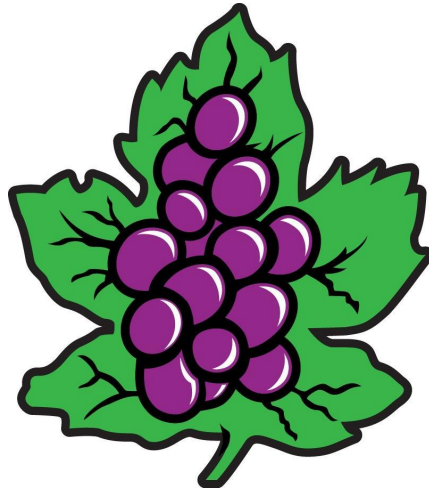




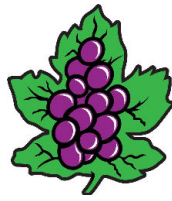
DATA BREACH POLICY

Kerem School

Approved by:	Safeguarding and Wellbeing Committee	Date: September 2021
---------------------	---	-----------------------------

Last reviewed on:	August 2026
--------------------------	--------------------

Next review due by: August 2027
--



KEREM SCHOOL

(This policy also applies to the Early Years Foundation Stage)

Data Breach Policy and procedure

Policy Statement

Kerem School holds large amounts of personal and sensitive data. Every reasonable care is taken to protect this 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 Kerem School and to all school staff, governors, volunteers, and contractors, referred to hereinafter as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Kerem School if a data protection breach takes place.

Types of Breach

Data protection breaches could be caused by a number of factors including:

- 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
- Poor data destruction procedures
- Human Error
- Cyber-attack
- Hacking
- 'Blagging' offences where data is obtained by deception

Managing a Data Breach

In the case of a personal data breach, the staff member must immediately inform the Head Teacher of the personal data breach. Should the Head Teacher not be available, you will be directed to one of the Deputy Head Teachers.

- The Head Teacher will investigate the report and determine whether a breach has occurred. To decide, the Head Teacher 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.
- The Head Teacher will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

Investigation

In most cases, the next stage would be for the Head Teacher (or nominated representative) to fully investigate the breach. The Head Teacher (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 were 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, 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. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Steps to be Taken Following Investigation

- The Head Teacher will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The Headteacher will work out whether the breach must be reported to the Information Commissioner's Office (ICO). This must be judged on a case-by-case basis. To decide, the Head Teacher 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
 - Identity 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 the ICO must be notified, the Headteacher will do this via the [‘report a breach’ page of the ICO website](#) within 72 hours.

The Headteacher 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.

The Head Teacher will alert the Chair of Governors.

The Headteacher will assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Headteacher 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 Head Teacher

- A description of how and when the breach occurred and what data was involved
- 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
- Specific and clear advice on what they can do to protect themselves and what the School is able to do to help them
- Details of how they can make a formal complaint if they wish (see the School's Complaints Procedure)

The Head Teacher will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks, or credit card companies.

Documenting the Breach

The Head Teacher 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)

Implementation

The Head Teacher should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision, and ongoing training. See Appendix 1 regarding guidelines for staff to best avoid a data breach. If staff have any queries in relation to the policy and associated procedures, they should discuss this with their line manager or the Head Teacher.

Appendix 1

Guidelines for teachers to help avoid a data breach

Please remember that in addition to all good practice guidelines, Kerem School is housed in a public building that is accessed outside of school hours.

- Ensure that your school iPad is password-protected
- Ensure that chosen passwords are strong (they must contain a mixture of upper and lower case letters plus at least 1 number) e.g. Rand0m7
- Ensure that you use two-factor authentication to log onto your laptop
- Ensure you have signed out of your email
- Ensure you have logged off your computer/closed your laptop
- Ensure you have put away any papers that you have been working on or that are on your table that contain any personal, identifiable information about pupils or staff
- Do not leave any school papers in a car