Procedure 1.7 Data Protection					
Prepared by	Ian Fleming	**Reviewed by**	Erhan Yurdakul Ercan Erkus	**Approved by**	Canan E. Celik
Review No	4	**Next Review Date**	July 2022	**Approved on**	20/07/2021

Procedure issued: April 2014

Procedure owner: Principal / CEO

- This procedure is shared with our students and/or can be obtained:
  - on our website https://docklandsacademy.co.uk/policies-and-procedures,
  - on the desktops of all computers in the library on the top floor,
  - by emailing us at info@docklandsacademy.co.uk.
- The policy is reviewed and monitored on a regular basis for currency and fitness as part of our Procedure 1.9 Review and Revision of Policies and Procedures.

This important procedural document comprises three parts, the formal Data protection procedure, Annex1, the DAL Privacy Notice and Annex 2, the DAL Data breach procedure

The Procedure

1 Background

The *Data Protection Act* 1988 has now been superseded by the EU *General Data Protection Regulation (GDPR) and Data Protection Act 2018 is also in force* and this procedure sets out the ways in which the Academy will meet the requirements of GDPR. Many of the GDPR`s concepts and principles are similar to those of the *Data Protection Act* but there are also new elements and significant enhancements.

Employees are entitled to access certain records and can seek compensation for damage or distress suffered as a result of a breach of the *Regulation*. This means that all managers should take special care when recording information about their staff.

This procedure and guide explains what records should be kept and for how long and offers advice and explains the Academy`s legal obligations as an employer and employees' rights regarding information held about them.

2 Requirements of GDPR

The *Regulation* is concerned with personal data: information about living, identifiable individuals (*natural persons*) held on computer or in certain structured manual filing systems.

There are clear principles for processing data to comply with the *Regulation*.

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. The principle of consent is vital
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

These principles should be considered when deciding what information to collect, when establishing procedures for processing this information and when dealing with requests from employees.

Failure to comply with the *Regulation* and the data protection principles could result in the Information Commissioner's Office (ICO) issuing an enforcement notice. Contravention of a notice is a criminal offence.

Staff and other individuals can also seek compensation if they suffer damage (usually physical or financial) or distress as a result of a breach of the *Regulation* by the business.

3 Keeping staff records: the legal requirements

To comply with the law, the Academy should keep records on:

- hours worked, and employees who have agreed to work more than 48 hours, to meet the requirements of the Working Time Regulations
- pay rates; to meet the statutory requirement to issue employees with pay statements and to ensure that the requirements of the National Minimum Wage Act 1998 are met
- payroll: i.e. on income tax and National Insurance deductions, for HM Revenue & Customs
- sickness of more than four days and how much statutory sick pay has been have paid
- accidents, injuries and dangerous occurrences - to meet health and safety requirements

- accounting data
- crime prevention information
- pensions data
- mortgage or insurance administration

Other staff records that should be kept:

Records of each employee`s:

- training and performance review
- employment history: date employment began, promotions, job title(s)
- absence: records of lateness, sickness, and any other authorised or unauthorised absences
- personal details: name, address, emergency phone number(s), qualifications, work-relevant disability
- terms and conditions and employment; including a copy of each employee's written and correspondence relating to any changes to their terms and conditions

More general records:

- meetings with workplace representatives
- any disciplinary action taken, and records of disciplinary hearings
- individual and collective redundancy consultation meetings and agreements
- negotiations relating to information and consultation agreements

4 The level of detail in employee records

Any personal information kept on employees should be adequate, relevant and not excessive. Inadequate records lead to problems when dealing with absence levels, staff turnover, sickness, lateness and discipline. The records system should be simple, reliable and flexible.

