West Croft School

Data Protection Policy

Version: 1.1

Policy Date: 25th June 2021

Approved by: West Croft Governing Body

If you require help with the interpretation of this policy, please email the Data Protection Officer at:
dpo@devonmoorsfederation.devon.sch.uk
or
the school Data Protection Link Lead at:
dpo@westcroft.devon.sch.uk

Contents

Introduction and purpose

West Croft 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 UK data protection law.
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 UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by

- The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR. It also reflects the ICO's code of practice for the use of surveillance cameras 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.

The data controller

The school is the data controller for the personal data it processes and is registered with the Information Commissioner's Office (ICO) under registration number Z8611077. Details about this registration can be found at www.ico.org.uk and has paid its data protection fee.

The purpose of this policy is to explain how the school handles personal data under the data protection legislation, and to inform employees and other individuals who process personal data on the school's behalf, of the school's expectations in this regard.

This policy will be reviewed annually and shared with the full governing board.

This policy applies to the processing of personal data held by the school. This includes personal data held about pupils, parents/carers, employees, temporary staff, governors, visitors and any other identifiable data subjects. The policy applies to the processing of personal data which is defined by article 4 of the GDPR, and the processing of special categories of personal data defined by article 9 of the GDPR.

This policy and its supporting guidance shall apply to all West Croft School employees, agency and temporary staff, contractors, members and third-party staff, who have access to information systems or information used for school purposes.

This policy should be read alongside

- *E-Safety Policy - Pupil Acceptable Use Agreement*
- *Staff Acceptable Use Agreement*
- *Volunteer Acceptable Use Agreement*
- *Consent Form for Educational Activities*
- *Privacy Notices Pupil, Staff and Governor*
- *Consent Forms*
- *Disposal of Records Policy and Schedule*
    - *Keeping Children Safe in Education – Child Protection and Safeguarding*

West Croft School processes a variety of personal data to enable us to deliver a range of education services. Therefore, West Croft School is required to comply with the GDPR as well as other supporting legislation which governs the processing of personal data.

When handling and managing information the School and its staff shall comply with other legislation in addition to the GDPR, to include but not limited to:

- *Computer Misuse Act 1990*
- *Copyright Designs and Patents Act 1988*
- *Environmental Information Regulations 2004*
- *Equality Act 2010*
- *Freedom of Information Act 2000*
- *Human Rights Act 1998*
- *Local Government Act 1972*
- *Local Government Act 2000*
- *Regulation of Investigatory Powers Act 2016*
- *Re-use of Public Sector Information Regulations 2005*

Breach of this policy

All reckless or deliberate breaches of this policy will be investigated and may be referred to the Governing Board of West Croft School acting under the advice of Devon County Council's Human Resources Department. They will consider whether disciplinary action should be taken against the staff member concerned. Alleged breaches of this policy will also be investigated by the Data Protection Officer as an information security incident in accordance with the Security Incident Management Policy and Procedure and may also be referred to the Governing Board and senior management as considered necessary.

Policy review

This policy will be reviewed by the Data Protection Officer on an annual basis. Formal requests for changes should be sent to the Data Protection Officer:

Alvin Scott
Copplestone Primary School
Bewsley Hill
Copplestone
Crediton
EX17 5NX Email: dpo@devonmoorsfederation.devon.sch.uk

Definitions

There are several terms used in the data protection legislation and in this policy, which must be understood by those who process personal data held by the school. These are:

- *Personal data*
- *Special categories of personal data*
- *Processing*
- *Data subject*

- *Data controller*
- *Data processor*

Definitions Appendix 1.

West Croft School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore the data controller.

Roles and responsibilities

Responsibility for GDPR compliance rests with the Head Teacher. The Data Protection Policy and its supporting guides and standards are managed, maintained and communicated to staff by the Data Protection Officer.

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 the school implements this policy and continues to demonstrate compliance with the UK data protection legislation.

- *This policy shall be reviewed by the governing body on an annual basis.*

Head Teacher

The Head Teacher acts as the representative of the data controller and has day-to-day responsibility for ensuring this policy is adopted and adhered to by employees and other individuals processing personal data on the school's behalf.

Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with UK data protection law, and developing related policies and guidelines where applicable.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

The school's DPO is an external consultant who performs the role under a service contract through the Devon Moors Federation. The DPO can be contacted at: dpo@devonmoorsfederation.devon.sch.uk

The DPO is supported in their role by a school employee; known as the DPO's Data Protection officer Lead Link. All enquiries, complaints, requests and suspected breaches of security, should be referred to the Data Protection Lead Link Officer (dpo@westcroft.devon.sch.uk) in the first instance, who will then notify the DPO.

The DPO shall provide a report to the governing body and shall provide regular updates on the school's progress and compliance with the data protection legislation and recommendations on school data protection issues.

Employees, temporary staff, contractors, visitors

All employees, temporary staff, contractors, visitors and other individuals processing personal data on behalf of the school, are responsible for complying with the contents of this policy.

All individuals shall remain subject to the common law duty of confidentiality when their employment or relationship with the school ends. This does not affect an individual's rights in relation to whistleblowing.

Failure to comply with this policy may result in disciplinary action or termination of employment or service contract.

All 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.*

Contacting the DPO in the following circumstances:

- *With any questions about the operation of this policy, UK 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 need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside of the UK.*
- *If there has been a data breach*
- *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*

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.

