Victorious Academies Trust
Success in education

Data Protection Framework	
Policy Ref:	HR 008
Purpose	
Committees	Trust Finance Business and Audit Committee
Other linked policies	Privacy Notice (Pupils), Privacy Notice (Workforce), Retention Schedule, Social Media Policy, Bring Your Own Device (BYOD) Policy, ICT Acceptable Use Policy, Off Site Working Policy, CCTV Policy, Privacy Notice (Governors), Special Category Data Policy, Information Policy, Remote Learning Policy
Issue date:	June 2026
Review Date	June 2027

Contents of this Framework (related documents)

Data Protection Policy
- i. Annex 1: Legal Conditions for Processing
- ii. Annex 2: Breach Procedure
- iii. Annex 3: Data Protection Impact Assessment Procedure
- iv. Annex 4: Subject Access Request Procedure
- v. Annex 5: Freedom of Information Request Procedure
- vi. Annex 6 Data Protection Complaints Policy

FOI Publication Scheme
Privacy Notice (Pupils)
Privacy Notice (Workforce)
Retention Schedule
Social Media Policy
Bring Your Own Device (BYOD) Policy
ICT Acceptable Use Policy
Off Site Working Policy
CCTV Policy (where appropriate)
Privacy Notice (Governors)
Special Category Data Policy
Remote Learning Policy
Artificial Intelligence Policy
AI Strategy
Pupil Guide to AI Use
Photo Policy

Introducing our Data Protection Framework

1. This framework comprises of a number of key documents; including our Data Protection policy and other associated policies and procedures, which together form our Trust school's commitment to protecting the data of its pupils, families, staff and volunteers.

2. Compliance with this framework is mandatory for all staff.

"

3. Personal data" means any information where a living person is either identified or identifiable, from the information alone, or with other information – these are known as Data Subjects. Personal data can include written information, pupil work, photographs, CCTV and film footage or voice recordings, in electronic format (which can include in Social Media, apps, databases or other electronic formats) or hard copy (including copies printed from electronic sources, and handwritten data when it is part of a filing system, or intended to be filed).

4. "Special category data" is personal data that needs more protection because it is sensitive.

Victorious Academies Trust
Success in education

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning physical and mental health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

5. In addition, the DfE advises that Pupil Premium/FSM status is treated as Sensitive Data

6. "Data Subjects" include our pupils, staff, contractors, parents (and family), local authority contacts, and anyone else we might come into contact with.

7. "Data Controller" means the school, alone or jointly with other Data Controllers, that decides on why and how personal data is processed.

8. "Processing" means collecting, storing, using, sharing and disposing of data.

9. "Processors" are the external bodies who processes personal data on behalf of the controller.

10. "Staff" includes current or former; permanent employees, temporary staff, agency staff, consultants, governors, volunteers, and anyone else working for the school. We will also expect job applicants and contractors (and their staff) to comply with this policy.

11. "Data Protection Officer" (DPO) is a statutory role with responsibility for:
    - advising schools about data protection obligations;
    - dealing with breaches, including suspected breaches and identified risks; and
    - monitoring compliance with this policy.

12. Our Data Protection Officer is: [Education Data Hub (CDDS Children's Services) | Children's Services | Derbyshire County Council | County Hall, Matlock, Derbyshire DE4 3AG | 01629 532888 dpforschools@derbyshire.gov.uk]

13. "Data Protection Lead" across our Trust is Nicky Wise and is the member of school staff nominated to manage communication with the DPO.

Responsibilities

14. All staff are responsible for:
    - reading and understanding this framework before carrying out tasks that involve handling personal data,
    - following this framework,
    - reporting any suspected breaches of it to our Data Protection Officer.

15. All leaders are responsible for ensuring their team sign to confirm they have read, understood and will comply with the documents in this framework, before carrying out tasks that involve handling personal data, including reporting any suspected breaches of it.

Data Protection Legislation and Regulator

16. Relevant legislation includes but is not limited to:
    - UK General Data Protection Regulation (UK GDPR);

- Data Protection Act 2018 (DPA 2018), which enacts the GDPR in the UK and includes exemptions and further detail, as well as offences that individuals can be prosecuted for;
    - Privacy and Electronic Communications Regulations (PECR), which cover electronic direct marketing ("marketing" includes fundraising and promoting an organisation's aims, not just selling.)
    - Freedom of Information Act 2000, which provides key definitions referred to in the other legislation.
    - Human Rights Act 1998
    - Computer Misuse Act 1990, which covers unauthorised access to, and use of, computers and computer materials.
    - Protection of Freedoms Act 2012
    - Data (Use and Access) Act 2025

17. In the UK, the Information Commissioner's Office (ICO) is the data protection regulator.

18. Breaches of data protection legislation can cause the risk of real harm to people whose data is handled in an unfair or unlawful way, as well as significant monetary penalties and damage to reputation.

19. Individual members of staff may be prosecuted for committing offences under Sections 170, 171 or 173 of the DPA 2018. These offences are: obtaining, disclosing, altering or retaining data without the authority of the Data Controller; purposefully identifying people from data that has been "de-identified"; and purposefully withholding data that a data subject has requested, and is entitled to receive.

Monitoring and review

20. This policy will be reviewed on an **annual basis**, or when new legislation/guidance regarding the subject is published and requires the approval of the **Trust board**.

End