Not all records can be maintained electronically; employee files will also need to hold signed copies of certain key documents; this is especially important in the event of any tribunal claims against the Academy. Good practice in data security includes:

- a lockable paper filing system
- access to the data only granted to staff who need to use it
- electronic records protected with passwords, anti-virus software and firewalls
- an audit trail used with electronic systems to enable checks on who has accessed a particular record and when

How long to retain staff records

It is good practice to retain records for six years, to cover the time limit for bringing any civil legal action against the Academy, including national minimum wage claims and contractual claims.

The following table gives more specific guidance for particular types of records.

Record	Statutory retention period
Accident reports	Three years after date of last entry. There are rules on recording incidents involving hazardous substances.
Payroll records	At least three years after the end of the tax year they relate to
Statutory maternity, adoption and paternity pay records	Three years after the end of the tax year they relate to
Statutory sick pay records	Three years after the end of the tax year they relate to
Working time	Two years from date on which they were made
National minimum wage records	Three years after the end of the pay reference period following the one that the records cover
Retirement benefits schemes - notifiable events, eg relating to incapacity	Six years from the end of the scheme year in which the event took place
Application forms/interview notes for unsuccessful candidates	One year
Health and safety records of consultations	Permanently
Parental leave taken	Five years from birth/adoption, or until child is 18 if disabled
Pensioners' records	12 years after benefit ceases
Disciplinary, working time and training records	Six years after employment ceases
Redundancy details	Six years from date of redundancy
Senior executives' records	Permanently for historical purposes
Trade union agreements	Ten years after ceasing to be effective
Minutes of trustee/work council meetings	Permanently
'Right to work' documents	Two years after employment ceases

The *Regulation* requires that data should not be retained any longer than is necessary for a particular purpose. When data is no longer required it should be disposed of securely and

effectively. Where possible, data on employees and former employees should be made anonymous before disposal.

5 Notifying the Information Commissioner`s Office

In addition to complying with the *Regulation* and the data protection principles, the Academy Data Controller is expected to notify the ICO about processing of personal information. The ICO issues guidance on this process and on how to comply with data protection legislation.

6 Employees` rights of access to data

Under the *Regulation*, individuals have a number of rights, in particular the right to access any information held about them. If an employee asks for any information held about them; a subject access request; they must make the request in writing, The Academy is not permitted to charge for providing the information and should reply within 30 days.

Information that the Academy is not required to provide under subject access requests:

- information held for management planning, e.g. plans to promote an employee or make an employee redundant
- information as to your intentions in respect of negotiations with the requester
- references you have given about the worker in confidence (references received by you are not exempt)
- information about the prevention or detection of a crime, or the arrest or prosecution of offenders
- information that may identify someone else

Employees` rights in relation to data held about them:

As well as the right to access data on themselves, an employee also has the right to:

- have inaccurate personal data corrected
- compensation for damage suffered as a result of any breach of the Regulation
- prevent processing likely to cause substantial damage or substantial distress
- be told the rationale for any automated decision taken about them, e.g. psychometric testing decisions

If an employee has reasonable grounds to believe you have not paid them the national minimum wage, they have the right to see their pay records. They must make a written request, and the records must be produced within 14 days.

7 Data protection by design and Data Protection Impact Assessments (DPIAs)

The GDPR makes privacy by design an express legal requirement, under the term *data protection by design and by default.* A Data Protection Impact Assessment (DPIA) is mandatory when data processing may result in high risk to individuals, such as:

- where new technology is introduced

- where a profiling operation may affect individuals
- where there is processing on a large scale of special categories of data

The ICO has produced helpful guidance on conducting Impact Assessments.

8 Data Controller

Although the Academy is not required by law to appoint a Data Protection Officer (DPO), the Academy has appointed a Data Controller to maintain an overview of data processing and information provision. The Data Controller is the CEO / Principal.

The DAL *Privacy Statement* states clearly how the Academy deals with personal data and forms an Annex to this procedure.

9 Related Documents

Policies 1-9 and its associated Procedures that have direct relevance to Data Protection

Student Terms and Conditions

External Reference Points

- **Data Protection Act 2018** *https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted*
- **Information Commissioners' Office** *https://ico.org.uk/*
- **Office for Students (OfS) Requirements and Guidance** at *https://www.officeforstudents.org.uk/advice-and-guidance/regulation/*
- **UK Quality Code Advice & Guidance – Admissions, Recruitment and Widening Access** at *https://www.qaa.ac.uk//en/quality-code/advice-and-guidance/admissions-recruitment-and-widening-access*
- **Higher Education Code of Governance** (Committee of University Chairs, December 2014) at *https://www.universitychairs.ac.uk/wp-content/uploads/2020/09/CUC-HE-Code-of-Governance-publication-final.pdf*
- **Association of Employment and Learning Providers (AELP) principles of Good Governance for Independent Training Providers** at *https://www.aelp.org.uk/media/2595/code-of-governance-final-sept-2018.pdf*
- **Competition and Markets Authority Guidance for HE Providers** at *https://www.gov.uk/government/publications/higher-education-consumer-law-advice-for-providers*
- **UKCISA Code of Ethics** at *https://www.ukcisa.org.uk/Membership/Codes-of-practice/Code-of-ethics*

Annex 1

GDPR Privacy Statement

Docklands Academy London (DAL) is committed to protecting your privacy

Docklands Academy London (DAL) is committed to data security and to the fair and transparent processing of personal data. This Privacy Statement sets out how we deal with the personal data which you provide to us, in compliance with the *General Data Protection Regulation* (GDPR).

Please read this Statement carefully, as it contains important information on how and why we collect, store, use and share personal data, your rights in relation to your personal data. It also states how to contact us and the supervisory authorities in the event of any concern about the way in which we process your data.

Docklands Academy London (DAL) is a not-for-profit company, with premises located at 11-13 Selsdon Way, London E14 9GL and with registered UK company number 06999859. Our registered address is 261 Green Lanes, Palmers Green, London N13 4XE.

Docklands Academy London (DAL) has appointed a Data Controller, who you can contact if necessary by sending an email to info@docklandsacademy.co.uk.

What personal data do we collect?

We may collect and process the following personal data:

Information about you:

If you are a student, tutor/lecturer, member of staff or administrator at Docklands Academy London (DAL), we may receive information about you when you register or liaise with us to receive products and/or services from us.

Information you provide to us:

If you:

- complete a form on our website
- complete a survey
- correspond with us by telephone, e-mail, or in writing
- report a problem
- sign up to receive our communications
- register as a student with us

- enter into a contract with us to receive products and/or services,

We may collect and store your name, date of birth, e-mail address, postal address, telephone number and other relevant data that you supply at that time.

If you are aged 16 or under you must have the Academy's Parental Consent Form signed by your Parents / Guardians. Unless you have this consent, you are not allowed to provide your information. We will not gather, hold or process any information without such consent.

Information about other people:

If you provide information to us about any person other than yourself, such as your relatives, next of kin, your advisers or your suppliers, you **must** ensure that they understand how their information will be used, and that they have given their permission for you to disclose it to us and for you to allow us to use it.

Sensitive personal data:

In certain limited cases, we may collect certain sensitive personal data from you, that is, information about your racial or ethnic origin, religious beliefs or details of criminal offences, or genetic or biometric data. However, we will only do so on the basis of your **explicit consent**

Cookies:

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

We use traffic log cookies to identify which pages are being used. This helps us analyse data about web page traffic and improve our website to better tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or to any information about you, other than the data you choose to share with us. **You can choose to accept or decline cookies**. Some web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may, of course, prevent you from taking full advantage of the website.

How do we use your personal data?

When we ask you to supply us with personal data, we will make it clear whether the personal

data we are asking for must be supplied so that we can provide the products and services to you, or whether the supply of any personal data we ask for is optional.

Contract performance:

We may use your personal data to fulfil a contract, or take steps linked to a contract:

- to provide products and/or services to you
- to communicate with you in relation to the provision of contracted products and services
- to provide you with administrative support, such as account creation, security, and responding to issues
- provide you with industry information, surveys, information about our awards and events, or offers and promotions related to our products and/or services

Legitimate interests:

Where this is necessary for purposes which are in our legitimate interests.

These interests are:

- providing you with newsletters, surveys, information about our awards and events, offers, and promotions, related to products and services offered by Docklands Academy London (DAL) which may be of interest to you
- communicating with you in relation to any issues, complaints, or disputes
- improving the quality of experience when you interact with our products and/or services, including testing the performance and customer experience of our website
- performing analytics on sales/marketing data, determining the effectiveness of promotional campaigns and activities

Note: you have the right to object to the processing of your personal data on the basis of legitimate interests as set out below, under the heading your rights.

Consent:

Where you have given your **explicit consent** to receive marketing communications, we may use your personal data to:

- send you newsletters, surveys, information about our awards and events, offers, and promotions, related to products and services offered by Docklands Academy London (DAL) which may be of interest to you
- develop, improve, and deliver marketing and advertise for products and services offered by Docklands Academy London (DAL)

Where required by law:

We may also process your personal data if required by law including responding to requests by government or law enforcement authorities, or for the prevention of crime or fraud.

Who do we share your personal data with?

We take all reasonable steps to ensure that our staff protect your personal data and are aware of their information security obligations. We limit access to your personal data to those who have a genuine business need to know it.

We may also share your personal data with trusted third parties, including legal and other professional advisers, consultants, and professional experts, service providers contracted to us in connection with provision of our products and services, such as providers of IT services and customer relationship management services; and analytics and search engine providers that assist us in the improvement and optimisation of our website.

We will ensure there is a contract in place with the categories of recipients listed above which include obligations in relation to the confidentiality, security, and lawful processing of any personal data shared with them.

Where a third party recipient is located outside the European Economic Area, we will ensure that the transfer of personal data will be protected by appropriate safeguards, namely the use of standard data protection clauses adopted or approved by the European Commission where the data protection authority does not believe that the third country has adequate data protection laws.

We will share personal data with law enforcement or other authorities if required by applicable law.

How long will we keep your personal data?

Where there is a contract between us, we will retain your personal data for the duration of the contract, and for an indefinite period following its termination or expiry, to ensure we are able to comply with any contractual, legal, audit and other regulatory requirements, or any orders from competent courts or authorities. Specifically, student registration and results data will be kept in perpetuity to enable us to confirm validity of awards on request

Where you have consented to marketing communications, you may change your preferences or unsubscribe from marketing communications at any time by clicking the unsubscribe link in an email from us. Consent for marketing communications will be deemed to expire after three years unless renewed.

Where do we store your personal data and how is it protected?

We take reasonable steps to protect your personal data from loss or destruction. We have procedures in place to deal with any suspected data security breach. We will notify you and the Information Commissioner`s Office (ICO) of a suspected data security breach where we are legally required to do so.

If you have a username or password (or other identification information) which enables you to access certain services or parts of our website, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your personal data transmitted to our website; any transmission is at your own risk. Once we have received your personal data, we will use strict procedures and security features to try to prevent unauthorised access.

Your rights

Under GDPR, you have various rights with respect to our use of your personal data:

Right to access:

You have the right to request a copy of the personal data that we hold about you by contacting us by email or post. Please include with your request any information that will enable us to verify your identity. We will respond with 30 days of request.

Please note that there are exceptions to this right. We may be unable to make all information available to you if, for example, making the information available to you would reveal personal data about another person, if we are legally prevented from disclosing such information or if your request is manifestly unfounded or excessive.

Right to rectification:

We aim to keep your personal data accurate and complete. We encourage you to contact us using the contact details provided to let us know if any of your personal data is not accurate or if it changes, so that we can keep your personal data up-to-date.

