Sir Charles Parsons School

DATA PROTECTION AND SECURITY POLICY
2018-2020

DOCUMENT HISTORY

Author(s)	**A Taylor**
Date of Issue	**April 2018**
Reviews	**19 June 2018**

Aims
Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and guidance
This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras (CCTV) and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005 which gives parents the right of access to their child's educational record.

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes

	• Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

The data controller
Our school processes personal data relating to pupils, staff, parents, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Roles and responsibilities
This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Body
The Governing Body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

The Head Teacher
The Head Teacher acts as the data controller for the school on a day to day basis.

The Data Protection Officer
The data protection officer (DPO) is responsible for monitoring our school's compliance with data protection law. They will provide an annual report of their activities to the Governing Body and, where relevant, report to the governors their advice and recommendations on school data protection issues.

The DPO is the first point of contact for the ICO. Full details of the DPO are set out in their job description.

Our DPO is Alex Coughlan, Veritau Ltd. and is contactable on 01609 767199 via email at alex.coughlan@veritau.co.uk

School Business Manager
The School Business Manager is responsible for overseeing the implementation of this policy and developing policies and guidelines relating to data protection. The School Business Manager is the first point of contact for individuals whose data the school processes.

All Staff
Staff are responsible for:

- collecting, storing and processing any personal data in accordance with this policy;
- informing the school of any changes to their personal data, such as a change of address, telephone number, email address;
- contacting the School Business Manager in the following circumstances
    - with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - if they have any concerns that this policy is not being followed
    - if they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - if they ned to rely on or capture consent, draft a privacy notice, deal with protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - if they need help with any contracts or sharing personal data with third parties;
- Contacting the DPO in the following circumstances
    - if there has been a data breach.

Data protection principles
The GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

- processed lawfully, fairly and in a transparent manner;
- collected for specific, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;
- accurate and, where necessary, kept up to date;
- kept for no longer than is necessary for the purposes for which it is processed;
- processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

Collecting personal data (see appendix 3 for fair obtaining and processing)

Lawfulness, fairness and transparency
We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law.

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering a contract.
- The data needs to be processed so that the school can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions.
- The data needs to be processed for the **legitimate interests** of the school or a third party (provide the individual's rights and freedoms are not overridden).
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent.**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will obtain parental consent.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's retention policy and is the responsibility of the staff member who collected the data.

Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- there is an issue with a pupil or parent/carer that puts the safety of our staff at risk;
- we need to liaise with other agencies – we will seek consent as necessary before doing this;
- our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law and GDPR;
    - establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share;
    - only share data the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- the prevention or detection of crime and/or fraud;
- the apprehension or prosecution of offenders;
- the assessment or collection of tax owed to HMRC;
- in connection with legal proceedings;
- where the disclosure is required to satisfy our safeguarding obligations;
- research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We my also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Subject access requests and other rights of individuals

Subject access requests
Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- confirmation that their personal data is being processed;
- access to a copy of the data;
- the purposes of the data processing;
- the categories of personal data concerned;
- who the data has been, or will be, shared with;
- how long the data will be stored for, or if this isn't possible, the criteria used to determine this period;
- the source of the data, if not the individual;
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted in writing, either by letter, email or fax to the School Business Manager (see appendix 1). They should include:

- name of the individual;
- correspondence address;
- contact number and email address;
- details of the information requested.

If staff receive a subject access request they must immediately forward it to the School Business Manager.

Children and subject access requests
Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Responding to subject access requests

When responding to requests we:

- may ask the individual to provide 2 forms of identification;
- may contact the individual via phone to confirm the request was made;
- will respond without delay and within 1 month of receipt of the request;
- will provide the information free of charge;
- may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- might cause serious harm to the physical or mental health of the pupil or another individual;
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- is contained in adoption or parental order records;
- is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

<u>Other data protection rights of the individual</u>
In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see collecting personal data section), individuals also have the right to:

- withdraw their consent to processing at any time;
- ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- prevent use of their personal data for direct marketing;
- challenge processing which has been justified on the basis of public interest;
- request a copy of agreements under which their personal data is transferred outside of the European Economic Area;
- object to decisions based solely on automated decision making or profiling (decision taken with no human involvement, that might negatively affect them);
- prevent processing that is likely to cause damage or distress;
- be notified of a data breach in certain circumstances;
- make a complaint to the ICO;
- ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the School Business Manager. If staff receive such a request they must immediately forward it to the School Business Manager.

Parental requests to the see the educational record
Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 days of receipt of a written request.

CCTV
We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

The internal CCTV cameras are "live" only and the data is not recorded. They are used only for remote supervision of students who are moving around the school independently.

Any enquires about the CCTV system should be directed to the school site caretaker.

Photographs and videos
As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school newsletters, brochures etc
- Outside of school by external agencies such as the school photographer, newspapers, campaigns etc
- Online on our school website, blogs or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the pupil, to ensure they cannot be identified.

Data protection by design and default
We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see data protection principles above);
- completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process);

- integrating data protection into internal documents including this policy, any related policies and privacy notices;
- regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters, we will also keep a record of attendance;
- regularly conducting reviews and audits to test our privacy measures and make sure we are compliant;
- maintaining records of our processing activities, including:
    - for the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we used and process their personal data (via our privacy notices);
    - for all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we use the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

Data security and storage of records
We will protect personal data and keep it safe form unauthorised or unlawful access, alteration, processing or disclosure and against accidental or unlawful loss, destruction or damage.

In particular

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access – (see appendix 4 – clear desk and clear screen policy).
- Where personal information needs to be taken off site, staff must sign it in and out from the school office.
- Passwords, that comply to NCC IT requirements are used to access school computers, laptops and other electronic devices. Staff are reminded to change their password at regular intervals and not to disclose to other persons.
- Encryption software is used to protect portable devices and removable media, such as laptops and USB devices.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our IT Policy, E-Safety Policy, Acceptable Use Policies).
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Disposal of records
Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal data breaches
The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 2.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium;
- safeguarding information being made available to an unauthorised person;
- the theft of a school laptop containing non-encrypted personal data about pupils.

Training
All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring arrangements
The School Business Manager and the DPO are responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the full governing body.

Links with other policies/documents

- Freedom of Information Publication Scheme
- E-Safety Policy
- Acceptable Use Agreements
- Safeguarding and Child Protection Policy
- Document Retention Policy/Schedule
- Reproduction of Images Policy
- Privacy notices – staff and pupils
- Appendix 4 of this policy – clear desk and clear screen policy

Sir Charles Parsons Appendix 1

Subject Access Request Form

Data Protection Act 1998 Section 7.
Enquirer's Surname…… Enquirer's Fore Names……..
Enquirer's Address ……. …… ……
Enquirer's Postcode ……Telephone Number …….
Are you the person who is the subject of the records you are enquiring about YES / NO (i.e. the "Data Subject")? If NO, Do you have parental responsibility for a child who is the "Data Subject" of the YES / NO records you are enquiring about? If YES, Name of child or children about whose personal data records you are enquiring …….
Description of Concern / Area of Concern
Description of Information or Topic(s) Requested (In your own words)
Additional information:
Please Reply to: (if different from enquirer's details as stated on this form) Name Address Postcode
Data subject declaration I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School. I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search. I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).
Signature of "Data Subject" (or Subject's Parent) ……
Name of "Data Subject" (or Subject's Parent) (PRINTED)…….
Dated …….

Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member of data processor must immediately inform the School Business Manager
- The School Business Manager will investigate the report, and determine whether a breach has occurred. To decide, the School Business Manager will consider whether the personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The School Business Manager will alert the Head Teacher and the chair of governors
- The School Business Manager will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors, where necessary. (Actions relevant to specific data types are set out at the end of this procedure.)
- The School Business Manager and DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identity theft or fraud
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in main school office.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will reports as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective or whether it is reported to the ICO. For each breach this record will include the:
    - Facts and cause
    - Effects
    - Action take to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
    - Records of all breaches will be stored in the main school office.
- The DPO, the School Business Manager and the Head Teacher will meet to review what happened and how it can be stopped from happening again. This meeting will take place as soon as reasonably possible.

Fair Obtaining and Processing

We will inform all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

- "processing" means obtaining, recording or holding the information or data or carrying out any set of operations on the information or data
- "data subject" means an individual who is the subject of personal data or the person to whom the information relates
- "personal data" means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, internet or media
- "parent" has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child

Registered purposes

The Data Protection Registration entries for the school are available for inspection, by appointment, at the school site or from the ICO website www.ico.org.uk Explanation of any codes and categories entered is available from the School Business Manager. Registered purposes covering the data held are listed on the Registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

Appendix 4

Clear Screen and Desk Policy

Introduction

Information is an asset. Like any other business asset it has a value and must be protected. Systems that enable us to store, process and communicate information must also be protected in order to safeguard information assets. 'Information systems' is the collective term for our information (both paper-based and computerised) and the systems we use to store, process and communicate it.

Rationale

Thomas Bewick School holds information about pupils, parents and staff in both computerised and paper forms, including particularly sensitive Special Category Data (health reports, SEN, child protection etc). The school is at risk of a serious data breach of unauthorised access to electronic records, when unlocked PC screens are left unattended or when paper records are left on desks/workstations overnight or for long periods of time. Both are at risk of theft, unauthorised disclosure and damage. Clear desks and clear screens protect against a data breach and also ensure that the school projects a professional and efficient image to visitors, members of the public and colleagues.

Roles and Responsibilities

It is important that all staff understand what is required of them and comply with this policy.

All staff are responsible for ensuring the information on their desk/workstation or screen is adequately protected in compliance with all relevant school policies and procedures.

Line Managers have a responsibility to ensure their staff are following procedures. The Data Protection Officer and School Business Manager have the responsibility to advise the school on data protection legal obligations and procedures to keep data safe, and to monitor compliance across the trust.

Scope

This policy applies to everyone who has access to the school's information, information assets or IT equipment. This may include, but is not limited to employees of the school, governors, temporary workers, partners and contractual third parties.

All those who use or have access to information must understand and adopt this policy and are responsible for ensuring the security of the school's information systems and the information that they use or handle.

This policy sets out school's requirements for each member of staff to protect any documents or records which are kept at their desk/workstation either temporarily or permanently and covers records in all formats including:

- Paper
- Electronic documents
- Emails
- Visual images such as work related photographs
- Audio and video CDs, DVDs etc

- Memory sticks and portable hard drives
- Databases

Clear Desk Procedure

All personal information about pupils, parents or staff **must** be locked away when not in use and never left unattended. Ideally, all staff should leave their desk paper free at the end of the day.

Ensure that you select an appropriately located printer where you are able to retrieve your printing immediately. Do not leave personal information for others to find. Coded printing will be used where possible when appropriate.

An easy way to comply with the clear desk procedure is to work with electronic documents whenever possible **– "Do you need to print it"?**

Ensure documents are disposed of securely. Never put documents containing personal or corporate sensitive information in the general waste bins. Use the confidential paper shredding boxes.

All Portable Computing & Data Storage Devices (PCDs) such as USB data sticks, mobile phones and laptops should be locked away at the end of the working day.

Clear Screen Procedure

Always lock the desktop when leaving the workstation/desk unattended. If using a shared workstation/desk log off rather than lock it. If anticipating an absence of more than 30 minutes log off or shutdown the computer. This also applies when using a laptop.

Pressing CTRL+ALT+DEL and clicking 'Lock this computer' is straightforward and simple.

To unlock press CTRL+ALT+DEL and log back in.

Always be aware of the position of the screen on your workstation. Wherever possible, ensure that it cannot be seen by unauthorised people while in use.

Always shutdown all computers at the end of every day!!

Monitoring Procedure

Line Managers should make random spot checks on unattended desks/screens, particularly when rooms are empty and at the end of the day.

Please document on the Monitoring Form below and return to the Data Protection Officer or School Business Manager.

Clear Screen and Desk Monitoring Form **Line Manager:**				
Date	**Name**	**Clear Desk**	**Clear Screen**	**Action Taken**