DATA BREACH POLICY

College Name:	Coulsdon Sixth Form College
College DPO Contact Details:	Data Protection Lead and Officer dpo@coulsdon.ac.uk
Name of Document (DP1):	Data Breach Policy
Topic:	GDPR – Data Breach Policy
Date:	25 May 2018
Version:	1

DATA PROTECTION POLICY
Approved by:
Date approved:
Responsibility Member of SLT: *Assistant Principal Curriculum & Quality*
Review date: August 2019

1. **This policy outlines Coulsdon Sixth Form College processes and procedures in the event of the following data breaches as listed below;**

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

2. **In the event of such breach; The DPO will;**

    - alert the Principal and the chair of Governors,
    - make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
    - assess the potential consequences, based on how serious they are, and how likely they are to happen
    - 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:
        a. Loss of control over their data
        b. Discrimination
        c. Identify theft or fraud
        d. Financial loss
        e. Unauthorised reversal of pseudonymisation (for example, key-coding)
        f. Damage to reputation
        g. Loss of confidentiality
        h. Any other significant economic or social disadvantage to the individual(s) concerned
        i.

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

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 are stored on the designated college computer drive set up for GDPR purposes.

3. **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
    - The categories and 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 and cause
    - 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 on the designated college computer drive set up for GDPR purposes.

- The DPO and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

4. Actions to minimise the impact of data breaches

Coulsdon College will take the actions set out below 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.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must 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 DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the Information Technology (IT) department to recall it
- In any cases where the recall is unsuccessful, the DP and/or member of staff who sent the data will 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 DPO will ensure the college receives a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, the college will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach that the college may consider a breach would include:

- Details of pupil premium interventions for named students published on the college website
- Non-anonymised candidate exam results or staff pay information being shared with governors
- A stolen or hacked College laptop containing non-encrypted sensitive personal data
- The college's cashless payment provider being hacked and parents' financial details stolen

It is advisable that you do not contact the Information Commissioner's Office with a complaint until you have exhausted the process with our DPO lead. However, if you feel we have not addressed any concerns you may have, you have the right to contact the Information Commissioner's Office at https://ico.org.uk/concerns/.

Further Information

If you would like to discuss anything in the Data Breach Policy, please contact: dpo@coulsdon.ac.uk

DISCLOSURES

We will advise you at the time, should we wish to disclose your personal data to any other appropriate third party (i.e. new contractors/partners), and this policy will be updated.