

**DATA SECURITY**

**FRAMEWORK**

|  |  |
| --- | --- |
| Approved Date | Sept 2018 |
| Approved At | S&F  |
| Reviewed  | Sept 2021 |
| Amendments | Updated for law changes Jan 2021 and minor changes |
| Date of Next Review | Sept 2023 |
| Statutory | NO |
| Adopted from Bracknell Forest | NO |

**DATA SECURITY FRAMEWORK**

1. Purpose

The purpose of this document is to lay out the policies and procedures for managing all data at College Town Primary School in order to comply with the Data Protection Act 2018, UK GDPR, Freedom of Information Act 2000 and to ensure the security of all information held at the school.

This document follows the guidance produced by the Information Commissioner’s Office and Bracknell Forest within the Data protection and UK GDPR section of the school management website and is a high-level document which refers to several more detailed policies.

1. Data Protection and the UK GDPR

2.1 Obligations and Data Collection

It is a statutory requirement to have a separate Data Protection Policy which is intended to ensure that personal information is dealt with correctly and securely in accordance with the Data Protection Act 2018 and other related legislation. The policy is reviewed every two years (or earlier if notified of changes to legislation.)

The requirements of the Data Protection Act 2018 and the UK GDPR apply to personal, sensitive, and confidential information as defined by the Information Commissioner. See the Data Protection Policy for detail.

The school is registered with the Information Commissioner’s office under the Data Protection Act 2018 to hold personal data as a data controller. The notification period is for one year and is renewed annually.

The school has Privacy Notices for Pupils/Parents; Staff and Governors detailing the data to be collected, the reason for holding the data, the lawful basis, who it is shared with and how it is stored and follows the UK GDPR guidance from the Information Commissioner. A data mapping spreadsheet is used to identify all the data within school. The privacy notice for pupils/parents is published on the school website. In addition to the privacy notices where data collection is carried out (e.g for new starters, updates) a statement is added to make it clear how and what the data is being used for. (See Appendix DSF1 for specific statements used by the school and Local Authority produced documents e.g via SIMs.)

* 1. Data Security

This section defines the schools’ measures to guard against unauthorised access to personal information and against accidental loss or destruction, or damage to, personal information. All sensitive information is protected and includes all personal information for pupils and staff such as assessment records, medical information and special educational needs data.

* + 1. Computer Security

The schools computer security procedures including disposal of IT equipment, password use, acceptable use, use of secure email, encrypted USBs, laptop use, access to SIMS/FMS, back-ups, automatic log-off, new/old users, computer and server locations, network access etc. are defined within the E-Safety Policy.

The network is protected by anti-virus software as part of the IT support contract.

* + 1. IT Recovery and Back Up Procedures

The whole IT network is backed up by the IT support company (SmarterInteractvie) off-site using their back up centre. The backups are carried out each night between 9pm and 12.00. A daily status email of the backup is sent to the backup section of the IT support company who monitor the status of the backup.

The school has full disaster recovery and if needed IT support would be able to either remove the infected server and download a clean copy of the system or install the system onto a new server within a day. Individual files can also be recovered and downloaded.

See e-safety policy

* + 1. Paper Data Security

All paper copies of confidential information must be stored in lockable cabinets with key access given only to the appropriate personal that require the information for the purpose of their daily role within the school. All staff and pupil information are locked in the school offices or archived in lockable cabinets within the school and can only be accessed by the Head, Assistant Heads, School Business Manager and Admin Team. Any pupil personal information used by the class teacher (e.g. tracking information, school records, reports) must be locked in a cupboard in the classroom or returned to the office.

It is the responsibility of staff to ensure that sensitive information is not left out when not being used. All confidential paper waste must be shredded when no longer required and in accordance with the schools Records Management Policy.

When sending personal information by post the package will be double wrapped and delivered using a recorded delivery service.

Personal information should only be sent via fax if necessary and there is no other practical alternative, by hand or by secure email are the preferred delivery methods. When faxing information the recipient should be contacted prior to sending to check that the fax number is correct, to ensure that they are present to receive the fax and to enable them to acknowledge its safe receipt immediately.

* + 1. Premises Security
			1. School Gates

The school premises are secured using high security fencing and gates maintained by an appropriate contractor to ensure they are in working order and comply with health and safety standards. Access to the school is via the driveway gates for transport or via pedestrian gates. All staff will be issued with a key fob to access the driveway gates, which must be signed for and any loss reported immediately.

Pedestrian gates are accessed using a key pad entrance system, the code for which is only given out to staff and changed annually. The pedestrian gates will open automatically at the beginning and end of the school day, the times to be determined in conjunction with the Alders Children’s centre and reviewed regularly to ensure they are appropriate.

Access to the grounds during the school day is controlled by the school office and Alders Childrens Centre via an intercom system on each gate. Staff must ensure they know who is gaining access and ask them to report to the office to sign in.

* + - 1. Building

The school building is alarmed and only the designated key holders have access to the school once it is locked and the alarm activated. They are:

 Head Teacher

Assistant Head

 School Business Manager

 Site Controller

 Cleaning Contractor

It is the responsibility of the Site Controller to ensure the site is fully secured at the end of the working day and that all windows and doors are locked and that the school is unlocked in the morning for staff to gain access. During school term time the locking up of the school has been delegated to the cleaning contractors.

Keypad codes for the entrance doors to the school are only given out to staff and will be changed regularly, at least once a year or sooner if a breach of security is reported.

* + - 1. Office/Stock Cupboard

The Finance Office will be locked at night and only those staff with a key will be able to gain access, Head, School Business Manager, Site Controller and Admin Officers.

The school safe will remain locked at all times and is located in a locked room.

 2.2.3.4 CCTV

CCTV is used around the school both inside and outside. The recordable devices are password protected and access to them restricted to appropriate staff, Site Controller, Head, SLT, SBM and Office Staff. The CCTV servers (two of) are locked away in the ICT comms cupboard in KS1 and the comms cupboard in KS2 buildings.

Signs are erected around the outside of the premises to inform the public about the CCTV and state ‘These premises are protected by CCTV and the images are recorded for crime prevention and safety.’ ‘CCTV in Operation’ signs are placed at the site of each camera and at other locations in and around the school.

CCTV information is recorded and kept on a 30 day loop system. The length of time the information is retained has been selected to ensure data is available for all periods when the school site is unattended. The maximum number of days the school site could be completely closed without one of the staff with allowed access to the CCTV system on site is 21 days during the school summer holidays.

* + 1. Staff Training

Training on Data Protection and E-Safety is included in the staff induction programme for new starters. A section on Data Protection and E-Security and staff responsibilities is also included in the staff handbook which is reviewed annually. A brief training session will also be given to staff on the first inset of the each school year.

Training includes:

* What is expected of staff
* E-Safety and Acceptable Use
* To be wary of people who may try and trick them into giving personal details
* That they can be prosecuted if they deliberately give out personal details without permission
* To use strong passwords and change them regularly
* Not to send offensive emails about other people, their private lives or anything else that could bring the school into disrepute
* Not to believe emails that appear to come from a bank and ask for account, credit card details or passwords.
* Not to open spam, not even to ask for no more mailings.
* GDPR and To explain the consequences of breaching the Data Protection Act even when inadvertently – *In Nov 2010Hert CC were fined £100,000 for sending on two occasions a fax containing sensitive information to the wrong fax number.’ ‘in Feb 2011 Hounslow and Ealing Council were fined £70,000 and £80,000 after the loss of two unencrypted laptops containing sensitive personal information.’*
	+ 1. Access to Pupil Information and Data protection request

The school follows the guidance of the Information Commissioners Office on requests for access to pupil information and who has the right to access information. How to access personnel data is defined in the data protection policy and privacy notices.

There are two distinct rights to information held by the school about pupils.

The Subject Access Right – Under the Data Protection Act 2018 a pupil has the right to a copy of their own information. Parents may make a request on behalf of their child when the child is unable to act on their own behalf or gives their consent.

The Right to the Education Record – Under the Education regulations 2005 a parent has the right to access their child’s educational record.

See the Data Protection Policy for detail. Any requests for information should be recorded including the nature of the request, who made the request, the response, any costs associated with the request and the timescale for the response. This will be recorded in the DP and FOI Request Log.

If in doubt staff should consult the Head/Local Authority/IC or take Legal advice when responding to a request for information.

* + 1. Privacy Notice and Information Sharing

The school has separate Privacy notices for Pupils, Staff and Governors under the GDPR guidelines.

The privacy notice defines how we collect data and what it is used for along with the legal status used. It also defines how the data is shared and who we routinely share our data with including to carry out the statutory function of the school. In addition, the Data Protection Act 2018 recognises that in some circumstances the public interest requires disclosure of personal information without the persons consent and that Safeguarding is paramount e.g.

* The Prevention of crime, apprehension or prosecution of offenders
* Where a child is believed to be at risk
* If necessary or in connection with any legal proceedings, obtaining legal advice or establishing, exercising or defending legal rights.
* When ordered to do so by a court

The school shares data with the following organisations on a regular basis and when collecting this data informs the individual that the data will be shared with them:

Pupil Data – Local Authority. DfE, School Nurse (Berkshire NHS)

The school registration form includes a statement informing parents about who the pupil data will be shared with. Any data collection sheets produced by SIMs used to update pupil information also includes an appropriate statement. (See Appendix DSF1 for example statements.)

Staff Data – Local Authority, DfE (SWC)

Job application forms include a tickbox for applicants to agree to the use of their data in accordance with GDPR and the Data Protection Act 2018. All HR employee forms (e.g New Starter, Change etc) also include a statement referring to the use of the information of the form for employment administration, pensions and benefit administration subject to the Data Protection act.

A statement is also added to the data collection sheets produced by SIMs during any data collection activities e.g for the School Workforce Census. (See appendix DSF1 for example statements.)

* + 1. Loss of Personal Information

If there is any loss of personal information due to a breach of security the following procedures must be followed whether it is due to theft, a deliberate attack on the school systems, unauthorised use of personal information by a member of staff, accidental loss or equipment failure: (see The Data Protection policy Section 10 and Appendix 2, for detail)

* Record the incident.
* Mitigate and further risks (The Data Protection Officer will assist the staff member in identifying and actioning any mitigation required.).
* Carry out a risk assessment associated with the breach.
* Inform the DPO and the information commission if required.
* Log the incident and the actions taken.
* Attempt to recover the information
* Inform the appropriate people and organisations that the breach has occurred.
* Review the school systems and information security in place and amend as appropriate
1. Freedom of Information

3.1 Freedom of Information Request

A Freedom of Information request is a request for specific information, made in writing, with a name and address for correspondence (which can be an email address) which is not answered in the schools normal course of business. It should be processed and responded to in accordance with the Freedom of Information Act which means it must be supplied within 20 school days (this excludes weekends and holidays) unless the request can be refused or the information can be withheld in accordance with the Act.

When a FOI request is received staff need to refer to the IC Guide to the Life Cycle of a Request which is Appendix K of the BF – information Pack to Schools. Further information on the process can be found on the IC website. Standard template letters for use are available from Appendix J of the BF Information Pack for Schools.

All FOI requests should be logged using the schools DP and FOI request Log which is kept on the Admin H Drive.

* 1. Publication Scheme

The school has produced a Publication Scheme as specified by the IC and a Guide to Information Available from the School under the Publication Scheme. These documents can be found on the school website and they define the information the school makes routinely available, explains how it can be accessed and whether a charge will be made for it.

Any information not listed in the guide can still be requested and will be made available under the FOI Act if available and unless it can be legitimately withheld.

1. Records Management

Record Management procedures and retention guidelines are defined in the Schools Record Management Policy. This includes a policy statement which is reviewed regularly by the Governing body and made available to all staff.

1. Business Continuity/Disaster Recovery

This policy defines how the school controls and stores electronic and paper information, informs staff of their obligations, and deals with a breach of information covering:

* Backup – E-Safety Policy
* Control of way Electronic Data is stored – E-Safety policy
* Passwords – E-Safety
* Location of Server – E-Safety
* Storage of Paper copies – Main Body of this Document
* Restricting Access/ Preventing theft – Main body
* Clear Desk Policy – Main Body
* Staff Training – Main Body
* Loss of Information – Main Body

In addition the schools Emergency Plan describe the procedures to follow in the event of a disaster and what access to school records/information will be required.

Appendix DSF1 – Data Protection Statements

 School registration form

‘***The data being collected, controlled and processed is in line with current data protection legislation. The school is required to share some of the data with the Local Authority, school nurse team and with the DfE’***

 SIMS Pupil Data Collection Sheets

***The data being collected, controlled and processed is in line with General Data Protection regulations. The school has a duty to protect this data and keep it up to date. The school is required to share some of the data with the Education Authority and the Department of Education.’***

Staff application form

 ‘***By ticking this box and submitting this form I consent to the processing of personal data relating to me for the purposes of managing my application, provided that such processing is in accordance with the GDPR 2016 and Data Protection Act 2018’***

New Employee Data Collection

**‘This information will be used for employment, pensions & benefit administration and is subject to the Data Protection Act 2018.’**

SIMS Staff Data Collection Sheets

**‘*This data is required to update the school’s management information system. The information you return will not disadvantage you in any way and will be stored and transferred securely. It is required to help us to monitor our own workforce’s diversity within the aims and objectives of the Equal Opportunities policy, as well as meet the requirements of the School Workforce Census (SWC) and other statutory data returns, and to ensure that the school has up to date contact information.’***

***‘Workforce data is essential for the school’s / local authority’s operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.***

***We are required to share information about our school employees with the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments. All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current*** [***government security policy framework***](https://www.gov.uk/government/publications/security-policy-framework)***. ‘***