# Ken Stimpson Community School

## Data Protection Breach Policy

Last Reviewed:- May 2018

# Policy Cover Sheet

| | |
|---|---|
| Document Name: | Data Protection Breach Policy |
| Type of document: | Policy |
| Purpose of document: | This document outlines the Data Protection Breach policy adhered to by Ken Stimpson Community School to comply with UK Law |
| Intended audience: | Students, Staff, Parents & third parties |
| Document lead/author | Lee Chambers, Technical Services Manager |
| Issue date: | May 2018 |
| Dissemination Method: | Published on website |
| Reviewer: | Technical Services Manager/Data Protection Officer |

# Contents

Policy Cover Sheet ..... 2
1. Introduction ..... 4
2. Aim ..... 4
3. Definition ..... 4
4. Scope ..... 5
5. Reporting an incident ..... 5
6. Procedure ..... 5
7. Conclusion ..... 7
8. Complaints ..... 7
9. Reviews & Updates to this policy ..... 7
10. Contact us ..... 7

## 1. Introduction

Data security breaches are increasingly common occurrences whether these are caused through human error or via malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached.
The School needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect its information assets as far as possible.

## 2. Aim

The aim of this policy is to standardise the School wide response to any reported data breach incident and ensure that they are appropriately logged and managed in accordance with best practice guidelines. By adopting a standardised consistent approach to all reported incidents, it aims to ensure that:

- Incidents are reported in a timely manner and can be properly investigated
- Incidents are handled by appropriately authorised and skilled personnel
- Appropriate levels of School management are involved in response management
- Incidents are recorded and documented
- The impact of the incidents is understood and action is taken to prevent further damage
- Evidence is gathered, recorded and maintained in a form that will withstand internal and External scrutiny
- External bodies or data subjects are informed as required
- The incidents are dealt with in a timely manner and normal operations restored
- The incidents are reviewed to identify improvements in policies and procedures

## 3. Definition

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

An incident in the context of this Policy 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 School's information assets and/or reputation

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

- Loss or theft of confidential or sensitive data or equipment on which such data is stored
- (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)
- Equipment theft or failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error

- 'Blagging' offences/Social Engineering where information is obtained by deceiving the organisation who holds it

## 4. Scope

This School wide policy applies to all School information, regardless of format, and is applicable to all staff, students, visitors, contractors and data processors acting on behalf of the School. It is to be read in conjunction with the School's Data Protection Policy

## 5. Reporting an incident

- Any individual who accesses, uses or manages the School's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer & if appropriate, ICT Services

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

- The report will 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.

- All staff should be aware that any breach of the Data Protection Act may result in the School's Disciplinary Procedures being instigated.

## 6. Procedure

- The DPO will investigate the report, and determine whether a breach has occurred. To decide, 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

- If necessary, The DPO will alert the headteacher and the chair of governors

- 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

If it's 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 schools IT 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
    - 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 Schools IT Network

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

## 7. Conclusion

Reporting potential or confirmed data protection breaches is the responsibility of all members of the school. Failure to report may result in access to School facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy would be taken up with the data controllers.

## 8. Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the reporting may be referred to the information Commissioner (The Statutory regulator)

## 9. Reviews & Updates to this policy

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice.

## 10. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this Policy, please contact our data protection officer.