Right to erasure:

You have the right to request the deletion of your personal data where, for example:

- the personal data are no longer necessary for the purposes for which they were collected
- where you wish to withdraw your consent to processing
- where there is no overriding legitimate interest for us to continue to process your personal data
- if your personal data has been unlawfully processed.

If you would like to request that your personal data is erased, please contact us.

Right to object:

In certain circumstances, you have the right to object to the processing of your personal data where, for example, your personal data is being processed on the basis of legitimate interests and there is no overriding legitimate interest for us to continue to process your personal data, or if your data is being processed for direct marketing purposes. If you would like to object to the processing of your personal data, please contact us.

Right to restrict processing:

In certain circumstances, you have the right to request that we restrict the further processing of your personal data. This right arises where, for example, you have contested the accuracy of the personal data we hold about you and we are verifying the information, you have objected to processing based on legitimate interests and we are considering whether there are any overriding legitimate interests, or the processing is unlawful and you elect that processing is restricted rather than deleted.

Right to data portability:

In certain circumstances, you have the right to request that some of your personal data is provided to you, or to another data controller, in a commonly used, machine-readable format. This right arises where you have provided your personal data to us, the processing is based on consent or the performance of a contract, and processing is carried out by automated means. If you would like to request that your personal data is ported to you, please contact us.

Please note that the GDPR sets out some exceptions to these rights. If we are unable to comply with your request due to an exception we will explain this to you in our response.

Complaints:

If you believe that your data protection rights may have been breached, you may follow our procedure 2.5 Complaints for a remedy. If you are unhappy with the outcome, you have the right to appeal to the Information Commissioner. Please visit https://ico.org.uk/concerns/ for more information on how to report a concern to the Information Commissioner's Office (ICO).

Contact

If you would like to contact us about this Privacy Statement, our use of your personal data, or about exercising any of your rights, please contact us:

Data Controller: CEO / Principal

Docklands Academy London (DAL)
11 Selsdon Way,
City Harbour,
London
E14 9GL

0207 515 9695

info@docklandsacademy.co.uk

www.docklandsacademy.co.uk

Annex 2

Data Breach Procedure

1. Introduction

1.1 Docklands Academy London (DAL) collects, holds, processes, and shares personal data, a valuable asset that needs to be suitably protected.

1.2 Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

1.3 Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.

2. Purpose and Scope

2.1 Docklands Academy London is obliged under Data Protection legislation (The General Data Protection Regulation – GDPR, Data Protection Act 2018- DPA) and related EU and national legislation to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

2.2 This document sets out the process to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across Docklands Academy London (DAL).

2.3 This document relates to all personal and special categories (sensitive) data held by the Academy regardless of format.

2.4 This document applies to all staff and students at the Academy. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the Academy.

2.5 The objective of this procedure is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

3. Definitions / types of breach

3.1 For the purpose of this procedure, data security breaches include both confirmed and suspected incidents.

3.2 An incident in the context of this procedure is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the Academy`s information assets and / or reputation.

3.3 An incident includes, but is not restricted to, the following:

3.3.1 loss or theft of confidential or sentitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record);

3.3.2 equipment theft or failure;

3.3.3 system failure;

3.3.4 unauthorised use of, access to or modification of data or information systems;

3.3.5 attempts (failed or successful) to gain unauthorised access to information or IT system(s);

3.3.6 unauthorised disclosure of sensitive / confidential data;

3.3.7 website defacement;

3.3.8 hacking attack;

3.3.9 unforseen circumstances such as a fire or flood;

3.3.10 human error;

3.3.11 'blagging' offences where information is obtained by deceiving the organisation which holds it.

4. Reporting an incident

4.1 Any individual who accesses, uses or manages the Academy`'s information is responsible for reporting data breach and information security incidents immediately to the Data Controller (at info@docklandsacademy.co.uk) and IT Services (at ayhan@aksystem.pro).

