SURBITON
CHILDREN'S CENTRE NURSERY

General Data Protection Policy

Committee ownership for this policy:	TBC
Must be approved by FGB:	No
Required by: • **Where 1 is indicated, the requirement is statutory** • **Where 2 is indicated, the requirement is recommended**	1
Frequency of review:	At least every two years
Date last reviewed:	March 2019
Date of next review:	March 2021
Display on website:	Yes
Purpose:	To set out how the school complies with its obligations under General Data Protection Regulation and to set out responsibilities in this area.
Consultation:	
Links with other policies:	None

General Data Protection Policy

Surbiton Children's Centre Nursery is a maintained nursery school in the Royal Borough of Kingston upon Thames, providing an exciting and stimulating learning environment. The school's excellence in both its mainstream nursery (106 children aged 3 to 4, 16 children aged 2 to 3) and specialist provision (12 young children with social and communication disorders) has been repeatedly recognised as 'outstanding'.

The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

Introduction
Surbiton Children's Centre Nursery needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The headteacher and governors of the school will comply fully with the requirements and principles of the General Data Protection Regulation (2018). All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within the guidelines established by the Act. The school has privacy notices for staff and pupils that outline the reasons why data is collected, used and stored.

Definitions under the Act

- **Consent**- freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data
- **Data Concerning Health** - any personal data related to the physical or mental health of an individual or the provision of health services to them
- **Data Controller** - the entity that determines the purposes, conditions and means of the processing of personal data
- **Data Erasure** - also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data
- **Data Portability** - the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller
- **Data Processor** - the entity that processes data on behalf of the Data Controller
- **Data Protection Authority** - national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union
- **Data Protection Officer** - an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR
- **Data Subject** - a natural person whose personal data is processed by a controller or processor
- **Encrypted Data** - personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access
- **Filing System** - any specific set of personal data that is accessible according to specific criteria, or able to be queried

- **Personal Data** - any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person
- **Personal Data Breach** - a breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data
- **Privacy by Design** - a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition
- **Privacy Impact Assessment** - a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data
- **Processing** - any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.
- **Profiling** - any automated processing of personal data intended to evaluate, analyse, or predict data subject behavior
- **Pseudonymisation** - the processing of personal data such that it can no longer be attributed to a single data subject without the use of additional data, so long as said additional data stays separate to ensure non-attribution
- **Right to be Forgotten** - also known as Data Erasure, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data
- **Right to Access** - also known as Subject Access Right, it entitles the data subject to have access to and information about the personal data that a controller has concerning them
- **Subject Access Right** - also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

1. The key principles of the General Data Protection Regulation (GDPR)*:*

1.1 Lawfulness, fairness and transparency- Transparency: Tell the subject what data processing will be done. Fair: What is processed must match up with how it has been described. Lawful: Processing must meet the tests described in GDPR [article 5, clause 1(a)].
1.2 Purpose limitations - Personal data can only be obtained for "specified, explicit and legitimate purposes"[article 5, clause 1(b)]. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.
1.3. Data minimisation - Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [article 5, clause 1(c)]. In other words, no more than the minimum amount of data should be kept for specific processing.
1.4. Accuracy- Data must be "accurate and where necessary kept up to date" [article 5, clause 1(d)]. Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.
1.5. Storage limitations - Regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than necessary" [article 5, clause 1(e)]. In summary, data no longer required should be removed.
1.6. Integrity and confidentiality- Requires processors to handle data "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage" [article 5, clause 1(f)].
1.7. Accountability - The accountability principle in Article 5(2) is the GDPR requires the school to demonstrate that they comply with the principles and states explicitly that this the responsibility of the school.

All staff or others who process or use personal information must ensure that they follow these principles at all times.

2. Status of this Policy

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the school from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings. All staff acknowledge that they have read, understood and will comply with the principles of this policy annually.

3. The Data Controller and the Designated Data Controllers

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Helen Gannon is the Data Protection Officer (DPO) with responsibility for data protection compliance.
- Staff are clear who the key contact(s) for key school information are (the Information Asset Owners).
- We ensure staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.

4. Responsibilities of Staff

- All staff are DBS checked and records are held in one central record on an encrypted spreadsheet.

We ensure ALL the following school stakeholders sign an Acceptable Use Agreement annually. We have a system so we know who has signed.

- staff
- governors
- pupils
- parents
- volunteers

This makes clear all responsibilities and expectations with regard to data security. All staff are responsible for: Checking that any information that they provide to the school in connection with their employment is accurate and up to date. Informing the school of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The school cannot be held responsible for any errors unless the staff member has informed the school of such changes. However, once the school has been informed of any change in circumstances, their record must be updated as soon as practicable.

5. Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely (through digital encryption or in physical locked storage.
- Personal information is not disclosed either orally or in writing or via digital or by
- any other means, accidentally or otherwise, to any unauthorised third party.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or
- If it is computerised, be coded, encrypted or password protected both on a network drive or school-approved Google services, that is regularly backed up; and
- Computer printouts as well as source documents must be shredded before disposal.
- No removable storage media (such as DVDs, USB sticks or memory cards) should be used to store data.

Overall security policy for data is determined by the Data Protection Officer and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.
Any queries or concerns about security of data in the school should in the first instance be referred to the headteacher.

The school is liable in law under the terms of the GDPR, and staff are responsible for ensuring that practices that have been put in place by the school are adhered to. The school may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this General Data Protection Policy by a member of staff will be treated as disciplinary matter, and serious breaches could lead to dismissal.

5.1 Strategic and operational practices to ensure data security

- We have approved educational web filtering across our wired and wireless networks.
- We monitor school emails, web usage and use of G-Suite to ensure compliance with the Acceptable Use Agreement.
- We follow borough guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
- We require staff to use strong passwords for access into our SIMS system.
- We require staff to change their passwords into the SIMS and USO logins twice a year.
- We require that any personal/sensitive material must be encrypted. We have an approved remote access solution (Google G-Suite for Education) so staff can access sensitive and other data from home, without need to take data home.
- No sensitive data is stored locally on any device, including laptops and USB sticks. All data is stored on SIMS on the school service.
- School staff who set up usernames and passwords for email and network access work within the approved system and follow the security processes required by those systems.
- The school network has up-to-date anti virus software, which is maintained by LGFL and Click on IT London Ltd.
- Pseudonymisation will be used for paper copies of sensitive information (e.g. lesson plans and incident reports) where possible to minimise risk
- We ask staff to undertake house-keeping checks at least termly to review, remove and destroy any digital materials and documents which need no longer be stored.

5.2 Technical or manual solutions to ensure data security

- Staff have Team Drive to store sensitive documents or photographs, which is encrypted with password protection.
- We require staff to lock or log-out of systems when leaving their computer, but also enforce lock-out after 10 mins for admin computers.
- We use LGfL for creation of online user accounts for access to services and online resources.
- We use LGfL's USO-FX2 to transfer documents to schools in London, such as references, reports of children.
- We store any sensitive/special category written material in lockable storage cabinets in a lockable storage area.
- We use cloud based software to backup and retrieve data for disaster recovery.
- We comply with the WEEE directive on equipment disposal, by using an approved disposal company for disposal of IT equipment. For systems, where any protected or restricted data has been held, (such as servers, photocopiers), we get a certificate of secure deletion.

- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure>
- Paper based sensitive information is shredded using Shred-On-Site disposal services.

6. Authorised disclosures

The School will, in general, only disclose data about individuals with their consent. However, the school is required, by law, to pass on some of this personal data to the local authority and the Department for Education (DfE). The school will share staff details with the following in order to facilitate the smooth running of the school:

- Strictly Education & Personnel Management Services – Payroll &HR
- Teacher/ Local Government Pension Scheme - Pensions
- Click on IT London Ltd and LGFL - IT services
- Cygnet - Single Information Management System (SIMS)
- Educational apps for children - to enable management of pupils' learning

Governing body meetings - The school will anonymise the data by removing staff members' names. To further ensure confidentiality, the minutes from the Pay Committee meeting will be kept confidential, and governors attending the meeting should be made aware that the information disclosed – and the meeting itself – is confidential. So that they do not breach the confidentiality of any members of staff, as a matter of good practice the school will ensure that no staff governors are present in the discussion of a teacher's appraisal targets.

Whilst the majority of pupil information provided to the school is mandatory, some of it is provided to on a voluntary basis. In order to comply with the General Data Protection Regulation, the school will inform parents whether they are required to provide certain pupil information to us or if they have a choice in this.

The categories of pupil information that is collected, held and shared include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)

Information collected about pupils will be kept for 6 years, unless there is additional legal circumstances to be kept longer.

The school is required, by law, to pass certain information about our pupils to our local authority (LA) and the Department for Education (DfE). The DfE may also share pupil level personal data that the school supplies to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the General Data Protection Regulation 2018. The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

The school is required by law, to provide information about pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in

the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

7. Rights to Access Information

All staff, parents and other users are entitled to:

• Know what information the school holds and processes about them or their child and why.
• Know how to gain access to it.
• Know how to keep it up to date.
• Know what the school is doing to comply with its obligations under the 1998 Act.

