r

Georgian Gardens C.P. School

Data Protection Policy

Autumn Term 2024

Approved by Governors Autumn 2024
Next Review Due:- Autumn Term 2025

Introduction

On the 25th May 2018 , new legislation on data protection came into force in the UK. This was then amended slightly after Brexit, so now we have "UK data protection legislation, including UK GDPR". This consists of The UK General Data Protection Regulation (UKGDPR); The Data Protection Act 2018; the Data Protection Fees regulations 2018 and the Privacy and Telecommunications Regulations (PECR) 2003 as amended 2011.

This Policy sets out the manner in which personal data of staff, students, Governors and other individuals is processed fairly and lawfully.

The School collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the School. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the School complies with its statutory obligations.

The School is the "data controller" - the legal entity responsible for the processing conducted by staff etc. The School has a Data Protection Officer appointed (the School Business Manager) who is responsible for ensuring that compliance is in place. Part of this is ensuring security of data and procedures are being followed to protect all. The School must be able to demonstrate compliance. Failure to comply with the Principles exposes the School and staff to civil and criminal claims and possible financial penalties.

The School's registration number is Z7111942. This registration is renewed annually and updated as and when necessary.

"PROCESSING DATA" can be collecting, collating, recording (either electronically or on paper) storing or appropriately disclosing data - regardless of the age of the person the data is about.

Aim

This Policy will ensure:

- The School processes personal data fairly and lawfully and in compliance with the rules set out in the legislation and school policies and procedures.
- All staff will be aware of their duties and responsibilities under this policy.
- That the data protection rights of those involved with the School community are safeguarded.
- Confidence in the School's ability to process data fairly and securely.

Scope

This Policy applies to:

- Personal data of all School employees, governors, students, parents and carers, volunteers and any other person carrying out activities on behalf of the School.
- The processing of personal data, both in manual form and on computer.

The Law

The school as a whole has a duty to ensure that all processing is "fair and lawful" – ie everyone is treated in the same manner and in line with the legislation. This policy and all other related policies/procedures have been drafted with this in mind.

Everyone has several rights under this legislation as well as "fair and lawful processing" – all the School policies and procedures have been drafted to provide guidance on this. Any queries should be directed to the Data Protection Officer.

Data Security and Data Security Breach Management

All staff are responsible for ensuring that personal data which they process is kept securely and is not disclosed to any unauthorised third parties.

Access to personal data should only be given to those who need access for the purpose of their duties.

All staff will comply with the Schools Acceptable IT use Policy.

Staff who work from home must have particular regard to the need to ensure compliance with this Policy and the Acceptable IT use Policy.

Data will be destroyed securely in accordance with the 'Information and Records Management Society Retention Guidelines for Schools'.

New types of processing personal data including surveillance technology which are likely to result in a high risk to the rights and freedoms of the individual will not be implemented until a Privacy Impact Risk Assessment has been carried out.

The School will have in place a data breach security management process and serious breaches where there is a high risk to the rights of the individual will be reported to the Information Commissioner's Office (ICO) in compliance with the GDPR.

All staff will be aware of and follow the data breach security management process.

All staff will be aware of and comply with the Do's and Don'ts in relation to data security in Appendix A.

Subject Access Requests

Requests for access to personal data (Subject Access Requests - SARs) will be processed by the Data Protection Officer. Records of all requests will be maintained.

The School will comply with the statutory time limits for effecting disclosure in response to a Subject Access Request. The statutory time limit is one calendar month from receipt of the request. The School has a basic procedure to follow in the event of receiving a request.

Sharing data with third parties and data processing undertaken on behalf of the School.

Personal data will only be shared with appropriate authorities and third parties where it is fair and lawful to do so. Any sharing will be undertaken by trained personnel using secure methods. Where a third party undertakes data processing on behalf of the School e.g. by providing cloud based systems or shredding services, the School will ensure that there is a written agreement requiring the data to be processed in accordance with the Data Protection Principles.

Ensuring compliance

All new staff will be trained on the data protection requirements as part of their induction.

Training and guidance will be available to all staff and on an annual basis as a reminder.
All staff will read the Acceptable IT use Policy and sign to acknowledge that this has been done.

The School has a Privacy Notice which explains broadly why the school collects and processes personal data. This is published on the website – there is no legal requirement for separate policies for staff, students or governors. The Notice includes certain elements:

- Contact details for Data Controller and Data Protection Officer
- Retentions period. Who we share data with.
- The right to request data or contact the school with any concerns.

Individuals Rights
The laws apply certain rights to individuals for the processing of their data. The main applicable rights are listed below:

- "right to be informed" ; This is the right for each individual to know why the school is collecting and processing their data – this is included in the privacy Notice published on the School website.
- "right of access" – see "subject Access requests" above
- "Right of rectification" - if the individual can prove an error in the data held, they have the right to request it be corrected.
- "right of erasure/to be forgotten" – this does NOT apply to student data in any form. For anyone else, it is the right to ask, not an automatic right to have it happen.

Photographs, Additional Personal Data and Consents

Where the School seeks consents for processing person data such as photographs at events it will ensure that appropriate written consents are obtained. Those consent forms will provide details of how the consent can be withdrawn. – Please note – this does NOT form part of Data Protection legislation, it is part of "safeguarding"

Where the personal data involves a child under 16 years written consent will be required from the adult with parental responsibility.

Appendix A

What staff should do:

DO get the permission of your manager to take any confidential information home.
DO only collect/keep the information you actually need.
DO practice good IT security – set strong passwords.
DO ensure your mobile/tablet is password protected if you access work emails/ sites such as tapestry on it.
DO use projector mode on Bromcom when in the classroom.
DO transport information from school on secure computing devices (i.e. Encrypted laptops). Wherever possible avoid taking paper documents out of the office.
DO use secure devices such as encrypted laptops when working remotely or from home.
DO ensure that all paper based information that is taken off premises is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.
DO ensure that any confidential documents that are taken to your home are stored in a locked drawer.
DO ensure that paper based information and laptops are kept safe and close to hand when taken off premises. Never leave them unattended. Particular care should be taken in public places (e.g. reading of documentation on public transport).
DO ensure that when transporting paper documentation in your car that it is placed in the boot (locked) during transit.
DO return the paper based information to the School as soon as possible and file or dispose of it securely.
DO report any loss of paper based information or computer devices to your line manager immediately.
DO ensure that all postal and e-mail addresses are checked to ensure safe dispatch of information. When sending personal information by post. clearly mark the envelope 'Private – Contents for Addressee only'.
DO ensure that when posting/emailing information that only the specific content required is sent.
DO use pseudonyms and anonymise personal data where possible.
DO ensure that access to Bromcom (or equivalent) is restricted to appropriate staff only, that leavers are removed in a timely manner and that generic user names such as 'Sysman' are disabled.

What staff must not do:

DO NOT take confidential information to an entertainment or public place such as a pub or cinema, whether held on paper or an electronic device. Any information must be taken to the destination directly and never left unattended during the journey.
DO NOT unnecessarily copy other parties into e-mail correspondence.
DO NOT e-mail documents to your own personal computer.
DO NOT store work related documents on your home computer.
DO NOT leave personal information unclaimed on any printer or fax machine.
DO NOT leave personal information on your desk overnight, or if you are away from your desk in meetings.
DO NOT leave documentation in vehicles overnight.
DO NOT discuss case level issues at social events or in public places.
DO NOT put confidential documents in non-confidential recycling bins.
DO NOT print off reports with personal data (e.g. pupil data) unless absolutely necessary.
DO NOT use unencrypted laptops
DO NOT use memory sticks to transport data to and from school
DO NOT make sensitive or confidential calls in a public space -this includes any school phone that could be overheard eg main office.