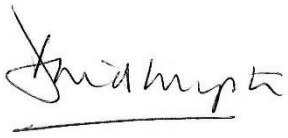
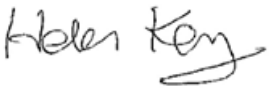
Chailey School

Data Protection Policy

Date of Governing Body's Approval: **8th March 2017**

Chair of Governors: 

Headteacher: 

Date Due For Review: **March 2018**

Relevant legislation

- Computer Misuse Act (1990) (http://www.legislation.gov.uk/ukpga/1990/18/contents)
- Copyright Design & Patents Act (1988) (http://www.legislation.gov.uk/ukpga/1988/48/contents)
- Data Protection Act (DPA) (1998)(http://www.legislation.gov.uk/ukpga/1998/29/contents)
- Freedom of Information Act (FOIA) (2000) (http://www.legislation.gov.uk/ukpga/2000/36/contents)
- Police & Justice Act (2006) (http://www.legislation.gov.uk/ukpga/2006/48/contents)
- Regulation of Investigatory Powers Act (2000) (http://www.legislation.gov.uk/ukpga/2000/23/contents)

Purpose
To ensure that:

- all aspects of data use at Chailey School conform to the relevant legislation
- there is no detriment to data subjects and the integrity and security of data is preserved
- data is used effectively and for the described purpose
- e-safety responsibilities are clear and best practice is followed by all stakeholders

Principles
The school believes in the welfare of data subjects and the handling of data with caution, confidentiality and sensitivity. It will therefore comply fully with the DPA's "Data Protection Principles", which state that personal information must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than is necessary
- Processed in accordance with an individual's rights
- Kept securely
- Not transferred without adequate protection

In addition the school will ensure that:

- E-safety is treated as both a child protection issue (rather than an ICT issue) and a partnership concern, not limited to school premises, equipment or hours. Internet access is filtered and monitored and the Senior Leadership Team and Pastoral Leadership Team oversee best practice.
- Appropriate protection is in place to protect the computer network against unauthorised intrusion or malicious software, and data is regularly backed up to ensure business continuity.
- Data held on the network is protected by appropriate access permissions, and storage areas for sensitive data and equipment are physically secured.
- Accurate inventories are maintained of software/hardware and unauthorized software/hardware is prohibited.
- Security is regarded as paramount in the procurement, implementation and development of new systems.
- Users are made aware that the school reserves the right to monitor any information on the network for auditing, maintenance and security purposes.

Detail
Data protection and e-safety are closely linked and the reference should be made to the School's policies on E-Safety and Social Media for further information. As new technologies come into use, best practice may change rapidly and therefore these operational documents may be updated as circumstances require, within the principles of this policy but without the need for further consultation.

Roles and Responsibilities
The **Governing Body** is responsible for reviewing the policy annually.

The **Headteacher**
- has shared responsibility with the School Business Manager and Learning Resources Manager for data security and integrity
- has shared responsibility with the School Business Manager for notifying the Information Commissioner's Office under the DPA

The **Deputy Headteacher (Student Support and Development)**
- is the designated E-Safety Officer

The **Learning Resources Manager**
- has shared responsibility with the Headteacher for data security and integrity
- has overall responsibility for managing the network and monitoring compliance with the procedures detailed above

The **Data Manager**
- is responsible for issuing the annual privacy notice and ensuring that it is published on the school website
- will determine access rights to the different SIMS modules and ensure their effective operation
- is responsible for ensuring the security of all data held on the SIMS system

Staff and other authorised users (e.g. PGCE students, Governors)
- must follow the procedures detailed above

Staff, **Students** and other authorised users (e.g. PGCE students, Governors)
- must sign and follow the Acceptable Use Policy and Social Media Policy

Parents and carers
- must provide the school with up-to-date information as appropriate and when requested
- must ensure that the data they supply to the school is accurate

Failure to follow the procedures or Acceptable Use Policies (AUPs) referred to above may lead to sanctions, disciplinary action or the involvement of the police or local authority.

Monitoring and Evaluation
This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments made to the relevant legislation. The Governing Body will monitor the effectiveness of the policy and review it annually as part of their cycle of Policy Review.

Related documents
Privacy Notice
E-Safety Policy
Social Media Policy
Acceptable Use Policy