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
		February 2022	5	February 2023
		January 2023	6	January 2024
		January 2024	6	January 2025
		January 2025	7	January 2026
		January 2026		January 2027

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.

All personal data breaches, regardless of severity, will be recorded in the Data Breach Log including the nature of the breach, potential or actual impact on individuals, and the decision on whether to notify the ICO.
The Data Protection Officer (DPO) will assess the likelihood and severity of risk to individuals' rights and freedoms. If a risk is likely, the breach will be reported to the ICO within 72 hours. Even breaches not requiring ICO notification will be documented along with the rationale for non-reporting.

Minimising the risk of a data breach.

- Staff are permitted to take photos of students providing we have obtained parental consent. GRW/GRC/GRK: all photos of the students are to be taken with The Green Room mobile.
- All communication regarding students 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.
- CPOMS is password protected and access to data is restricted to safeguarding personnel only.
- 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 The Green Room has withdrawn the use of memory sticks/flash drives to store or transfer personal data to mitigate risk.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 personal data breaches should be reported to the ICO primarily through their **online breach reporting portal.** Alternative methods (phone or post) may be used if necessary. Reports should include the required information as outlined in UK GDPR Article 33, including categories of personal data affected, number of individuals affected, and measures taken to mitigate harm.

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

The Green Room will provide affected individuals with a **clear and plain-language explanation** of the breach, including:

- A description of the incident
- Contact details of the DPO or other contact point
- Likely consequences or risks arising from the breach
- Steps already taken or planned to mitigate risks
- Recommended actions for individuals to protect themselves (e.g., changing passwords, monitoring accounts, reporting suspicious activity)

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

This policy is approved by the CEO of The Green Room Foundation.

Date:

CEO:
