Clarendon Primary School, Nursery & Children's Centre

Data Handling Policy

'Doing our best to achieve our best'

The management of personal data in an electronic form is done in accordance with the statutory requirements of the Data Protection Act 1998.

1. Personal data

As part of their role, the Children's Centre, school and their staff will have access to some personal data concerning children and families including, but not limited to; names, dates of birth, the name of their parents or guardian, address and contact numbers as well as legal information and curricular data. Sensitive information may also be held in accordance with our safeguarding policy.

2. Responsibility

School, Nursery and Children's Centre

- It is the school and Children's Centre's responsibility to ensure that the data handling policy is followed by the members of the establishment and respect the Data Protection Act 1998

Staff

- The staff are responsible for their safe handling of the school and Children's Centre's available, and potentially sensitive, data. Staff need to adhere to the Data Protection Act of 1998.

Data Protection Officer

- The school and Children's Centre keep up to date with the current legal guidance and apply new legislations.

Governors

- As with members of the school and Children's Centre's staff, governors need to adhere to the same rules as other members of staff when, as part of their role, they have access to data.

3. Registration

The Data Protection Act 1998 requires every organisation that processes personal information to register with the Information Commissioner's Office (failure to do so is a criminal offence).Schools are responsible for ensuring they are registered as a Data Controller on the Data Protection Register, held by the Information Commissioner: http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

4. **Data storage and disposal**

Securely Accessing and Storing Data

ICT systems and MIS should be managed in such a way that protected files can be given permission levels, with protected files being hidden from unauthorised users. Access to data should be granted as required for the employee's role only.

Personal and sensitive data should only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods). Autolock should be enabled when devices are left unattended.

The school and Children's Centre encourage users to have strong passwords, which are changed regularly. User passwords must never be shared.

Storage media is stored in a secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school and Children's Centre equipment (this includes computers and portable storage media (iron keys issued to all staff). Private equipment must not be used for the storage of personal data. Where personal devices are used to access data remotely passwords should not be stored on the device and personal data should not be downloaded.

When personal data is stored on any mobile device or removable media:

- the data must be encrypted and password protected,
- it must have virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (see guidance below) once it has been transferred or its use is complete.

The school does not recommend the use of "Cloud Based Storage Systems" (for example dropbox, google apps and google docs) and users in both the school and Children's Centre sign an Acceptable Use Policy agreeing to comply with this.

The school and Children's Centre is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material is held in lockable storage, either on or off site.

The school recognises that under Section 7 of the DPA, (http://www.legislation.gov.uk/ukpga/1998/29/section/7) data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to contact Surrey's Local Area Officers to seek advice before dealing with Subject Access Requests

Secure transfer of data and access out of school:

On occasion it may be necessary for personal data to be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Before removing or copying sensitive, restricted or protected data the user must gain permission from the data controller and ensure the media is encrypted and password protected and is transported and stored securely.
- If data is taken or transferred to another country, particularly outside Europe, advice should be taken from the local authority in this event. For example, staff should not take such data on holiday unless there is a justifiable need and permission has been sought.

Data Disposal:

The school and Children's Centre will comply with the requirements for the safe destruction of personal data when it is no longer required. The DPA states within its fifth principle that "data shall not be kept for longer than is necessary".

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

5. Cloud services

The school and Children's Centre do not subscribe to cloud based services. If this decision changes the policy we would conduct a thorough investigation to be carried out before moving to a cloud system. If staff employed by the Children's Centre or school choose to subscribe to cloud based services outside of

school it is their responsibility to ensure that only non-personal and non-sensitive data is saved to the cloud. When staff sign the Acceptable Use Agreement they indicate their agreement to this clause.

6. Training and CPD

All staff need to be trained on electronic data handling and need to be reminded of their responsibilities, as per this policy.

Training normally takes the form of an induction, as well as annual training as part of Safeguarding. Any relevant updates involving the emergence of new technology will be given as they arise.

7. Data Breach and reporting incidents

Logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use police.

All significant data protection incidents will be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

8. Electronic communications

The school and Children's Centre will adhere to the Privacy and Electronic Communications Regulations which protects staff and pupils' privacy.

9. Supporting Reading

- http://www.dft.gov.uk/vca/data-protection-act-guidance-on-compliance.asp
- http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted
- https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools
- https://www.gov.uk/government/publications/data-handling-procedures-in-government