



Data Protection Policy

Draft prepared by: Sarah Fleming

Agreed by governing body: February 2016

Signed

Chair of Governors:

Headteacher:

A handwritten signature in black ink, appearing to be 'M. S. S.', written over the 'Chair of Governors:' line.

Introduction, aims, purpose of policy

The Data Protection Act 1998 provides protection for personal data kept in school - the school admission register, attendance registers, pupils' curricular records, assessment data, class lists, reports to parents, pupils' disciplinary records, school personnel files, school financial information, school strategic and school improvement plans, recorded CCTV footage, pupils' family and home contact details, records of contractors and suppliers and records of pupils entering public examinations.

The school will ensure that under the Data Protection Act 1998 all school personnel are able to access their personal data that is held about them within a maximum of 40 days.

The school will ensure that a pupil's educational records will be made available to their parents or carers on receipt of a written request within 15 school days.

The school aims to fulfill its obligations under the Data Protection Act 1998 and to protect the right of school personnel and pupils to privacy in line with the Act.

Policy summary

- To allow all school personnel their right to have access to their personal data.
- To allow all parents their right of access to their child's records.
- To protect all school personnel's right to privacy in line with the Data Protection Act 1998.
- To protect all pupils right to privacy in line with the Data Protection Act 1998.

Please also refer to the following policies and documents

- Grievance Procedure
- eSafety Policy
- Freedom of Information Act

Contents

p.3	Role of the Governing Body
p.3-4	Role of the Headteacher
p.4	Role of the nominated governor
p.4	Role of school personnel
p.4	Data protection principles
p.5	Security measures
p.5	Disclosure of data
p.5	Requests for access to data
p.5	Rights of individuals
p.5	Grievance procedure
p.5	Rights of parents, carers and pupils
p.6	Training

The school believes that this policy relates to the following legislation:

- EC Convention on Human Rights and Fundamental Freedoms 1950
- Rehabilitation of Offenders Act 1974
- Access to Medical Records 1988
- Data Protection Directive 95/46/EC
- Asylum and Immigration Act 1996
- Employment Rights Act 1996
- Data Protection Act 1998
- Human Rights Act 1998
- Public Interest Disclosure Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) Regulations 2000
- Protection of Freedoms Act 2012

Role of the Governing Body

The Governing Body has:

- the responsibility to comply with the legal requirements of the Data Protection Act 1998;
- the responsibility to ensure data is processed in accordance with the eight principles of the Data Protection Act 1998;
- delegated powers and responsibilities to the Headteacher as 'Data Controller' for the school;
- delegated powers and responsibilities to the Headteacher to ensure all school personnel and stakeholders are aware of and comply with this policy;
- responsibility for ensuring that the school complies with all equalities legislation;
- responsibility for ensuring funding is in place to support this policy;
- responsibility for ensuring this policy and all policies are maintained and updated regularly;
- responsibility for ensuring all policies are made available to parents;
- nominated a link governor to visit the school regularly, to liaise with the Headteacher and to report back to the Governing Body;
- responsibility for the effective implementation, monitoring and evaluation of this policy

Role of the Headteacher

The Headteacher will:

- act as 'Data Controller' for the school;
- ensure the school complies with the Data Protection Act 1998 and the eight data protection principles;
- ensure all data is processed fairly and lawfully;
- ensure security measures and confidential systems are in place to protect personal data and pupil records;
- ensure data is obtained for specific and lawful purposes;
- ensure data is adequate, relevant and not excessive;
- ensure all personal data is accurate and that inaccurate data is corrected or erased;
- ensure that at the beginning of every academic year all school personnel will receive a copy of their personal data;
- ensure procedures are in place to deal with requests for access to personal data;
- ensure data is not kept longer than is necessary;
- ensure school personnel are aware of their rights;
- ensure school personnel are aware of their responsibilities;

- ensure a pupil's educational records will be made available to their parents or carers on receipt of a written request within 15 school days;
- ensure a Common Transfer File is sent when a pupil joins another school;
- make effective use of relevant research and information to improve this policy;
- work closely with the link governor;
- provide leadership and vision in respect of equality;
- provide guidance, support and training to all staff;
- monitor the effectiveness of this policy;
- annually report to the Governing Body on the success and development of this policy

Role of the nominated governor

The Nominated Governor will:

- work closely with the Headteacher and the coordinator;
- ensure this policy and other linked policies are up to date;
- ensure that everyone connected with the school is aware of this policy;
- attend training related to this policy;
- report to the Governing Body every term;
- annually report to the Governing Body on the success and development of this policy

Role of school personnel

School personnel will:

- comply with all aspects of this policy;
- be aware of all other linked policies;
- follow the safe and confidential system procedures that are in place to protect personal data and pupil records;
- inform the admin team of any changes in personal data e.g. address
- apply in writing for access to their personal data;
- comply and respect confidentiality of personal information at all times but especially when involved with interviewing new school personnel;
- provide accurate and up to date personal information;
- inform the school and the Local Authority of any changes to their personal data
- report and deal with all incidents of discrimination;
- report any concerns they have on any aspect of the school community

Data Protection principles

Personal data must:

- be processed lawfully;
- be obtained and processed for specific and lawful purposes;
- be sufficient, appropriate and not excessive in relation to the precise purpose;
- be accurate and up to date;
- not be kept for a great length of time;
- be processed in agreement with the individual's legal rights;
- be protected against unlawful processing, accidental loss, destruction or damage;
- not be transferred outside the EU unless the rights and freedom of the individual is protected

Security measures

We work in conjunction with the Local Authority Code of Practice to ensure that computers and servers comply with all up to date Government regulations and are secure with:

- anti-virus software;
- fire wall software;
- passwords

Password Policy

All staff have their own unique username and private password to access school systems. Passwords should be strong and kept private. Different systems will use different usernames and passwords and users are prompted to change passwords on a regular basis.

Cloud-based services

Cloud based services provide a significant number of benefits including stability and ease-of-use. At Chase Bridge we take security seriously and when choosing a cloud service provider we ensure they comply with the Data Protection Act (DPA). When complying with the DPA the supplier must make guarantees about their technical and organisational security measures.

Data

Back up data is performed by our Technical Support Provider and has a retention period of 30 days.

Personal Devices

Staff are not permitted to use personal devices to transfer or store sensitive data using non-school approved email accounts or any cloud based services. When working off-site staff will use a 2-factor authentication to remote access onto the schools network systems.

All school personnel are trained to:

- be discreet and confidential;
- consider the safe and secure positioning of computers;
- turn off computers when not in use;
- remember password access;
- lock filing cabinets and doors to offices;
- shred confidential material;
- clear their desk before they leave school

Security measures for the Governing Body

Members of the Governing Body have access to an area of the school website specifically for the purpose of accessing documents relevant to their role – access is given on a read only basis. This area is controlled by a single user name and password given to all governors, sent using the LA's secure data transfer system. Data is protected by a change to the password when a governor resigns from or leaves the Governing Body. It is the responsibility of the Clerk to initiate this change with the school.

Disclosure of data

Personal data cannot be disclosed to a third party without the consent of the individual except when it is legally required.

Requests for access to data

All requests from school personnel for access to their data must be made in writing on headed note paper and sent to the data controller, Andrew King, Headteacher.

Freedom of Information requests

All requests made under the Freedom of Information Act should be directed in writing to Andrew King, Headteacher.

Such requests may be refused for the following reasons:

- It would cost too much or take too much staff time to deal with the request.
- The request is vexatious.
- The request repeats a previous request from the same person.

Rights of individuals

Individuals have rights to:

- know when their data is being processed, the reason it is being processed and the name of the person or organisation requesting the information;
- prevent processing which could be harmful to them or others;
- prevent the processing of their performance management records;
- go to court to prevent inaccurate data being used;
- be compensated if a data controller contravenes the Data Protection Act;
- stop data being processed for direct marketing

Individuals are not entitled to:

- copies of their references;
- information on pay reviews;
- examination results until they have been released

Grievance procedure

Any member of the school personnel who disputes any aspect of their personal data with the Data Controller has the right to take up the matter under the school's formal grievance procedures.

Rights of parents, carers and pupils

Pupil's educational records will be made available to their parents or carers on receipt of a written request within 15 school days.

Pupils may also request access (in writing) to their educational records.

Training

All school personnel:

- have equal chances of training, career development and promotion
- receive training on this policy on induction which specifically covers:
 - Data Protection Act 1998
 - Freedom of Information 2000
 - Access to Personal Records
- receive periodic training so that they are kept up to date with new information
- receive equal opportunities training on induction in order to improve their understanding of the Equality Act 2010 and its implications

Appendices

The Data Protection Act 1998 <https://www.gov.uk/data-protection/the-data-protection-act>