The Data Protection Policy

Updated on January 2021

Reviewed and approved by:
OSG TEAM

AL AMEER ENGLISH SCHOOL AJMAN

DATA PROTECTION POLICY

The COVID-19 pandemic has brought unprecedented challenges to our safety, health and education. In the process of online learning, Personal data are produced through the interaction between students/teachers and tools or platforms. Personal data and privacy are the tranquility of the private life of a natural person, and the private space, private activities, and private information that one is unwilling to be known to others. This policy sets out how we seek to protect personal data and ensure that staff understand the policy to ensure that the Data Protection Officer (DPO) be notified regarding any new data processing activities or data incidents to ensure that relevant compliance steps are adopted.

Top cyber security threats for schools includes:

Cyber security policy exists to ensure that all staff, students and third parties follow certain basic rules with regard to internet use and use of IT in general. Its aim is to prevent students or staff coming to harm as a result of others accessing intolerant, extremist or hateful web sites.

The school ensures,

- Cyber security for all student and staff.
- Critical use of technology delivered to the appropriate user groups.
- Users understand their IT security.
- A culture of security awareness and persistent maintenance program to ensure continual awareness is built.
- Responsible, safe and intelligent use of Information Technology.
- Sensitive information is protected from unauthorized disclosure.
- Integrity is maintained through accuracy, completeness, consistence and timeliness of data.
- Safeguarding necessary resources and associated capability.
- Cyber bullying is totally curbed.
- Investigation into incidents of cyber bullying.
- Parental and peer support for cyber safety.

The School should:

- Dent in confidentiality of records will result in suspension or dismissal/ termination for a term /year/permanently.
- Improper use or display of information technology in school will initiate serious disciplinary action.
- Backup data on a server that is not accessible by the rest of the network and therefore not vulnerable to the ransom ware encryption agent.
- Train end users in what data they are responsible for protecting and how to handle data.
- Training staff to detect and report suspicious e-mails is the first and most important step to deal with phishing.

- Cyber bullying will be dealt with severe disciplinary actions.

DATA SECURITY

The data within the school's systems and networks may be the most valuable asset. In establishing the physical security measures and user access framework, the school should also pay attention to the protection of data. In general, data security requires data files to be properly created, labeled, stored and backed up. The data should also be protected from attack.

Some of the common IT security controls for data protection we follow include:

- The IT equipment, such as servers, workstations, backups, recovery diskettes, original software packages etc. are kept in a safe place against unauthorized access.
- Access controls are defined for and assigned to specific data files, resources and other system rights. Role based access control is followed as users are allowed to access only specific information
- Password complexity, minimum and maximum length is set for e learning platforms. Parameters like number of invalid password attempts, lockout duration and unlocking procedures are also defined
- The School endeavor to have all access points located in physically secure locations, and access to wireless management is limited and have strong authentication.
- To prevent unauthorized access faculty, staff and students must use strong passwords. All default passwords are changed. On occasion, when guest access is required, the guest network is enabled and the password is given out. The guest password is changed regularly. Passwords are regularly changed to ensure access is gained only by authorized users.
- The access to wireless management is limited to the Systems Administrator or the designate, using an account with a strong password
- Automatic updates are configured to keep access point software patched.
- The network administrator checks for rogue devices monthly, and unidentified devices are denied access.
- Wireless access point, firewall rules and application rules, as well as an encrypted password for the SSID are configured to help prevent and minimize virus and malware programs from being installed, or gaining access to sensitive, confidential or financial data.
- Ensure network permissions are set correctly so users can only access the data and files they require to carry out their duties. All network users have individual logins. Don't share usernames or passwords. Personal data should not be sent from staff/top admin personal accounts.
- All backup and recovery procedures are well documented, tested and properly implemented. System administrator is responsible for data backup and recovery. Data backup should be performed and monitored at regular intervals. Periodically, it is advised to perform a trial restoration to verify that files could be properly backed up

- Security logging is followed to detect the occurrence of threats. Monitoring and review of the school‘s online platform and networks on a periodic basis for IT security incidents
- School provides well-conceived and committed security training programs, which enable users to be better prepared to avoid incidents.

DATA PROTECTION OFFICER

The Data Protection Officer’s responsibilities:

- Provide proper training on Data Protection Policies for staffs and Students
- Manage internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits
- First point of contact for any data concerns by parents, authorities and school top admin and responsible for answering any data related queries
- Review all data protection procedures and policies on a regular basis
- Ensure that third parties or service providers adhere to data protection and privacy policies of school.
- Ensure all IT systems, services, software and equipment meet acceptable security standards
- Ensure checking and scanning security hardware and software is carried out regularly to ensure it is functioning properly

DATA RETENTION PERIOD AND DATA DELETION

Records that reached the end of minimum retention period are archived or deleted. Record that are no longer required are reviewed and deleted in each academic year. Paper records ,CDs, audio video tapes, hard disks containing personal information should be made unreadable or unreconstructable

SUBJECT ACCESS REQUEST

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. If you would like to make a subject access request, you should refer that request immediately to the DPO.

DATA BREACHES

- Staffs should immediately report any possible data breaches to top management and DPO .
- Reporting breaches Data breaches must be reported to the ICO within 72 hours.
- If the breach is sufficiently serious to warrant notification to the public, the breach must be reported without undue delay.
- If there is a high risk to the rights and freedoms of individuals, data subjects must be notified.
- DPO should Investigate the failure and take remedial steps if necessary
- Incident will be marked on a compliance register.
- A risk management team including Principal, other top admin and DPO will evaluate and assess the risk level of the incident.

- All responses regarding the incidents should be recorded by DPO.
- Identify the extent of data breach, loss of data and stop additional data loss by securing IT systems.
- If any risk arise to the rights and freedom of data subjects affected by data breaches, notify them.
- Inform police and notify regulatory bodies if necessary (notification should contain the details of the nature of data breach, number of data subjects/personal data records affected, possible consequences of the incident and the steps taken or must be adopted to reduce the adverse effect).

MONITORING AND REVIEWING THE POLICY

Failure to comply the policy would place both staff and organization at risk. So every staff must have clear idea of this policy. Monitoring and reviewing should be done by DPO.

INFORMATION WE COLLECT

For a better experience while using our Service, we may require you to provide us with certain personally identifiable information, including but not limited to your name, phone number, and postal address. The information that we collect will be used to contact or identify you.

THE PERSONAL INFORMATION

The information we may directly collect from you includes personal, sensitive information such as:

- Student's name,Staff name, Parent's or Guardian name.
- Email address, telephone or mobile number, postal address, etc.
- Student'sStaff age, date of birth, details of family members, siblings, etc.
- Future communication preference.
- Payment information, if payment is made through net banking, credit or debit card, etc.
- Medical ailment.
- Details of school staffs

HOW WE USE THIS INFORMATION

We provide information to students, parents and staffs by way of digital or electronic communication such as email, mobile, SMS, phone call and postal mail

WHAT INFORMATION WE SEND

We collect the information to provide the progress, improvement and other information about the student's matters related to their schooling and also related to staffs of the school. We also provide the day to day administrative activities, events, celebrations, competitions, sports and others activities organized by the school.

OUR LEGAL BASIS ON USING DATA

We only collect and use students' and staffs' personal data when the law allows us to. Most commonly, we process it where:

- To respond to your application
- To register in MOE.
- To register in CBSE
- To perform an official task in the public interest
- To notify you about changes to our services
- To enter staff details in MOE and Ministry of Labour
- To comply with a legal obligation.

Where we have obtained consent to use students' and staffs' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn. Some of the reasons listed above for collecting and using students' and staffs' personal data overlap, and there may be several grounds which justify our use of this data.

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Mr.Navas Rahimkutti, Data Protection Officer.