Data Breach Policy

This policy has been written with guidance from DfE Data protection: a toolkit for schools

Owner: NA/**W**AA/**K**LF/**6**NA

Date Created	Date 1st Review Due	Date Reviewed	Version	Next Review Due
May 2018	May 2019	May 2019	2	May 2020
		October 2020	3	October 21
		February 2021	4	February 2022

Definition

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Note: it is more than just the loss or theft of personal data.

A data breach is likely to have significant detrimental effect on individuals - eg. discrimination, damage to reputation, financial loss, loss of confidentiality, or social disadvantage - or pose a risk to any other right or freedom.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

If a personal data breach has occurred, The Green Room will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we will notify the ICO within 72 hours; if it's unlikely then we don't need to report it. However, in order to be able to justify this decision, it will be documented in the Data Breach Log

Minimising the risk of a data breach.

- Staff are permitted to take photos of pupils providing we have obtained parental consent, however the photo must be uploaded to the Google drive and deleted from the phone by the end of the day.
- All communication regarding pupils must use initials rather than full name.
- All staff have their own login and password for Arbor and Google and we are able to view actions taken by individual staff.
- All devices have a screen password.
- Many data breaches occur via 'innocent mistakes'/human error, and unintended misuse of technology. The Green Room has withdrawn the use of memory sticks/flash drives to store or transfer personal data to mitigate risk.
- All files sent containing sensitive information which are sent to a third party are password protected or shared securely via Google.
- Paper records are kept to a minimum and kept in a locked environment. They are shredded once no longer needed.
- Staff regularly update computer software; employ strong passwords; use anti-virus software, use encryption, and do not leave computers unlocked to prevent external hackers from gaining access to data.

The Green Room response if a data breach occurs:

- All personal data breaches will be captured, categorised and reported in accordance with defined procedures and all breaches or suspected breaches will be immediately reported to the Data Protection officer who will determine the nature, severity and level of risk associated with the breach/suspected breach and ensure that appropriate advice and actions are taken
- All personal data breaches or suspected breaches will be categorised and reported using the Data Breach Log
- All data breaches will be contained and remedied as soon as possible, and where necessary all appropriate data subjects will be informed of the data breach
- All personal data breaches will be reported to any other appropriate regulatory body in accordance with legal requirements
- Corrective and preventive actions will be implemented and communicated following investigations known or suspected personal data breaches

Reporting a Data Breach

When reporting a breach, the UK GDPR says The Green Room must provide:

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
- the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

How to notify the ICO

Serious breaches should be reported to the ICO using the DPA security breach helpline on 0303 123 1113 (open Monday to Friday, 9am to 5pm). Speak to staff who will record the breach and give you advice about what to do next.

If you would like to report online please visit the Data Breach Reporting page on the ICO website to download the Personal Data Breach Reporting form and guide to filling it in. If this is an initial report please send to icocasework@ico.org.uk or send by post to the office address Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

What information must we provide to individuals when telling them about a breach?

The Green Room will describe in clear and plain language, the nature of the personal data breach and, at least:

- A description of the incident

- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

This policy is used in conjunction with the Data Breach Log and the Data Protection Policy.

This policy is approved by the Co-CEO of The Green Room School.

Date:

Co-CEO:
