D'OVERBROECK'S

DATA BREACH POLICY AND PROCEDURE

Policy Statement

d'Overbroeck's holds large amounts of personal and sensitive data.

Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This breach procedure applies to all personal and sensitive data held by d'Overbroeck's. This procedure applies to all School staff including volunteers, contractors and governing bodies which are referred to as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at d'Overbroeck's if a data protection breach takes place.

Legal Context

Data security is a cornerstone of the EU General Data Protection Regulation (GDPR). The sixth data protection principle – the integrity and confidentiality principle – requires us to take appropriate technical and organisational measures to process personal data in a manner that ensures appropriate security including protection against:

- Unauthorised or unlawful processing; and
- Accidental loss, destruction or damage.

Types of Breach

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Data protection breaches could be caused by a number of factors. Some examples are:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error, such as accidental deletion or alteration of data or sending data to the incorrect recipient;
- Unforeseen circumstances such as fire or flood;
- Deliberate attacks on systems, such as hacking, viruses or phishing scams, and;
- 'Blagging' offences where information is obtained by deception.

STEP ONE: Immediate Containment/Recovery

On discovery of a data protection breach, the following steps should be followed:

1. **Inform the Principal or nominated representative.** The person who discovers/receives a report of a breach must immediately inform the Principal or, in their absence, either of the Deputy Principals or Bursar. If the breach occurs or is discovered outside normal working hours, this person should nevertheless take all practical steps possible to inform the Principal or nominated representative as soon as possible.

2. **Containment and recovery.** The Principal (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT Manager. The Principal will also immediately inform the police 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.

3. **Assess and record.** The Principal (or nominated representative) must inform the Chair of Governors as soon as possible and undertake a detailed investigation of the breach and enter the incident on the data breach register. As a registered Data Controller, it is the School's responsibility to take the appropriate action and conduct any investigation. Further information on investigations can be found in the Investigation section (below).

4. **Notify the Information Commissioner's Office (ICO).** Notification is not required where the breach is unlikely to result in a risk to the rights and freedoms of individuals. Further information on ICO notification can be found in the Notification section (below).

5. **The Principal (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage.** Steps might include:

    a. Attempting to recover lost equipment.

    b. Contacting the relevant staff, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned.

    c. Consideration should be given to a global email to all school staff.

    d. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details (if possible) and confirm that they will ring the individual making the enquiry back. Whatever the outcome of the call, it should be reported immediately to the Principal (or nominated representative).

    e. Contacting the School's Marketing Department so that they can be prepared to handle any press enquiries. The Marketing Department can be contacted by telephone on 01865 688650 or via email at marketing@doverbroecks.com

    f. The use of back-ups to restore lost/damaged/stolen data.

    g. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

    h. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

STEP TWO: Investigation

In most cases, the next stage would be for the Principal (or nominated representative) to fully investigate the breach as a matter of urgency. The Principal (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections are in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, parents, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency and, wherever possible, within 5 days of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

STEP THREE: Notification

The School may have already notified the ICO and/or police as part of the initial containment. However, this decision to notify the ICO will normally be made once an investigation has taken place. The Principal (or nominated representative) should, after seeking expert or legal advice, decide whether anyone should be notified of the breach. Every incident should be considered on a case by case basis. The following points will help you to decide whether and how to notify:

Should the School notify the ICO and/or affected individuals?

- Are there any legal or contractual requirements to notify?
- Will notification help prevent the unauthorised or unlawful use of personal data?
- Could notification help the individual(s) affected – could they act on the information to mitigate risks?
- How are individuals affected? This can include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised.
- If a large number of people are affected, or there are very serious consequences, the School must notify the ICO. The ICO should only be notified if personal data is involved. There is guidance available from the ICO website and helpline on when and how to notify the ICO.

- If a breach is likely to result in a high risk to the rights and freedoms of individuals, the School must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.
- Consider the dangers of over-notifying. Not every incident warrants notification and over-notification may cause disproportionate enquiries and work.

How to notify the ICO and affected individuals

- If the School decides to notify the ICO, it must report the breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If the School takes longer than this, it must give reasons for the delay.
- The notification should include a description of how and when the breach occurred, what data was involved and how many individuals are affected. The School should include details of what it has already done to mitigate the risks posed by the breach. Further information on what to include in a notification can be found on the ICO's website.
- When notifying individuals, give specific and clear advice on what they can do to protect themselves and what you are willing to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure).

If the School does not notify the ICO

- If the School decides not to notify the ICO, it must still record that decision and the reasons for it.

STEP FOUR: Review and Evaluation

The Principal (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be written and sent to the next available Headsforum (Management Team) meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance. Consideration should be given to reviewing this breach procedure whenever the Data Protection Policy is reviewed.

Advice and Assistance

The Data Compliance Administrator is responsible for data protection compliance within the School. If you have any questions or comments about the content of this policy or if you need further information, you should contact the Data Compliance Administrator (Heather Bates) by calling 01865 688621 or emailing heather.bates@doverbroecks.com.

*

Last reviewed: 22 May 2018