DATA PROTECTION POLICY
AY 2024-25

HABITAT SCHOOL
AL JURF, AJMAN

Creation Date: 20/05/2014

Last Amendment Date: March2024

Next Review Date: April 2025

Policy Committee Members

- CEO- Academic division
- Dean Academics
- Principal
- Administrative Officer
- Software Analyst- Corporate
- School IT Administrator
- Head of the Counseling department
- Head of Computer Department
- HR Coordinator

DATA PROTECTION POLICY

Introduction

Habitat School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered to enable the school to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

This policy is intended to ensure that personal information is dealt with correctly and securely. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines. It is the responsibility of all members of the school community to take care when handling, using, or transferring personal data, that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Data breaches can have serious effects on individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the School head. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to the relevant school policy which brings together the statutory requirements contained in relevant data protection legislation and relevant regulations and guidance

Scope & Objective

This is a policy that applies to all Users and all Systems.

“Users” are everyone who has access to any of the school's IT systems. This includes permanent employees and also temporary employees, parents, students, contractors, agencies, consultants, suppliers, customers and business partners. “Systems” means all IT equipment that connects to the School network or access school applications. This includes but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third-party networking services, telephone handsets, video conferencing systems, and all similar items commonly understood to be covered by this term.

POLICY

All student, employee, and Habitat Schools Data is the property of the Habitat School.

If data on the school's systems is classified as confidential this should be indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorized access to confidential information.

Users are expected to exercise reasonable personal judgment when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise transfer to a non-school system any information that is designated as confidential, or that they should reasonably regard as being confidential to the school, except where explicitly authorized to do so in the performance of their regular duties.

Habitat Schools Data should not be shared with a third party, including parents or community residents unless authorized to do so in the performance of their regular duties.

Users who are supplied with computer equipment by the school are responsible for the safety and care of that equipment, and the security of software and data stored on other school systems that they can access remotely using it.

Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

What is Personal Information or Data?

The school and its employees will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal information or data is defined as data that relates to a living individual who can be identified from that data, or other information held.

This will include

- Personal information about members of the school community – including students/pupils, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular/academic data e.g. class lists, student/pupil progress records, reports, references
- Professional records e.g. employment history, taxation and insurance records, appraisal records and references any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

SECURE STORAGE OF AND ACCESS TO DATA

The school ensures that systems are set up so that the existence of protected files is hidden from unauthorized users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords made up of a combination of simpler words and must ensure all passwords comply with the school's safe password policy. Users must keep passwords secure, never share them with anyone and not allow others to access their accounts.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data (desktops and laptops) should be secured with a lock-on-idle policy active after at most 5 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on school equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school personal data.

Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

All paper-based personal data must be held in lockable storage, whether on or offsite. Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into the school systems by whatever means and must report any actual or suspected malware infection immediately.

BACKUP AND DISASTER RECOVERY POLICY

Habitat School critical servers are backed up automatically by Imperious at regular intervals. IT personnel regularly monitor and verify the backup process and files. In case of a server failure, a new server can replace the existing one by restoring the Backup on the new server. The verification and monitoring process is in place and quarterly backups are restored and verified.

A centralized antivirus system is functional at Habitat School to tackle the viruses and Trojans. Gateway firewalls are also up and running to secure the internet and email communication. The firewall works to prevent users from watching unintended materials, torrent downloading etc. As per the levels set by the administration, some of the users have rights over some areas of the internet for educational and research purposes.

SECURE TRANSFER OF DATA AND ACCESS OUT OF SCHOOL

The school recognizes that personal data may be accessed by users out of school or transferred to other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorized premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorized user from outside the organization’s premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.

BACKUP AND DISASTER RECOVERY POLICY

Habitat School critical servers are backed up automatically by Imperis at regular intervals. IT personnel regularly monitor and verify the backup process and files. In case of a server failure, a new server can replace the existing one by restoring the Backup on the new server. The verification and monitoring process is in place and quarterly backups are restored and verified.

A centralized antivirus system is functional at Habitat School to tackle the viruses and Trojans. Gateway firewalls are also up and running to secure the internet and email communication. The firewall works to prevent users from watching unintended materials, torrent downloading etc. As per the levels set by the administration some of the users have the rights over some areas of the internet for educational and research purposes

SECURE TRANSFER OF DATA AND ACCESS OUT OF SCHOOL

The school recognizes that personal data may be accessed by users out of school or transferred to other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorized premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorized user from outside the organization's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.

DISPOSAL OF DATA

The disposal of personal data, in either paper or electronic form, is conducted in a way that makes reconstruction highly unlikely. Electronic files are securely disposed of, and other media must be shredded, incinerated, or otherwise disintegrated. A Destruction Log is kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method, and authorization.

DATA BREACHES

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. The school has a policy for reporting, logging, managing, and recovering from information risk incidents, which establishes a:

- "responsible person" for each incident
- communications plan, including escalation procedure
- plan of action for rapid resolution
- plan of action for non-recurrence and further awareness-raising

Everyone in the school has the responsibility of handling protected or sensitive data safely and securely.

TRAINING & AWARENESS

All staff should receive data handling awareness/data protection training and will be made aware of their responsibilities. This should be undertaken regularly. You can do this through

- Induction training for new staff
- Staff meetings/briefings/training sessions
- Day-to-day support and guidance from System Controllers

ENFORCEMENT

It is the responsibility of the end user to ensure the enforcement of the policies above. All concerns, questions, and suspected, or known breaches shall be immediately reported to the Data Protection Officer.

Data protection Officer and Information asset owner of Habitat School, Al Jurf: **Mr. Boney R**

REVIEW

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 1 year. The Principal, or nominated representative will undertake the policy review.

CONTACT

If you have any queries or concerns regarding this policy then please contact itsupport@ajm.habitatschool.org