DOWNSVIEW PRIMARY SCHOOL

Data Security Breach Prevention Policy and Data Breach Procedure

Originator: **Carol Christodoulou**

Created: March 2025
Review Date: March 2027

Downsview Primary School
Biggin Way
Upper Norwood
London
SE19 3XE

Telephone: 020 8764 4611
Email: sec1@downsview.croydon.sch.uk
Webpage: www.downsview.croydon.sch.uk

Data Security Breach Prevention Policy and Data Breach Procedure

CONTENTS

Statement of Intent

Downsview Primary & Nursery School is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the school are only accessible by the appropriate individuals. It is therefore important to uphold high standards of security, take suitable precautions, and to have systems and procedures in place that support this.

The school recognises, however, that breaches in security can occur, particularly as the majority of information is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks. This being the case, it is necessary to have a contingency plan containing procedures to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence.

1. Legal Framework

1.1. This policy has due regard to statutory legislation and regulations including, but not limited to, the following:

- The Data Protection Act 2018
- The Computer Misuse Act 1990
- The UK General Data Protection Regulation (UK GDPR)
  Guidance produced by the Information Commissioner's Office (ICO).

1.2. This policy has due regard to the school's policies and procedures including, but not limited to, the following:

- Data Protection Policy
- Data Retention Policy
- Online Safety, Social Media, Devices and Acceptable Use Policy
- IT Security Policy
- Cyber Response Plan

2. Types of Security Breach and Causes

2.1. **Unauthorised use without damage to data** – involves unauthorised persons accessing data on the school system, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it.

2.2. **Unauthorised removal of data** – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it,

2.3. **Damage to physical systems** – involves damage to the hardware in the school's ICT system, which may result in data being inaccessible to the school and/or becoming accessible to unauthorised persons.

2.4. **Unauthorised damage to data** – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

2.5. Breaches in security may be caused as a result of actions by individuals, which may be accidental, malicious or the result of negligence – these can include:

- Accidental breaches
- Malicious breaches
- Negligence

2.6. Breaches in security may also be caused as a result of system issues, which could involve incorrect installation, configuration problems or an operational error – these can include:

- Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the school software is more vulnerable to a virus
- Incorrect firewall settings are applied, e.g. access to the school network, meaning individuals other than those required could access the system
- Confusion between backup copies of data, meaning the most recent data could be overwritten

3. Roles and Responsibilities

3.1. The Governing Board is responsible for holding regular meetings with the Headteacher to discuss the effectiveness of data security, and to review incident logs.

3.2. The School, as Data Controller, is responsible for the overall monitoring and management of data security.

3.3. Headteacher is responsible for establishing a procedure for managing and logging incidents.

3.4. The Computing Leader is responsible for implementing effective strategies for the management of risks posed by internet use, and to keep its network services, data and users secure.

3.5. All members of staff, pupils and authorised guest users of the school's IT systems are responsible for adhering to the processes outlined in this policy, alongside the school's Online Safety, Social Media, Devices and Acceptable Use Policy.

4. Secure Configuration

4.1. An inventory will be kept of all IT hardware currently in use at the school, including mobile phones and other devices provided by the school. This will be stored in the school's Asset Management software and will be audited on an annual basis to ensure it is up-to-date. Any changes to IT Hardware must be authorised by the Headteacher and recorded on the school's Asset Management Software.

4.2. The school's appointed System Manager is Octavo Information Systems under a Service Level Agreement which is reviewed annually in April each year. The System Manager is responsible for the school's IT systems and network security and for ensuring that any new versions of software or new security patches added to system do not affect network security.

4.3. Any software that is out-of-date or reaches its 'end of life' will be removed from the school's IT systems.

4.4. Laptop and computer passwords will be changed termly by arrangement with the school's System Manager in order to prevent unauthorised access to the school's IT systems.

5. Network Security

5.1. The school ensures that robust firewalls are in place in order to prevent unauthorised access to the school network.

5.2. The school's firewall is deployed as a centralised deployment: the broadband service connects to a firewall that is located in a network location outside of the school.

5.3. The school's firewall is managed locally by the school's System Manager, who will ensure that:

- Any changes and updates that are logged by authorised users within the school are undertaken efficiently by the provider to maintain operational effectiveness.
- Patches and fixes are applied quickly to ensure that the network security is not compromised.

6. Malware Prevention

6.1. The school understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

6.2. The System Manager will ensure that all school devices have secure malware protection and undergo regular malware scans. The System Manager will update malware protection on a regular basis to ensure it is up-to-date and can react to changing threats.

6.3. The school uses the London Grid for Learning's MailProtect software to detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users.

7. User Privileges

7.1. The school understands that controlling what users have access to is important for promoting network security. User privileges will be differentiated according to user's rights.

7.2. Access rights are determined by the Headteacher and recorded in the school's Access Rights to School IT Network and Software Log.

7.3. The System Manager will ensure that user accounts are set up to allow users access to the facilities required, in line with the Headteacher's instructions.

7.4. The Computing Leader will be the official point of contact for IT security issues and, as such, is responsible monitoring the IT System and for notifying the Headteacher, or a Deputy Headteacher in their absence, of any suspected or actual breach of IT security occurring within the school.

8. Monitoring Usage

8.1. The school will inform all pupils and staff that their usage will be monitored, in accordance with the school's Online Safety, Social Media, Devices and Acceptable Use Policy.

8.2. Any unauthorised or inappropriate content which is alerted to the school's Computing Leader will be investigated and logged in accordance with the school's Online Safety, Social Media, Devices and Acceptable Use Policy.

9. Removable Media Controls and Home Working

9.1. The school understands that staff may need to access the school network from areas other than on the premises. Effective security management is in place to prevent access to, or leakage of, data, as well as any possible risk of malware.

9.2. All school-owned devices which may be used off the school site, such as laptops, mobile phones and Ipads are password encrypted to prevent unauthorised access.

9.3. Pupils and staff are not permitted to use their personal devices for school use where the school provides alternatives, e.g. laptops/Ipads/mobile phones, unless approved by the Headteacher.

9.4. Staff who use school-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off school premises.

9.5. The school uses tracking technology, where possible, to ensure that lost or stolen devices can be retrieved.

9.6. The Wi-Fi network at the school is password protected and will only be given out to staff members for school use.

9.7. A separate guest Wi-Fi login is available for visitors at the school to limit their access to printers, shared storage areas and any other applications, which are not necessary.

10.User Training and Awareness

10.1. The school arranges training for pupils and staff to ensure they are aware of how to use the network appropriately in accordance with the Online Safety, Social Media, Devices and Acceptable Use Policy.

10.2. Through training, all pupils and staff will be aware of who they should inform first in the event that they suspect a security breach, and who they should inform if they suspect someone else is using their passwords.

11.Security Breach Incidents

11.1. The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, school staff must follow the **Data Breach Procedure** set out below.

12.Monitoring and Review

12.1. This policy will be reviewed every two years.

12.2. The Headteacher is responsible amending this policy and communicating any changes to staff members.

Data Breach Procedure

In the event of a suspected data breach this procedure must be followed by employees at Downsview Primary & Nursery School.

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The breach may relate to electronic or hard copied data.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Headteacher, or a Deputy Headteacher in their absence, on the **Data Breach Notification Form** in **Appendix 1**

Upon receipt of a **Breach Notification Form** the breach will be recorded in the school's **Data Breach Log, including the following information**:

- **Name of the individual who has raised the incident**
- **Data and Time of the actual Breach**
- **Summary of the Breach**
- **Description and identification codes of any devices involved, e.g. school-owned laptop**
- **Location of the equipment involved**
- **Contact details for the individual who discovered the incident**

The following questions will be considered by the Headteacher, or their Deputy, in order to fully assess the risks of the security breach and to help take the next appropriate steps:

- Is the breach a minor internal breach or external?
- What type and how much data is involved?
- How sensitive is the data? Special categories of 'sensitive data' include data which is sensitive because of its very personal nature (e.g. health records) whilst other data types are sensitive because of what might happen if misused (e.g. bank account details).
- Is it possible to identify what has happened to the data – has it been lost, stolen, deleted or tampered with?
- If the data has been lost or stolen, were there any protective measures in place to prevent this, such as data and device encryption?
- If the data has been compromised, have there been effective measures in place that have mitigated the impact of this, such as the creation of a back-up and/or spare copies?
- How many individuals are affected? Who are these individuals – are they pupils, staff, governors, volunteers, stakeholders, suppliers?
- Could their information be misused or manipulated in any way?
- Could harm come to individuals? This could include risks to the following: e.g., physical safety, emotional wellbeing, reputation.
- Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence/damage to the school's reputation, or risk to the school's operations?
- Who could help or advise the school on the breach? Could the local authority or Data Protection Officer provide support?

In the event that the Headteacher, or other persons involved in assessing the risks to the school, are not confident in the risk assessment, advice should be sought from the schools Data Protection Officer and/or the Information Commissioner's Office (ICO).

The school will decide whether the incident is a Minor Breach or Major Breach, examples are shown below:

MINOR INTERNAL BREACH

A Minor Breach may consist of:

- Mislaid document within the school building
- Leaving a cupboard containing personal data unlocked
- Leaving personal data unattended on a PC or Laptop
- Leaving papers containing personal data on desks

MAJOR BREACH

A Major Breach may consist of:

- Safeguarding information being made available to an unauthorised person
- The theft or hacking of a school laptop containing non-encrypted personal data about pupils
- Sensitive information being disclosed via email
- The school's cashless payment provider being hacked and parents' financial details stolen

ACTION TO BE TAKEN IN THE CASE OF A MINOR INTERNAL BREACH

- The Headteacher will take the lead in investigating the breach.
- The breach will be logged in the school's **Data Breach Log.**
- The Headteacher will ascertain the severity of the breach and determine if any personal data is involved or compromised. The Headteacher will consider, as necessary, the need to notify any third parties – police, insurers, professional bodies, funders, trade unions, website system owners and banks – who can assist in helping or mitigating the impact on individuals.
- The cause of the breach, and whether or not it has been contained, will be identified – ensuring that the possibility of further loss/jeopardising of data is eliminated or restricted as much as possible.
- The Headteacher will consider any immediate actions necessary to mitigate the risks associated with the breach.
- The Headteacher will determine whether any amendment to school policy or further staff training is required to prevent a recurrence.
- In the event of an IT breach the school will work with the third-party provider to provide an appropriate response to the attack, including any in-house changes. Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups. The school will also take steps to prevent further data loss, if necessary.
- Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the school, as Data Controller, will inform the police of the security breach.

ACTION TO BE TAKEN IN THE CASE OF A MAJOR BREACH

- The Headteacher will decide whether the breach should be referred to the DPO. If a large number of people are affected, or there are very serious consequences, the DPO will be notified.
- The Data Protection Officer, Judicium Consulting Ltd, can be contacted as follows:
  Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
  Email: dataservices@judicium.com
  Telephone: 0345 548 7000 option 1 then option 1 again

- The DPO will investigate the reported breach which has occurred. The DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions).
- The DPO will keep the Headteacher informed of the outcome of their investigation.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

- Where a breach is likely to result in significant risk to the rights and freedoms of individuals, the DPO will advise the school to notify those concerned directly with the breach.
- If it is likely that there will be a risk to people's rights and freedoms, the DPO will report the data breach to the Information Commissioner's Officer within 72 hours.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions will be stored in the school's **Data Breach Log** on the school's network.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible: the categories and approximate number of individuals concerned and the approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts, cause and effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored in the Data Breach Log on the school's network.
- The DPO and headteacher will meet, as soon as reasonably possible, to review what happened and how it can be stopped from happening again. The school will take action to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

The school takes its duties under UK data protection law seriously. The Headteacher may issue disciplinary sanctions to a pupil in accordance with the school's Behaviour Policy or to a member of staff under the school's Disciplinary Code of Conduct in situations where data has been shared with malicious intent.

Please see the Breach Management Flowchart in **Appendix 2** for actions to be taken in the event of a breach.

EVALUATION AND RESPONSE

The school, as Data Controller, will establish the root of the breach and where any present future risks lie.
The Headteacher will identify any weak points in existing securing measures and report on findings and, with the approval of the Governing Board, take steps to improve levels of security and training.

ACTIONS THE SCHOOL WILL TAKE FOR WHERE SENSITIVE PERSONAL DATA IS BREACHED (INCLUDING SAFEGUARDING RECORDS)

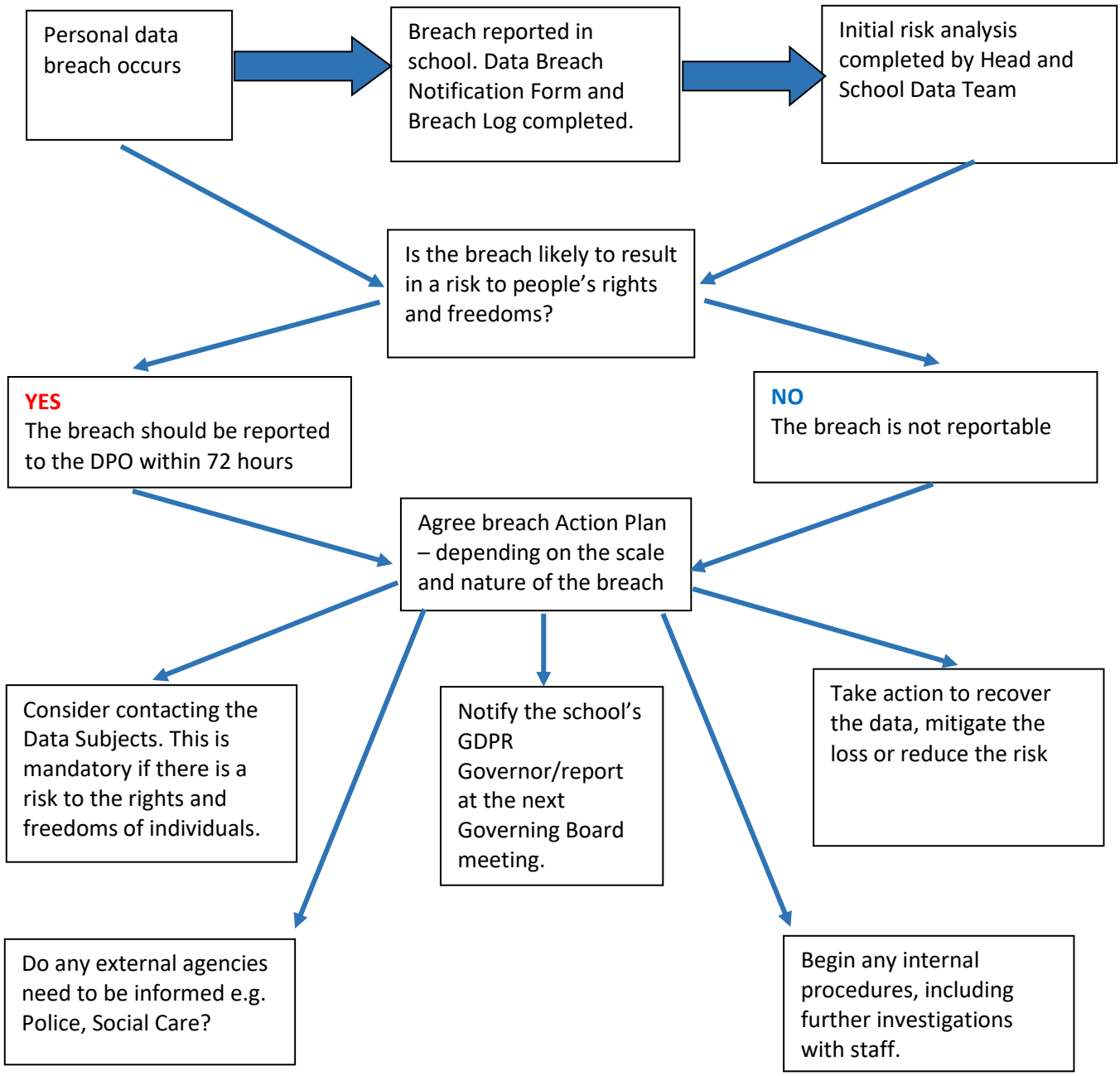
- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must notify the Headteacher or Deputy in their absence and attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the Headteacher or Deputy in their absence as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the Headteacher or Deputy in their absence will ask the school's outsourced IT provider to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence).
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the Headteacher or Deputy in their absence will consider whether it is appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The Headteacher or Deputy in their absence will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- The Headteacher or Deputy in their absence will carry out an internet search to check that the information has not been made public; if it has, the school will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- If safeguarding information is compromised, the Headteacher as designated safeguarding lead, in consultation with the DPO where deemed necessary, will decide whether to inform any, or all, of its 3 local safeguarding partners, namely:
  - Senior representatives from the local authority e.g. Single Point of Contact (SPOC), Local Authority Designated Officer) LADO
  - The Police
  - The Clinical Commissioning Group

Appendix 1 - Data Breach Notification Form

DOWNSVIEW PRIMARY & NURSERY SCHOOL - DATA BREACH NOTIFICAITON FORM	
Section A: To be completed by person reporting the breach	
Data Breach Reported by:	
Date and Time the incident occurred:	
Date and Time Headteacher (or Deputy) notified	
Summary of the event and circumstances:	Include when, what, who was affected
Approximately how many data subjects have been affected?	
Does the breach involve electronic or paper copied documents:	
Type and amount of personal data: provide title or name of the documents and what personal information is included	
Detail any actions taken by recipient when they inadvertently received the information, if known	
Have you taken any action to minimise/mitigate the effect on the data subjects involved? If so, please provide brief details. Has the information been retrieved?	
Breach reported to:	
Print Name:	
Contact Email Address:	
Signed (by person reporting the breach)	
Please hand this form to the Headteacher, or Deputy Headteacher in their absence as soon as you become aware of the breach.	
Section B: to be completed by the Headteacher	
Summarise details of the investigation into the incident	
If a MINOR BREACH, Is any further action required to mitigate risks, e.g. staff training?	
If a MAJOR BREACH, has the Data Protection Officer (DPO) been contacted?	
Date and time reported to DPO:	
Will the DPO be reporting the breach to the ICO?	
Has the breach been recorded	

on the school's Data Breach Log?	
Date reported to Governing Board	
Signed(Headteacher)	

Appendix 2 Breach Management Flowchart



Fulfil any communication and updating obligations or agreements with the relevant parties e.g. ICO and the Data Subjects.