Hatfield Community Free School, Briars Lane, Hatfield, Herts, AL10 8ES
Website: www.hcfs.org.uk **Telephone:** 01707 276018 **Email:** office@hcfs.org.uk

@hatfieldcfs1 @hatfieldcfs

Principal: Mrs Victoria Hobson

UK GDPR Data Breach Response Policy

September 2025

To be reviewed annually in the Autumn Term

Next Review: September 2026

History of Document

Issue No.	Date Issued	Prepared By	Approved By	Comments
Issue 1	Sept 2021	J Sutton		
Issue 2	September 2023	Victoria Hobson	Trust Board	Updated with minor changes to match the model policy from HfL Education
Issue 3	September 2024	Victoria Hobson	Trust Board	No updates required
Issue 4	September 2025	Jonathan Durbin	Trust Board	Re-written using latest templates from The Key. To be read in conjunction with UK Personal data breach procedure September 2025

1. Purpose

This policy sets out how Hatfield Community Free School will respond to personal data breaches, in line with the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018. Its aim is to ensure prompt and effective action to protect individuals' data and the school's reputation.

2. Scope

This policy applies to all staff, governors, contractors, volunteers, and anyone else processing personal data on behalf of the school.

3. Definition of a Data Breach

A data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Examples:

- Sending personal data to the wrong recipient
- Losing a laptop or USB stick with unencrypted data
- Hacking, malware or ransomware attacks
- Accidental deletion of files containing personal data

4. Roles and Responsibilities

- Data Protection Officer (DPO): Jonathan Durbin sbm@hcfs.org.uk – leads the response, investigation, and notification process.
- All Staff: Must report any suspected breach immediately to the DPO.
- Headteacher & SLT: Support the investigation and communication process.

5. Procedure

a) Identifying and Reporting a Breach

- Any member of staff who discovers or suspects a data breach must report it immediately to the DPO (or nominated lead if DPO is unavailable).
- Use the school's Data Breach Reporting Form (see template below).

b) Containment and Recovery

- DPO (or lead) will assess the breach and take steps to contain it, e.g. revoke access, recover lost data, isolate affected systems.
- Engage IT support if needed (Interm).

c) Assessment of Risk

- Assess the potential impact on individuals, including likelihood and severity of harm.

- Consider what type of data is involved, how many individuals are affected, and the risk of further disclosure.

d) Notification

- If the breach is likely to result in a risk to individuals' rights and freedoms, notify the Information Commissioner's Office (ICO) within 72 hours.
- If high risk, affected individuals must also be informed without undue delay.
- All actions and decisions must be documented.

e) Review and Lessons Learned

- After containment, the DPO will review the breach, identify causes, and make recommendations to prevent recurrence.
- Update policies/training as needed.

6. Record Keeping

- All data breaches, regardless of severity, must be recorded using the Data Breach Reporting Form (see below).

7. Training and Awareness

- All staff will receive regular training on data protection and breach response. Reminders will be issued annually and when updates are made.

8. Policy Review

- This policy will be reviewed annually or following a significant breach or change in legislation.

Appendix A - Data Breach Reporting Form

Date/Time	Reporter Name	Nature of Breach	Personal Data Involved	Individuals Affected	Containment Steps	DPO Actio

-