The school will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the school holds and processes about them, and the reasons for which they are processed.
All staff, parents and other users have a right under the General Data Protection Regulation 2018 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should complete the *Subject Access Request* Form and submit it to the headteacher.
Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

The school aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days, as required by the GDPR Act.

8. Subject Consent

In many cases, the school can only process personal data with the consent of the individual.
In some cases, if the data is sensitive, as defined in the GDPR Act, express consent must be obtained. Agreement to the school processing some specified classes of personal data is a condition of acceptance of employment for staff. This includes information about previous criminal convictions.
Working within a school will bring the applicants into contact with children. The school has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. The school has a duty of care to all staff and students and must therefore make sure that employees and those who use school facilities do not pose a threat or danger to other users.
The school may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The school will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

9. Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This is known as personal data and data concerning health. This may be to ensure that the school is a safe place for everyone, or to operate other school policies, such as the Sick Pay Policy or the Equal Opportunities Policy. Because this information is considered **sensitive** under the 2018 Act, staff (and students where appropriate) An offer of employment may be withdrawn if an individual refuses to consent to this without good reason. Non-sensitive information will be collected by the school annually via a Google Form. Staff and parents have the right to withhold consent to give any non-sensitive data. The school has data erasure systems in place to ensure that an individual's right to be forgotten can be exercised. The Single Information Management System (SIMS) ensures data portability through the use of common transfer protocol (CTF) files.

10. Publication of School Information
Certain items of information relating to school staff will be made available via searchable directories on the public website, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the school. Permission for this is obtained annually from staff via a Google Form.

11. Processing and storing data
The school is a data controller and collects data for a variety of purposes (see Annex 1). This data is stored principly on the Single Information Management System (SIMS) and the school's GoogleDrive. Additional third parties are also used a data processors. The school is responsible for ensuring that all data processors are compliant with the GDPR Act (see Annex 4). All pupils and staff are aware of what data is processed by the school, the basis for collection and the retention period for the data as outlined in the school's privacy notices for staff and pupils. Staff and parents acknowledge they have read and understood the privacy notices annual via a GoogleForm.

12. Retention of Data
The school has a duty to retain some staff and student personal data for a period of time following their departure from the school, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time. Data held about individuals will not be kept for longer than necessary for the purposes required. It is the duty of the Data Protection Officer to ensure that obsolete data is properly erased.

13. Rights of individuals
Under the GDPR Act, all stakeholder have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing or school fundraising purposes
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

14. Complaints
Complaints about the above procedures should be made to the Chair of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure. Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

15. Data breaches
In the event of a personal data breach, the school will conduct an assessment to determine the potential risk of harm to the data subject(s) rights and freedoms. The school will report a personal data breach to the Information Commissioner's Office (ICO) if it is likely to result in a risk to people's rights and freedoms. In the event of a data breach, the school will contact the ICO using reporting tool (https://report.ico.org.uk/security-breach/)

16. Compliance
Compliance with the GDPR Act is the responsibility of all members of the school. Any

deliberate breach of the General Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

Related Policies: None

Approved Governing Body:
Reviewed date: March 2019
Review date: March 2021

Additional documents
Annex 1: School data audit - this outlines what data is processed by the school, the basis for collection and the retention period for the data.
Annex 2: Staff privacy notice
Annex 3: Pupil privacy notice
Annex 4: Data processor audit- this outlines who processes data on on behalf of the school and demonstrates their compliance with the GDPR act
Annex 5: Subject Access Request (SAR) letter

Please note some documentation is not included in the online version of the policy.

ANNEX 5

[Your full address]
[Phone number]
[The date]

[Name and address of the organisation]

Dear Sir or Madam

Subject access request

[Your full name and address and any other details to help identify you and the information you want.]

Please supply the information about me I am entitled to under the Data Protection Act 1998 relating to: [give specific details of the information you want, for example

- **your personnel file;**
- **emails between 'A' and 'B' (between 1/6/11 and 1/9/11);**
- **CCTV camera situated at ('E' location) on 23/5/12 between 11am and 5pm;**

If you need any more information from me, or a fee, please let me know as soon as possible.

It may be helpful for you to know that a request for information under the Data Protection Act 1998 should be responded to within 30 days.

If you do not normally deal with these requests, please pass this letter to your Data Protection Officer. If you need advice on dealing with this request, the Information Commissioner's Office can assist you and can be contacted on 0303 123 1113 or at ico.org.uk

Yours faithfully
[Signature]