SIAL

(LA SCUOLA ITALIANA A LONDRA)

DATA PROTECTION POLICY

Last Reviewed May 2018

Date of next review May 2021

SIAL DATA PROTECTION POLICY

Introduction

SIAL needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, staff and board of directors and other people SIAL has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law. For the purpose of the UK Data Protection Act 1998 (henceforward referred to as the 1998 Act), SIAL is the data controller.

1 This data protection policy ensures SIAL:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

2 SIAL collects, handle and store personal information in accordance with the Data Protection Act 1998. More specifically SIAL ensure that all personal information is collected and used fairly, stored safely and not disclosed unlawfully. SIAL commits to ensuring that all personal data is:

- processed fairly and lawfully;
- obtained only for specific, lawful purposes;
- adequate, relevant and not excessive;
- accurate and kept up to date;
- Not held for any longer than necessary;
- processed in line with data subjects' rights;
- secure; and
- not transferred to other countries outside the European Economic Area without adequate protection.

3 This policy applies to the school office of SIAL, all its staff and volunteers, the board of directors and all its contractors, suppliers and other people working on behalf of SIAL. It applies to all data that SIAL holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998.

Under GPDR, 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

4 SIAL further commits to monitoring, the effectiveness of all policies guiding data use, and by providing ongoing training for staff handling data. In addition, all new systems, policies and procedures introduced at SIAL will be designed to include consideration of data privacy concerns.

5 Everyone who works for or with SIAL has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas responsibility:

- The board of directors is ultimately responsible for setting SIAL's strategy and agreeing the security posture and risk appetite, whilst meeting its legal obligations;

- The Data Protection Officer (DPO) together with the Senior Leadership Team is responsible for:

  - Keeping the board updated about data protection responsibilities, risks and issues.

  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.

  - Arranging data protection training and advice for the people covered by this policy.

  - Handling data protection questions from staff and anyone else covered by this policy.

  - Dealing with requests from individuals to see the data SIAL holds about them (also called 'subject access requests').

  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The [SLT] is responsible for:

  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

  - Performing regular checks and scans to ensure security hardware and software is functioning properly.

  - Evaluating the security posture and risk appetite of any third-party services the company is considering using to store or process data. For instance, cloud computing services.

  - Approving any data protection statements attached to communications such as emails and letters.

  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

- The staff is responsible for:

  - Following the security guidelines detailed in the staff handbook;
  - Raising any concerns relating to information security to the SLT

6 In handling personal data, SIAL is guided by the following principles:

- The only people able to access data covered by this policy are those who need it for their work.

- Data is not shared informally. When access to data is required, staff, volunteers and directors can request it from the school office.

- SIAL will provide training to the board, staff and volunteers to help them understand their responsibilities when handling data.

- The board, staff and volunteers should keep all data secure, by taking sensible precautions and following SIAL's guidelines.

- SIAL will make it easy for data subject to update the information SIAL holds about them (for example via the website).

- Strong passwords must be used, and they should never be shared.

- Staff should request help from the DPO if they are unsure about any aspect of data protection.

- When data is stored on paper**,** it is kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

- When not required, the paper or files should be kept in a locked drawer or filing cabinet and held in as few places as necessary.

- Staff must make sure paper and printouts are not left where unauthorised people could see them, like on a printer.

- Data printouts should be shredded and disposed of securely when no longer required.

- When data should be stored electronically, it will be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Data stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.

- Data should only be stored on designated drives and servers and it will only be uploaded to an approved cloud computing services.

- Servers containing personal data is sited in a secure location, away from general office space.

- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

- Data should never be saved directly to laptops or other mobile devices like tablets

  or smart phones.

- All servers and computers containing data should be protected by approved security software and a firewall.

7 SIAL recognises the important of being transparent and of providing accessible information to individuals about how we will use their personal data is important for our organisation.

8 SIAL recognises that all individuals who are the subject of personal data held by SIAL are entitled to ask what information SIAL holds about them and why, how to gain access to it, how to keep it up to date. If an individual contacts SIAL requesting this information, this is called a Data Subject Access Request. Data Subject Access Requests from individuals should be made by email, addressed to SIAL DPO at dpo@scuolaitalianalondra.org. Individuals will not be charged for this request, unless the request is manifestly unfounded or excessive, particularly if it is repetitive. SIAL will aim to provide the relevant data within one month. If a request is manifestly unfounded or excessive, SIAL may refuse to respond but will provide evidence of how the conclusion that the request is manifestly unfounded or excessive was reached. SIAL will always verify the identity of anyone making a subject access request before handing over any information. However, SIAL will withhold personal data if disclosing it would adversely affect the rights and freedoms of others.

9 SIAL recognises its duty to report to the Information Commissioner's Office any data breach likely to result in a risk for the rights and freedoms of individuals. SIAL also commits to reporting any such breach within 72 hours of first becoming aware of it, and of appropriately notifying data subjects and data controllers without undue delay

10 In certain circumstances, legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances SIAL will disclose requested data. However, SIAL will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

11 SIAL aims to ensure that individuals are aware that their data is being processed, and that they understand how the data is being used and how to exercise their rights. To these ends, SIAL has a privacy policy, setting out how data relating to individuals is used by the company. A version of this policy is also available on the SIAL's website.

12 SIAL has guidelines governing the use of encryption that enable staff to understand when they should and should not use it.