4.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

4.3 The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process (refer to Appendix 1).

4.4 All staff should be aware that any breach of Data Protection legislation may result in disciplinary procedures being instigated.

5. Containment and recovery

5.1 The Data Controller will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

5.2 An initial assessment will be made by the Data Controller in liaison with relevant officer(s) to establish the severity of the breach and who will take the lead investigating the breach, as the Lead Investigation Officer (this will depend on the nature of the breach; in some cases it could be the DC).

5.3 The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

5.4 The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

5.5 Advice from experts across the Academy may be sought in resolving the incident promptly.

5.6 The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

6. Investigation and risk assessment

6.1 An investigation will be undertaken by the LIO immediately and wherever possible, within 24 hours of the breach being discovered / reported.

6.2 The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

6.3 The investigation will need to take into account the following:

6.3.1 the type of data involved;

6.3.2 its sensitivity;

6.3.3 the protections are in place (e.g. encryptions);

6.3.4 what has happened to the data (e.g. has it been lost or stolen;

6.4.5 whether the data could be put to any illegal or inappropriate use;

6.4.6 data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);

6.4.7 whether there are wider consequences to the breach.

7. Notification

7.1 The LIO and / or the DC, in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

7.2 Every incident will be assessed on a case by case basis; however, the following will need to be considered:

7.2.1 whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation;

7.2.2 whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks);

7.2.3 whether notification would help prevent the unauthorised or unlawful use of personal data;

7.2.4 whether there are any legal / contractual notification requirements;

7.2.5 the dangers of over notifying. Not every incident warrants notification and over-notification may cause disproportionate enquiries and work.

7.3 Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how

and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks.

Individuals will also be provided with a way in which they can contact Docklands Academy London (DAL) for further information or to ask questions on what has occurred.

7.4 The LIO and / or the DC must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

7.5 The LIO and or the DC will consider whether senior management should be informed regarding a press release and to be ready to handle any incoming press enquiries.

7.6 A record will be kept of any personal data breach, regardless of whether notification was required.

8 Evaluation and response

8.1 Once the initial incident is contained, the DC will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

8.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

8.3 The review will consider:

8.3.1 where and how personal data is held and where and how it is stored;

8.3.2 where the biggest risks lie including identifying potential weak points within existing security measures;

8.3.3 whether methods of transmission are secure; sharing minimum amount of data necessary;

8.3.4 staff awareness;

8.3.5 implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

8.4 If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Board of Governance.

9. Review

9.1 This procedure will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify your managerl immediately, complete Section 1 of this form and email it to the Data Controller (info@docklandsacademy.co.uk) and IT Helpdesk (ayhan@aksystem.pro) where appropriate.

Section 1: Notification of data security breach	To be completed by manager of person reporting incident
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Controller	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of severity	To be completed by the Lead Investigation Officer in consultation with the Head of area affected by the breach and if appropriate IT

	where applicable
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for (DAL) or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data • Special categories personal data (as defined in the Data Protection Legislation) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious beliefs; c) trade union membership; d) genetics; e) biometrics (where used for ID purposes) f) health; g) sex life or sexual orientation	
Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	

Personal information relating to vulnerable adults and children;	
Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals	
Security information that would compromise the safety of individuals if disclosed.	
Data Controller and/or Lead Investigation Officer to consider whether it should be escalated to the appropriate Board member	

Section 3: Action taken	To be completed by Data Controller and/or Lead Investigation Officer
Incident number	e.g. year/001
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	YES/NO If YES, notified on: Details:
Follow up action required/recommended:	
Reported to Data Controller and Lead Officer on (date):	
Reported to other internal stakeholders (details, dates):	
For use of Data Controller and/or Lead Officer:	
Notification to ICO	YES/NO If YES, notified on: Details:

Notification to data subjects	YES/NO If YES, notified on: Details:
Notification to other external, regulator/stakeholder	YES/NO If YES, notified on: Details: