventory.*
    C. *Contact the requesting department for clarification.*
    D. *Decline the request and forward the request form along with an explanation back to the originating department.*

Approved equipment

1. *If the equipment exists in inventory, the equipment is prepped as needed and installed for the requesting department.*
2. *If the equipment is ordered through Purchasing, the IT Department will either be notified of receipt at the requesting department, or the equipment will be sent directly to the IT Department for prep, staging, and installation.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_10

Policy Name: **New employee startup/ IT Role**

Objective:

Provide Principals guidelines to use when starting a new employee with Dasman Bilingual School

Applies to:

Principals

Key guidelines:

Getting new employees off to a fast and productive start is important for the employee and for our School and sets the tone of professionalism we strive for.

General

The purpose of the New Employee Startup policy is to help the new employee:

- **The Department Principal will notify IT Department Help Desk of new hire.**
  - *Order list of required software/hardware and other technology equipment.*
  - *Request network setup with assignment of primary network printer.*
  - *Request for Internet access if applicable.*
  - *Request email setup.*
  - *Fingerprint access for Attendance*

The IT department will install and configure all the requested items and will send all details to HR department. Principals can get the details from HR department and can distribute the same to Employee.

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE

Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_11

Policy Name: **Information security**

Objective:

Provide guidelines that protect the data integrity and proprietary nature of Dasman Bilingual School information systems.

Applies to: *All employees.*

Key guidelines:

- *By information security we mean protection of Dasman Bilingual School data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.*
- *The purpose of the information security policy is:*
    - *To establish a School-wide approach to information security.*
    - *To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of School data, applications, networks, and computer systems.*
    - *To define mechanisms that protect the reputation of Dasman Bilingual School and allow Dasman Bilingual School to satisfy its legal and ethical responsibilities regarding its networks' and computer systems' connectivity to worldwide networks.*
    - *To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.*
- *Dasman Bilingual School will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of Dasman Bilingual School data, network and system resources.*
- *Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews will include monitoring access logs and results of intrusion detection software.*
- *The IT Organization must see to it that:*
    - *The information security policy is updated on a regular basis and published as appropriate.*
    - *Appropriate training is provided to data owners, data custodians, network and system administrators, and users.*
    - *Each department must appoint a person responsible for security, incident response, periodic user access reviews, and education of information security policies for the department.*
- *Vulnerability and risk assessment tests of external network connections should be conducted on a regular basis.*
- *Education should be implemented to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data.*

- *Violation of the Information Security Policy may result in disciplinary actions as authorized by Dasman Bilingual School*

Data classification

- *It is essential that all School data be protected. Different types of data require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance.*
- *Dasman Bilingual School classifies data in the following three classes:*
  High Risk - *Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure.*

    - *Data covered by federal and the state of Kuwait or the Data Protection Act, are in this class.*
    - *Payroll, personnel, and financial information are also in this class because of privacy requirements.*
    - *Dasman Bilingual School recognizes that other data may need to be treated as high risk because it would cause severe damage to Dasman Bilingual School if disclosed or modified.*
    - *The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.*

  Confidential – *Data that would not expose Dasman Bilingual School to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.*

  Public - *Information that may be freely disseminated.*

- *All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through Dasman Bilingual School*
    - *Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification level.*
    - *No School owned system or network can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.*
    - *Data custodians are responsible for creating data repositories and data transfer procedures that protect data in the manner appropriate to its classification.*
    - *High risk and confidential data must be encrypted during transmission over insecure channels.*

- *All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.*
- *Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or re-purposed, data must be certified deleted, or disks destroyed consistent with industry best practices for the security level of the data.*

Access control

- *Data must have sufficient granularity to allow the appropriate authorized access.*
- *There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized and addressed appropriately.*
- *Where possible and financially feasible, more than one person must have full rights to any School owned server storing or transmitting high risk data.*
- *Dasman Bilingual School will have a standard policy that applies to user access rights. This will suffice for most instances.*
- *Data owners or custodians may enact more restrictive policies for end-user access to their data.*
- *Access to the network and servers and systems will be achieved by individual and unique logins and will require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.*
- *As stated in the Appropriate Use Policy, users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. All users must secure their username or account, password, and system from unauthorized use.*
- *All users of systems that contain high risk or confidential data must have a strong password, the definition of which will be established and documented by the IT Organization.*

- *Empowered accounts, such as administrator, root, or supervisor accounts, must be changed frequently, consistent with guidelines established by the IT Department.*
- *Passwords must not be placed in emails unless they have been encrypted.*
- *Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.*
- *Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.*
- *Users are responsible for safe handling and storage of all School authentication devices. Authentication tokens (such as a SecureID card) should not be stored with a computer that will be used to access Dasman Bilingual School network or system resources.*
- *If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing unit so that the device can be disabled.*
- *Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon transfer or termination.*

- *Since there could be delays in reporting changes in user responsibilities, periodic user access reviews should be conducted by the unit security person.*
- *Transferred employee access must be reviewed and adjusted as found necessary.*
- *Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.*
- *Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks.*
- *There should be a documented procedure for reviewing system logs.*

Virus prevention

- *The willful introduction of computer viruses or disruptive/destructive programs into Dasman Bilingual School environment is prohibited, and violators may be subject to prosecution.*
- *All desktop systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.*
- *All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that is kept updated according to the vendor's recommendations.*
- *Where feasible, system or network administrators should inform users when a virus has been detected.*
- *Virus scanning logs must be maintained whenever email is centrally scanned for viruses.*

Intrusion detection

- *Intruder detection must be implemented on all servers and workstations containing data classified as high or confidential risk.*
- *Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.*
- *Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled, and alerts should be transmitted to the administrator when a serious security intrusion is detected.*
- *Intrusion tools should be installed where appropriate and checked on a regular basis.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE

Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_12

Policy Name: Remote access

Objective:

Provide guidelines on appropriate use of remote access capabilities to Dasman Bilingual School network, business applications, and systems.

Applies to: *All employees.*

Key guidelines:

- *The purpose of this policy is to define standards for connecting to Dasman Bilingual School network from a remote location outside Dasman Bilingual School*
- *These standards are designed to minimize the potential exposure to Dasman Bilingual School from damages that may result from unauthorized use of Dasman Bilingual School resources. Damages include the loss of sensitive or confidential School data, intellectual property, damage to critical School internal systems, etc.*
- *This policy applies to all Dasman Bilingual School employees, contractors, vendors and agents with a School owned or personally owned computer or workstation used to connect to Dasman Bilingual School network.*
- *This policy applies to remote access connections used to do work on behalf of Dasman Bilingual School including reading or sending email and viewing Intranet web resources.*
- *Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, cable modems, etc.*
- *It is the responsibility of Dasman Bilingual School employees, contractors, vendors, and agents with remote access privileges to Dasman Bilingual School corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Dasman Bilingual School network.*

Remote connection

- *Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong password phrases.*
- *At no time should any School employee provide his/her login or email password to anyone, not even family members.*
- *School employees and contractors with remote access privileges must ensure that their School owned or personal computer or workstation, which is remotely connected to Dasman Bilingual School corporate network, is not connected to any other network at the same time.*
- *Dasman Bilingual School employees and contractors with remote access privileges to Dasman Bilingual School corporate network must not use non School email accounts (i.e., Yahoo, AOL), or other external resources to conduct Dasman Bilingual School business, thereby ensuring that official business is never confused with personal business.*
- *Routers for dedicated ISDN lines configured for access to Dasman Bilingual School network must meet minimum authentication requirements established by the IT Department.*
- *Frame Relay must meet minimum authentication requirements of DLCI standards.*
- *All hosts that are connected to Dasman Bilingual School internal networks via remote access technologies must use the most up-to-date anti-virus software.*
- *Third party connections must comply with requirements defined by the IT Department.*

- *Personal equipment that is used to connect to Dasman Bilingual School networks must meet the requirements of Dasman Bilingual School owned equipment for remote access.*
- *Organizations or individuals who wish to implement non-standard Remote Access solutions to Dasman Bilingual School production network must obtain prior approval from the IT Department.*

Enforcement

- *Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.*
- *The IT Department is responsible for monitoring remote access and addressing inappropriate use of remote access privileges.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE

Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_13

Policy Name: **Service level agreements**

Objective:

Provide guidelines for the IT Organization's commitment in providing Service Level Agreements.

Applies to: *Principals.*

Key guidelines:

- *Service Level Agreements will be maintained between the IT Department of Dasman Bilingual School and its main users and includes data suppliers and output users.*
- *These Service Level Agreements will be reviewed on a regular basis to provide flexibility in the light of changing needs.*

Background

- *The products and services offered by the IT Department need to be clearly defined and agreed upon with the major user departments, particularly funding partners, and larger suppliers of data, in order to moderate potential demand.*
- *Demand for the IT Department's products and services is likely to increase over time and there should be clear agreement over the extent and type of information to be provided and over services to be carried out in respect to supporting the User.*
- *Part of the function of a Service Level Agreement is to manage expectations of both sides of the agreement.*

Activities Supporting Service Level Agreements

- *The IT Department will establish a basis upon which supplied services can be provided that will be agreed upon by its principal and Dasman Bilingual School IT management team.*
- *An approach is taken based upon the relative capacity and other work of the IT Department considered being the best way of defining the basis for a Service Level Agreement.*
- *Within this framework, the IT Department, and its users, will agree on:*
    - *the level of response considered acceptable.*
    - *parameters by which that response is considered unacceptable.*
    - *The kind of response expected by differing parties to the Service Level Agreement which can be defined in terms of products or by the duration of time needed to deliver a product.*
- *The Service Level Agreement will stipulate any limits applicable to the geographical extent of service and the nature of any level of responses, or kinds of products, which are outside the terms of the agreement.*
- *The agreement may stipulate the basis upon which such extra service(s) or product(s) might be made available.*
- *Service Level Agreements will specify any limitations in terms of duration of time to be spent, or kinds of products which will be made available, within such a service.*
- *Service Level Agreements will stipulate timeframes for their review specific to the products and services involved.*
- *When required, the IT Department staff will operate a time-recording system to monitor the apportionment of time to specific areas of work under a Service Level Agreement and will make use of this time record to inform both the recipient of services and the IT Department.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_14

Policy Name: **Transfer of I.T Hardware / Equipment**

Objective:

- *To organize and process the IT related Hardware transfer and create documentation/records.*
- *For efficient distribution of IT Recourses to accommodate User Requests.*
- *To keep track of hardware movements.*

Applies to: *All Employees*

Guidelines:

1- *Inform IT Department of the request through http://desk-sw:8080/, the request will be acknowledged by IT dept.*

2- *Requestor must show the approval from the department Principal.*

3- *Work order number will be created and sent to requestor upon receipt of approved requisition form together with the approximate schedule as per IT's assessment of the request.*

4. *Implementation / execution of request as per scheduled date and time of transfer.*

5. *IT Technical support assigned for the transfer request should send a confirmation email to the requestor once job is done.*

6. *Requestor should reply to confirm if work requested has been completely done copy furnished.*

7. *Work order will be closed by the helpdesk upon receipt of requestor's confirmation of a complete work done as per request, non - receipt of user confirmation in two days will automatically close the work order.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_15

Policy Name: Work Order Request

Objective:

To understand user requirement efficiently.

- *To reduce the coordination time between helpdesk and user.*
- *For efficient distribution of IT Resources to accommodate User Requests.*

Applies to: *All Employees.*

Guidelines:

1. *User must submit the IT related problems and requests at http://desk-sw:8080/, wherein request must contain the following:*
    a. *Description of the problem*
    b. *Screenshot / image of the problem (if possible)*
    c. *Approval from the authorized personnel if the request requires approval otherwise request will not be accepted.*
    d. *Complete details of the requestor such as: Name, Designation, Department, Location, and contact numbers.*

2. *Helpdesk will acknowledge the request by creating and sending the work order number to the requestor and no follow ups will be entertained unless work order has been issued.*

3. *Follow ups should always come with the issued work order number and requestor should not submit multiple requests for one same problem / issue.*

4. *Please note that work order priorities are set by IT Dept.*

5. *A confirmation email to the requestor will be sent once work is done.*

6. *Requestor should reply to confirm if work requested has been completely done.*

7. *Work order will be closed by the helpdesk upon receipt of requestor's confirmation of a complete work done as per request, non - receipt of user confirmation in two days will cancel out or close the work order.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_16

Policy Name: X and Z drive use

Objective: *Employee X and Z drive quota assignment and its usage.*

Applies to: *All Employees.*

Guidelines:

- *Every employee will be provided with a 500mb disk space upon creation of staff's account access.*
- *X drive space may only be used to store files related to work.*
- *Any user must not exceed the assigned disk space, contact IT dept. for any additional disk space required.*
- *IT department will not be responsible for any loss of the data unless saved in X or Z drive.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_17

Policy Name: **Hardware Sticker Labels**

Objective:

- *In order to control and monitor the inventory of IT resources*
- *To track changes in inventory locations due to inventory movement.*
- *Efficiently allocate and conserve IT resources*

Applies to: *All Employees.*

Guidelines:

- *End users are strictly not allowed to remove or change any sticker labels in any of the IT hardware.*
- *System Administrator should be notified via email incases of worn out label for proper replacement*
- *Anyone caught violating this policy will be subject for a disciplinary action set by the management.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*

Review date	*1st June Annually*

No. IT_18

Policy Name: **Data Transfer and Removable Media Policy**

1- USB MEMORY STICKS

Applies to: *All Employees*

Guidelines:

1- These are useful devices as they are of high capacity, small, transfer data quickly and are easily used in machines with compatible connectors. However, they present a high risk. Therefore, special care is required to reduce the risks associated with memory sticks. And however, the usage of these devices must be very rare as users can transfer their data through emails or through the shared and managed folders over the network.

2- Many memory sticks cannot be password protected and may bypass the virus and Malware checking software. Such devices must not be used.

3 Any memory stick used in connection with council equipment, or the network must be on the IT Department approved list and purchased through the approved supplier. These devices have security features that must be used.

3- As a large amount of data can be stored on a memory stick care should be taken over what data is transferred onto such devices. Only the data that is authorized and necessary to be transferred should be saved on to the device. Data that has been deleted can still be retrieved. Formatting the memory stick is the only way to remove data.

4- Due to their small size there is a higher risk of the memory stick being mislaid or lost and a risk of the memory stick being damaged. Therefore, special care is required to physically protect the memory stick and the data. Anyone using a memory stick to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

5- Virus and malware checking software must be used when the memory stick is connected to a machine. Please coordinate with IT Technician at your place and ask him to check the memory stick for you before using it.

6- Memory sticks are not to be used for archiving or storing records as an alternative to other storage equipment.

2- RECORDABLE COMPACT DISKS, DVD'S OR DISKETTES

1- Only data that is authorized and necessary to be transferred should be saved on to the device. The files should be password protected and / or encrypted if they are taken outside of council buildings. Anyone using a CD, DVD, or diskette to transfer data must consider the most appropriate way to transport the media and be able to demonstrate that they took reasonable care to avoid damage or loss.

2- Storage of data on a CD, DVD or diskette is a snapshot of the data at the time it was saved to the media. When using this method to store data, adequate labeling must be undertaken to easily identify the version of the data as well as its content. Appropriate security and storage methods should be applied to the media so that this business asset is protected.

3- Employee-Owned Laptops and other Employee-owned machines:

As today, many workers use their own desktop or laptop system at home and are a source of malware introduction in corporate networks. They also have increasingly more functional smart phones, tablets, flash drives, and other digital devices that connect to corporate networks. The situation isn't that much different from how instant messaging and Skype has spread virally in enterprises and is almost impossible to stamp out.

Although the IT Department still do not encourage the Employee-Owned Laptops and other Employee-owned machines to be used at the school but it is still an option that has formal support from IT, as long as users follow the guidelines and procedures to secure the network and corporate data.

If you need to use your own laptop or machine at work, you have to get the permission of your principal and under your department responsibility.

Before start using your own machine, a special request has to be authorized by your Principal and passed to the IT Manager, special Security, Antivirus, Malware, and other software has to be installed and verified by the IT department before you can start using your machine.

Moreover, your laptop \ owned machine has to go into regular checks and will be scheduled by the IT department when they receive it for preparation and installation.

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_19

Policy Name: Public folder Access

Objective:

Employee access to Network drive "Public Folder"

Applies to:

All Employees.

Guidelines:

- *Every Employee has given read only access to network drive named "Public folder".*
- *Full access given to any specific folder upon approval from Curriculum coordinator.*
- *Employees are not allowed to copy the content of public folder and use for other purposes unless authorized by line manager.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_20

Policy Name: Data Protection and Acceptable use Policy

Objective:

Every employee must be aware of data protection and responsibilities of using ICT systems.

Applies to:

All Employees.

School Policy

New technologies have become integral to the lives of children and young people today, both within schools and in their lives outside school. The internet and other digital

information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should always have an entitlement to safe internet access.

This Acceptable Use Policy is intended to ensure:

- *That staff will be responsible users of communications technologies used for educational and personal use.*
- *That staff are protected from risks in their use of technology and are aware of the potential problems that may arise from misuse of technology.*
- *To ensure that staff understand their data usage rights and responsibilities.*
- *To provide staff with guidance on how they should utilize school systems.*

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognize the value of the use of ICT for enhancing learning and will ensure that the young people receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

Safety for my professional and personal:

- ✓ *I understand that the school will monitor my use of the ICT systems, email, and other digital communications.*
- ✓ *I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, tablets, etc.) out of school.*
- ✓ *I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.*
- ✓ *I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.*
- ✓ *I will immediately report any illegal, inappropriate, or harmful material or incident, I become aware of, to a member of the Senior Leadership team.*
- ✓ *I will be responsible for all activities on my assigned electronic instructional device.*
- ✓ *Also, we can add in that passwords should be changed regularly, and accounts/ devices should not be left open or unattended while on school premises.*
- ✓ *All data on USB's should be password protected or encrypted (In case of theft or loss)*

I will be professional in my communications and actions when using school ICT systems:

- ✓ *I will not access, copy, remove or otherwise alter any other user's files, without their express permission.*
- ✓ *I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.*
- ✓ *I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will only use my personal equipment to record these images if it is password protected.*
- ✓ *I will only use chat and social networking sites in school in accordance with the school's policies.*
- ✓ *I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school into disrepute.*
- ✓ *I will only communicate with young people and parents using official school systems. Any such communication will be professional in tone and manner.*
- ✓ *If the data on any device is breached, I will report it to the Senior Leadership Team.*

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- ✓ *When I use my personal handheld / external devices (iPads/PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.*
- ✓ *I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs.*
- ✓ *I understand the importance of regularly backing up my work.*
- ✓ *I will not try to upload, download, or access any materials which are illegal (child sexual abuse images, racist material, adult pornography) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.*
- ✓ *I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.*
- ✓ *I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.*

- ✓ *I will not disable or cause any damage to school equipment, or the equipment belonging to others.*
- ✓ *I will only transport, hold, disclose or share personal information about myself, or others, as outlined in the School Data Protection Policy. Where personal data is transferred outside the secure school network, it must be encrypted.*
- ✓ *I understand that the data protection policy requires that any staff or young person's data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law, or by school policy, to disclose such information to an appropriate authority.*
- ✓ *I will immediately report any damage or faults involving equipment or software; however, this may have happened.*
- ✓ *I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.*

Staff Name	
Signed	
Date	

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_21

Policy Name: **Backup Policy**

Objective:

Backing up of computer and server data

Applies to:

All Employees.

Guidelines:

- *Every Admin employee will be provided with a department shared drive where you can find a folder with your name and a personal shared folder from server.*
- *Employees are requested to store all department related shared data in the department folder and other office data in your personal shared folder.*
- *Only these network folders will be backup. DBS IT will not backup the entire computer and won't be responsible for any data lose apart from the shared folder.*
- *Automatic data backup will be happening daily.*
- *Server backup is done daily, weekly and monthly.*
- *One copy of monthly data is transferred to head office on barcoded tape drive before 5th of every month.*
- *Tape drive must be submitted to CEO office Manager before 5th of Every month.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_22

Change Management Policy for Dasman IT Department

1. Purpose and Scope

The purpose of this Change Management Policy is to establish a standardized and structured approach to managing changes within the school IT department's technology environment. This policy outlines the procedures, responsibilities, and guidelines to ensure that all changes are effectively planned, assessed, approved, implemented, and reviewed in a controlled manner. This policy applies to all IT systems, applications, hardware, and network infrastructure managed by the school IT department.

2. Objectives

The objectives of this Change Management Policy are as follows:

a. Minimize disruptions to the school's IT services and operations by ensuring that changes are implemented with minimal risks.

b. Enhance communication and collaboration among IT staff and stakeholders throughout the change process.

c. Promote transparency and accountability in managing changes to the IT environment.

d. Provide a clear framework for assessing and prioritizing changes based on their impact and urgency.

3. Change Management Process

3.1 Change Request Submission

Any proposed change to the IT environment must be submitted as a formal change request using the designated Change Request Form. This form should include details such as the nature of the change, the reasons for the change, expected benefits, potential risks, and proposed implementation timeline.

3.2 Change Evaluation and Prioritization

The school IT department will review and assess each change request based on its impact, complexity, and alignment with the school's IT strategy. Changes will be categorized as follows:

a. Standard Changes: Routine changes that follow established procedures and have a low impact.

b. Normal Changes: Changes requiring moderate planning and coordination.

c. Major Changes: High-impact changes requiring thorough planning, testing, and approval.

3.3 Change Approval

Change requests will be evaluated by the Change Advisory Board (CAB), which consists of representatives from IT management, relevant department managers, and key stakeholders. The CAB will review and approve changes based on their potential impact, risks, and benefits. The CAB will convene regularly to assess and approve change requests.

3.4 Change Implementation

Approved changes will undergo detailed planning, testing, and documentation. The school IT department will ensure that necessary resources, expertise, and communication are in place for successful change implementation. Regular updates will be provided to stakeholders during the implementation process.

3.5 Change Review and Documentation

Following the implementation of a change, a post-implementation review will be conducted to evaluate its success and identify any lessons learned. Documentation of the change, including procedures, outcomes, and any required adjustments, will be updated accordingly.

4. Roles and Responsibilities

IT Management: Overall accountability for change management and approval of major changes.

Change Advisory Board (CAB): Review and approve change requests based on their impact and alignment with school objectives.

Change Manager: Responsible for coordinating and overseeing the change management process.

IT Staff: Responsible for planning, testing, implementing, and documenting changes.

Stakeholders: Provide input and feedback during the change process and receive regular updates.

5. Communication and Training

Regular communication will be maintained with stakeholders regarding upcoming changes, potential disruptions, and outcomes. Training will be provided to IT staff on changing management procedures, tools, and best practices.

6. Compliance and Enforcement

Non-compliance with this Change Management Policy may result in delays or refusal of change implementation. Repeating non-compliance may lead to disciplinary actions.

7. Policy Review

This Change Management Policy will be reviewed annually to ensure its effectiveness, relevance, and alignment with the school's IT objectives.

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_23

Log Management Policy for Dasman IT Department

1. Purpose and Scope

The purpose of this Log Management Policy is to establish a standardized and secure approach for collecting, storing, monitoring, and analyzing logs generated by various servers within the School IT Department's network. This policy outlines the procedures, responsibilities, and guidelines to ensure the effective management of logs in a centralized system.

2. Objectives

The objectives of this Log Management Policy are as follows:

a. Ensure the availability, integrity, and confidentiality of logs generated by IT systems and servers.

b. Facilitate the timely detection, analysis, and response to security incidents and anomalies.

c. Enhance compliance with regulatory requirements by maintaining proper log records.

d. Streamline log management processes through centralized collection, storage, and analysis.

3. Log Collection and Centralization

3.1 Log Sources

All servers within the School IT Department's network, including application servers, network devices, and security appliances, shall be configured to send their logs to a centralized log management system.

3.2 Centralized Log Management System

A dedicated system or platform will be established for the collection, storage, and analysis of logs. This system will be responsible for receiving logs from all relevant sources, organizing them into a structured format, and securely storing them for the designated retention period. Currently we are doing it per server but planning to have a centralized System.

4. Log Retention and Storage

4.1 Retention Period

Logs will be retained for a specified period based on legal and regulatory requirements, as well as the School IT Department's internal policies. The retention period may vary depending on the type of log data. For basic logs will retain for 6 months

4.2 Secure Storage

Log data will be stored in a secure and tamper-evident manner to prevent unauthorized access, alteration, or deletion. Access controls, encryption, and regular backups will be implemented to ensure the integrity and availability of log records.

5. Log Monitoring and Analysis

5.1 Real-time Monitoring

The centralized log management system will provide real-time monitoring capabilities, enabling IT staff to promptly detect and respond to security incidents and abnormal system behavior.

5.2 Regular Analysis

Logs will be regularly analyzed to identify patterns, trends, and potential security risks. The analysis may involve the use of automated tools, intrusion detection systems, and manual review by qualified personnel.

6. Incident Response

In the event of a security incident or breach, logs will play a crucial role in investigating and mitigating the incident. The School IT Department will have documented incident response procedures that outline the steps to be taken based on the severity of the incident.

7. Access and Audit Controls

Access to log data and the centralized log management system will be restricted to authorized personnel only. Audit logs of access and changes to log data will be maintained to ensure accountability and traceability.

8. Training and Awareness

IT staff responsible for log management will receive appropriate training on log collection, analysis, and incident response procedures. Regular awareness campaigns will be conducted to promote the importance of effective log management across the department.

9. Compliance and Enforcement

Non-compliance with this Log Management Policy may result in disciplinary actions. Regular audits and assessments will be conducted to ensure adherence to the policy.

10. Policy Review

This Log Management Policy will be reviewed annually to ensure its effectiveness, relevance, and alignment with the School IT Department's objectives and changing technology landscape.

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

Patch Management Policy for Dasman School IT Department

1. Purpose and Scope

The purpose of this Patch Management Policy is to establish a systematic and secure approach to identifying, testing, deploying, and monitoring software patches and updates within the School IT Department's network. This policy outlines the procedures, responsibilities, and guidelines to ensure the timely and efficient management of patches while minimizing potential risks.

2. Objectives

The objectives of this Patch Management Policy are as follows:

a. Enhance the security and stability of the school's IT infrastructure by applying timely software patches and updates.

b. Minimize vulnerabilities and potential threats by implementing a consistent and organized patch management process.

c. Maintain compliance with software vendors' recommendations and regulatory requirements related to patching.

d. Reduce downtime and disruptions caused by unpatched software vulnerabilities.

3. Patch Management Process

3.1 Patch Identification

The School IT Department will continuously monitor vendors' websites, security advisories, and relevant industry sources to identify available software patches and updates. Patches will be categorized based on severity, impact, and applicability to the school's IT environment.

3.2 Patch Testing

Before deploying patches to production systems, they will undergo thorough testing in a controlled environment to ensure compatibility and minimize potential conflicts with existing applications and configurations.

3.3 Patch Deployment

Once patches have been tested and approved, they will be deployed to the production environment following a scheduled maintenance window. Critical and security patches may be deployed immediately, while less critical patches can be included in regular update cycles.

3.4 Patch Monitoring

After patch deployment, IT staff will monitor systems for any adverse effects or anomalies resulting from the patching process. This includes observing performance, functionality, and user experience.

4. Critical and Security Patches

4.1 Critical Patches

Critical patches, which address severe vulnerabilities posing an immediate threat, will be given the highest priority and deployed as soon as possible after testing.

4.2 Security Patches

Security patches addressing significant vulnerabilities will be deployed promptly within a defined timeframe after successful testing.

5. Non-Critical Patches

Non-critical patches, which provide feature enhancements or bug fixes, will be included in regular update cycles to minimize potential disruption to operations.

6. Rollback and Contingency Plan

If a deployed patch causes significant issues or disruptions, a rollback plan will be in place to revert to the previous software version. A contingency plan will outline steps to address unexpected consequences and restore normal operations.

7. End-of-Life Software

Software that reaches its end-of-life (EOL) or end-of-support (EOS) will be phased out in a timely manner, and systems running such software will be upgraded or replaced to maintain security and compliance.

8. User Awareness and Communication

Regular communication will be maintained with users, stakeholders, and relevant departments to inform them about upcoming patch deployments, expected impacts, and the benefits of patch management.

9. Compliance and Enforcement

Non-compliance with this Patch Management Policy may lead to disruptions, security vulnerabilities, or other risks. Regular audits and assessments will be conducted to ensure adherence to the policy.

10. Policy Review

This Patch Management Policy will be reviewed annually to ensure its effectiveness, relevance, and alignment with the School IT Department's objectives and changing technology landscape.

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*

Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_24

HANDLING SENSITIVE INFORMATION POLICY

DEFINITIONS:

Data or Privacy Breach

An incident in which sensitive or highly sensitive data has potentially been viewed, stolen, or used, or altered by an individual unauthorized to do so.

Compromised Data

The data exposed in a data or privacy breach.

Sensitive Data

Data, information, or intellectual property in which the school has a legal interest or ownership right and is intended for only limited dissemination. Such materials, if compromised, could be expected to cause minor, short-term harm or embarrassment to the institution and/or specific individuals.

Electronic Data

Data that are stored, transmitted, or read in an electronic format such as a file on a drive or device, information in a database, or unstructured formats such as email.

Cloud Service

Refers to remotely hosted computing resources, applications, and data storage which is operated by a third party.

Electronic Data

Refers to the practice of placing a non-transient copy of electronic data on any device or cloud service,

Purpose/Reason for Policy:

In conjunction with the principles outlined in the Dasman bilingual data protection policy, the purpose of Dasman Policy on Handling Sensitive Electronic Information is to establish a framework for classifying and handling electronic data which will.

- *Ensure the schools regulatory, legal, contractual and privacy obligations with respect to privacy and data security are met.*

- *Ensure the schools proprietary data and information is kept confidential to the institution as required.*

Scope of this Policy:

This Policy applies to all administrators, faculty, staff, who as part of their role and responsibilities, may create, use, process, store, transfer, administer, and/or destroy data electronically. The Policy applies to all electronic data in which Dasman school has a legal interest or ownership right, regardless of where such data are stored.

Policy Statement:

Administrators, faculty, staff of Dasman bilingual must use care when handling sensitive electronic information and must abide by the following as related to the storage, transmission, access, and disposal of electronic data. The IT department will provide the necessary technology support for the implementation of this Policy. The IT department may also deploy automated scanning tools intended to detect and/or prevent data breaches in real time.

Storage:

Sensitive electronic information may only be stored.

- *On servers which are managed directly by Dasman Bilingual Technology Department*
- *On computers and laptops that have been encrypted using IT-approved full-disk encryption software*
- *On IT-approved cloud services which require Dasman credentials to access.*
- *In any other location approved by IT*

Sensitive electronic information may not be stored.

- *On unencrypted computers, laptops, devices, or portable storage.*

- *With cloud storage services where credentials are not managed by Dasman IT.*
- *In any other location not approved by IT.*

Please note that accessing email from a mobile device will sync a portion of your mail to that device. If you are expected to send or receive sensitive via email, you must ensure that device is password protected.

Reporting

- *In the event of an actual or suspected data breach, the user must inform the Dasman IT department.*

- *If the breach involved the physical theft of a device, the theft must be reported Administration and IT.*

Related Policies, Procedures & Guidelines

- *Data Protection Policy*

I have read and understand the above and agree to take precautions in order protect sensitive data (both in and out of school when carrying out communications related to the school) within these guidelines.

Staff Name	
Signed	
Date	

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Dasman Internal Administration*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Bitu Skaria*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

*No. IT_***25 Guidelines for Online Learning Videos**

1. *Teacher in video must be professionally dressed.*
2. *The purpose of the video is to maximize student engagement and to promote active learning.*
3. *Videos created with an eye for strong pedagogical choices.*
4. *Choose appropriate instructional strategies and pair them with an effective media format.*
5. *Video should be of 8 – 10 minutes duration.*
6. *Be clear and explicit regarding the learning objectives.*
7. *Focus of acquisition and application of skills*
8. *State what preparations or support material students will need, and manipulative required.*
9. *Decide which visuals will be most effective.*
10. *Create a coherent narrative path.*
11. *Information must be factually correct.*
12. *Videos should have a personal feel for it to be more engaging.*
13. *Mix spurts of discussion, collaboration, videos and audio clips, hands-on exercises and supporting text notes*
14. *Focus on active learning and student engagement.*
15. *Make references to corresponding pages in the textbook and activity books.*
16. *Have multiple worked examples as text for effective learning and comparison.*
17. *Embrace multi-media Assignments.*
18. *Games need to be interactive – immediate feedback.*
19. *Indicate what the assessment exercise will be with due dates.*
20. *Time frame for entire lesson should be 45 minutes.*
21. *Instruct how students can request additional assistance/queries.*
22. *Video recordings must be of an acceptable quality (visuals and sound)*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Local legislation*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Waseem Bacus & Fay Khan*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_26 **Disclosure and Transparency of Information**

Instances of malpractice or impropriety which would be in the public interest to disclose might include:

- *financial malpractice or impropriety or fraud.*
- *failure to comply with a legal obligation or with the regulations of the school.*
- *dangers to health and safety or the environment.*
- *academic or professional malpractice.*
- *miscarriage of justice.*
- *improper conduct or unethical behavior.*
- *serious conflict of interest without disclosure.*
- *criminal activity (not covered by the above).*
- *attempts to conceal any of the above.*

School Financial Transparency *The transparency of School Finances directs the Board to post financial information online for free school community access.*

Required Financial Information

- *Annual Budgets*
- *Financial Audit*
- *Quarterly Financial Statements*
- *Salary Schedules or Policies*
- *Investment Performance Reports or Statements*

Prior two budget years' financial information shall be maintained on-line until the end of the current budget year.

Protection

The policy is designed to offer protection to individuals who make a disclosure provided that the disclosure is made:

- *in good faith.*

- *in the reasonable belief that the disclosure is substantially true and tends to show malpractice.*
- *without a view to personal gain.*
- *to an appropriate person.*

The school will handle disclosures confidentially, protecting the identity of the discloser whenever possible, except when disclosure is necessary for a thorough investigation or legal reasons. While anonymity is guaranteed to the extent possible, the school cannot prevent all speculation. The school will protect the discloser from retaliation. However, the policy discourages anonymous allegations.

Concerns expressed anonymously will be considered at the discretion of the school considering the following:

- *the seriousness of the issues raised.*
- *the credibility of the concern.*
- *the likelihood of confirming the allegation from attributable sources.*
- *prospect of being able to conduct a thorough investigation.*
- *fairness to any individual mentioned in the allegation.*

If an investigation finds an allegation unsubstantiated but made in good faith and with reasonable belief in its truth, no action will be taken against the person who made the allegation. However, individuals making malicious disclosures, misusing the policy, or inappropriately reporting concerns to external parties before following internal procedures may face disciplinary action.

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Local legislation*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Samar Dizmen & Fay Khan*
Implementation	*Annually-August to June*
Review date	*1st June Annually*

No. IT_27 **CYBER SAFETY & ANTI BULLYING POLICY**

This policy is part of a series of interrelated policies for the safety and wellbeing of students, parents, and staff.

This policy should be read in conjunction with the following policies:

- *Sensitive Data Policy*
- *Data Protection Policy*
- *Acceptable use Policy*

PURPOSE OF POLICY

- *Promote safe and responsible use of digital platforms and encourage positive interaction within the digital community.*
- *Educate students and parents on appropriate online behavior for educational purposes.*
- *Set expectations for student behavior when using digital technology, in line with school policies and procedures.*
- *Implement policies and procedures to prevent and address cyberbullying within the school community.*

AT DBS, STUDENTS ARE TAUGHT TO:

- *Understand how to use technology safely and be aware of the risks and consequences of misuse.*
- *Know how to respond if they or someone they know is being cyberbullied.*
- *Report any issues related to cyberbullying and seek support from the school and parents to address the problem.*

STATEMENT OF POSITION:

- *DBS ensures cyber-safety through core values, including rigorous cyber-safety practices and educational programs.*
- *The school provides appropriate use agreements for both staff and students, emphasizing responsibilities and obligations for safe use of ICT equipment.*
- *The goal is to create and maintain a cyber-safe culture aligned with the school's values and legal requirements.*
- *Students will receive an acceptable use policy, and after signed consent, they can access school ICT devices, with clear consequences for breaches related to cyber-safety and bullying.*

CYBER SAFETY

- *Cyber safety covers technologies such as the Internet, mobile phones, and wireless devices.*
- *With advanced and affordable communication technologies, it is important to educate children and young people about the benefits and risks.*
- *It provides safeguards and awareness to help users manage their online experiences.*
- *Promotes the appropriate and responsible use of all technologies.*

GOOD HABITS:

- *Cyber-safety relies on responsible ICT use by both staff and students, supported by education and clear policies.*
- *Effective implementation of cyber-safety policies in administration and curriculum, including secure network design, is essential.*
- *Safe and secure broadband usage, along with proper content filtering management, is crucial for cyber-safety.*

AT DBS:

- *The school takes all reasonable steps to protect students online but acknowledges the risk of exposure to undesirable content.*
- *Students are regularly reminded to:*
- *Turn off the screen if they encounter inappropriate material.*
- *Report the issue immediately to a teacher or supervising adult, who will document the details.*
- *Refrain from describing or encouraging others to access the site.*
- *If unsuitable content is encountered on school platforms, both learners and teachers must contact the IT manager immediately.*

STEPS WE TAKE TO PROTECT OUR LEARNERS AT DBS

- *Filtered Service: Internet access is provided through a filtered service on-site.*
- *Supervision: All children's internet use is supervised by a teacher, as no filtering service is 100% effective.*
- *Planned Activities: Internet use is planned and purpose-driven, not for aimless surfing. Children use the internet in response to specific class needs or questions.*
- *Websites: Teachers preview and revisit websites to ensure they meet curriculum needs and are age appropriate. Britannica search engine is used, and teachers guide students in using safe search terms.*
- *Internet Safety Rules: Children are taught Internet Safety Rules and encouraged to discuss how to handle encountering inappropriate content.*

DBS School Website:

- *Children are only referred to by their first names.*
- *No images of children will be labeled with names or shown close-up.*
- *Personal details like addresses or phone numbers are not shared on the website.*

STAFF PERSONAL SOCIAL MEDIA RESTRICTIONS

- *Parental consent for filming students is strictly for the school's official use on approved social media and publications.*
- *Teachers are prohibited from sharing videos featuring students' faces on personal social media or with people outside the school.*
- *Such unauthorized sharing breaches confidentiality and undermines parental trust.*

- *Teachers may share innovative teaching practices or classroom setups if students' faces are not visible.*
- *All content involving students must follow the school's guidelines and be used only for official school representation.*

SAFETY POINTS FOR STUDENTS TO CONSIDER

- *Use only your own login credentials to access school computers, the internet, and other tech equipment.*
- *Do not view, alter, or delete other people's work/files.*
- *Do not modify or delete any settings on school devices.*
- *Ask for permission before accessing any website unless already approved by a teacher.*
- *Only send emails that have been approved and reviewed by a teacher, ensuring the messages are polite and appropriate.*
- *Never share your personal information (name, address, phone number) or arrange meetings with anyone via email.*
- *Do not share others' personal information.*
- *Do not enter Internet chat rooms while using school computers.*
- *If you encounter something inappropriate or receive unpleasant messages, turn off the screen and immediately inform a teacher.*

CYBER BULLYING

- *Cyberbullying involves bullying through communication technology like text messages, emails, or websites.*
- *Common forms include:*
- *Sending threatening or abusive text messages or emails, either personally or anonymously.*
- *Posting insulting comments about someone on websites or social networking sites.*
- *Sharing derogatory or embarrassing videos of someone via mobile phones or email.*
- *Cyberbullying, using any form of technology to bully others, will not be tolerated.*

INFORMATION FOR PARENTS:

- *At DBS, cyberbullying is taken as seriously as other types of bullying and is addressed individually.*
- *Consequences may include:*
- *Verbal warnings.*
- *Parental discussions.*
- *More serious actions for severe cases.*
- *Cyberbullying can occur anonymously, 24/7 and is harder to detect as it leaves no physical scars.*

- *It can be highly intrusive and cause severe emotional harm, especially to young people.*
- *Young people often use acronyms in communication (e.g., POS, TUL), which can be difficult for adults to understand, increasing the challenge of identifying threats.*
- *Incidents can be reported to the division principals.*

POINTS FOR PARENTS TO CONSIDER AT HOME:

It is important to promote phone and Internet Safety in the home, and to monitor Internet use.

Tips to Promote Internet Safety at Home:

- *Discuss the fact that there are websites which are unsuitable.*
- *Discuss how children should respond to unsuitable materials or requests.*
- *Remind children never to give out personal information on the Internet.*
- *Remind children that people online may not be who they say they are.*
- *Be vigilant. Ensure that children do not arrange to meet someone they meet online.*
- *Be aware that children may be using the Internet in places other than in their own home or at school.*
- *Be aware of the safety issues regarding mobile phones.*
- *Encourage children to talk about how they use mobile phones.*
- *Remind children not to give mobile numbers to strangers and people they do not know very well.*
- *Talk about responsible use of the internet and technology.*

Monitor Internet use:

- *Keep the computer in a communal area of the home.*
- *Monitor online time and be aware of excessive hours spent on the Internet.*
- *Take an interest in what children are doing.*
- *Discuss with the children what they are seeing and using on the Internet.*
- *Advise children to take care and to use the Internet in a sensible and responsible manner.*
- *Check internet history log. This will tell you what websites your child is frequenting.*

FILTERING FOR THE HOME COMPUTER:

- *Parents may wish to invest in security software for their children's computers.*
- *Some of this software works by monitoring all Internet activity for trigger words.*
- *There are many types of security software available, the following are only a few.*

  Examples include:

  - *Net Nanny*

- *Cyber Patrol*
- *Surf watch*

INFORMATION FOR STUDENTS:

If you are being bullied:

- *Remember, bullying is never your fault. It can be stopped, and it can usually be traced.*
- *Don't ignore the bullying. Tell someone you trust, such as a teacher or parent.*
- *Try to keep calm; if you are frightened, try to show it as little as possible.*
- *Don "get angry, it will only make the person bullying you more likely to continue.*

ON THE INTERNET:

- *Don't share personal details online such as your address, school, or email, as it can help someone harm you.*
- *Save evidence of bullying, including emails, text messages, or images, to show to parents, teachers, or authorities.*
- *Note the time, date, and details about the sender of any bullying messages or images.*
- *Seek online advice on how to handle cyberbullying, such as from resources like www.kidscape.org and www.wiredsafety.org.*

HANDLING CYBER-SAFETY COMPLAINTS:

- *Prompt action is required if a complaint is made regarding cyberbullying or internet misuse.*
- *The facts of the case will need to be established, including whether the issue occurred outside of school or through home internet use.*
- *Transgressions by students will be handled according to the school's behavior policy.*
- *In serious situations, the police must be contacted.*
- *Complaints about internet misuse will be dealt with by senior staff.*
- *Complaints about staff misuse should be referred to the division Principal.*
- *Complaints about a child protection nature will be handled according to the school's child protection procedures.*

DOCUMENT CONTROL

COMPLIANCE	
Compliant with	*Local legislation, CIS and NEASC*

AUDIENCE	
Internal	*All staff in Dasman Bilingual School*

VERSION CONTROL	
Author	*Samar Dizmen, Waseem Bacus & Fay Khan*
Implementation	*Annually-August to June*
Review date	*1st June Annually*