Policy content

Data Protection Principles

The UK GDPR provides a set of principles which govern how the school handles personal data and is underpinned by six common-sense principles which governs the way that West Croft School must process personal data. These principles say that personal data must be:

- *Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').*
- *Collected for specified, explicit and legitimate purposes*
- *Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')*
- *Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')*
- *Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.*
- *Processed in a manner that ensures it is appropriately ('integrity and confidentiality').*

The school and all individuals processing personal data controlled by the school, shall comply with the data protection principles and follow when processing personal data to ensure compliance with each of the principles listed above.

Collecting Personal Data

Lawfulness, fairness and transparency

West Croft School and its staff only process personal data fairly and will not process personal data unless we have one or more of the lawful bases (legal reasons) to do so under the UK 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 into 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 or another person i.e. 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 or exercise its official authority***
- *The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided 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***

Special categories of personal data, will only be done where a lawful basis has been identified and meets one of the special category conditions for processing (for example, health or medical data, racial or ethnic origin or biometric data (e.g. facial images and fingerprints)), under UK data protection law:

- *The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent***
- *The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law***
- *The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent*
- *The data has already been made **manifestly public** by the individual*
- *The data needs to be processed for the establishment, exercise or defence of **legal claims***
- *The data needs to be processed for reasons of **substantial public interest** as defined in legislation*
- *The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law*
- *The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law*
- *The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.*

For criminal offence data, we will meet both a lawful basis and a condition set out under the UK data protection law. Conditions include:

- *The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent***
- *The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent*
- *The data has already been made **manifestly public** by the individual*
- *The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights***
- *The data needs to be processed for reasons of **substantial public interest** as defined in legislation*

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by UK data protection law.

West Croft School will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Limitation, minimisation and accuracy

The school 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 and will publish privacy notices which explain:

- *What personal data the school processes and why*
- *What our lawful basis is when we process that data*
- *Who we might share that data with*
- *How long we keep the data for*
- *What rights data subjects have in relation to their data*
- *Who our Data Protection Officer is and how to contact them*

The school shall ensure the personal data it processes is adequate, relevant and limited to what is necessary for the purpose(s) it was collected for.

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.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 record retention schedule.

Privacy Notices

The school's privacy notices shall be clear, concise and easily accessible. Privacy notices will be provided to parents/carers of pupils when their child is enrolled at the school, which will explain how the school handles pupil information. This privacy notice will be provided on an annual basis thereafter and will be published on the school's website.

Employees will be given a privacy notice explaining how the school handles employee information when they join the school, and annually thereafter.

The school shall provide privacy notices to other categories of data subjects, as appropriate.

When collecting personal data, West Croft School will make available the information contained in our Privacy Notice. This may be available online and referenced on data capture forms, directly referenced on documentation or provided verbally. If West Croft School receives personal data from third parties, we will ensure that the information contained in a privacy notice, is made available to a data subject as soon as practical. This will usually be at the first point we are required to communicate with the data subject.

Further advice on Privacy Notices is available from the School's Data Protection Officer.

Consent

Most of the school's processing of personal data will not require consent from data subjects (or their parents/carers as appropriate); as the school needs to process this data in order to carry out its official tasks and public duties as a school.

We will only collect personal data for specified, explicit and legitimate reasons.
West Croft School is only required to obtain someone's consent if there is no other legal basis for processing their personal data. If we are required to obtain consent, we will ensure that the following requirements are met:

- *The consent is freely given*
- *The person giving consent understands fully, what they are consenting to*
- *There must be a positive indication of consent (opt-in as opposed to opt-out)*
- *The person giving consent must be able to withdraw their consent at any time*
- *Consent should be documented so that it may be referred to in the future, if necessary*

Children under the age of 13 merit specific protection regarding their personal data. Such specific protection should apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data regarding children when using services offered directly to a child. If West Croft School is required to deliver such services to children, it will ensure that the requirements of article 8 of GDPR are met.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individual's parents/carers as appropriate) 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 the school relies on consent as its lawful basis, it shall ensure the person providing it has positively opted-in to the proposed activity and is fully informed as to what they are consenting to and any non-obvious consequences of giving or refusing that consent. Consent shall not be assumed as being given if no response has been received e.g. a consent form has not been returned.

Rights of Data Subject

GDPR outlines the rights afforded individuals in respect of the processing of their personal data. These rights are summarised below:

- *The right to transparency in respect of the processing of their personal data*
- *The right of subject access*
- *The right to rectification*
- *The right to erasure*
- *The right to restriction of processing*
- *The right to data portability*
- *The right to object to processing*
- *The right to request human intervention if processing is by automated means*

Requests to exercise any of these rights are managed by the Data Protection Officer. The School's procedures for managing such requests are available from the Data Protection Officer and shall be adhered to whenever West Croft School receives a request from someone wishing to exercise these rights.

When designing, implementing or procuring systems or services, West Croft School must ensure that those systems or services can allow members of the public to exercise any of the rights listed in section 11.1. Any systems or services found to be incapable of managing such requests should be referred to the Data Protection Officer and must be subject to a Data Protection Impact Assessment.

GDPR and procurement

West Croft School is committed to upholding the confidentiality, availability and integrity of information that is processed by our contractors on our behalf. The school's Data Protection Officer, IT Manager and Data Protection Link Officer shall assess the appropriateness of data processors before purchase of these services. Underpinning this commitment, we will ensure that the following measures are followed when procuring goods and services that involve the processing of personal data:

- A Data Protection Impact Assessment is undertaken prior to any significant new procurement which involves the processing of personal data
- A security assessment is completed to ascertain the technical and organisational measures that prospective contractors will put in place to protect the data that they will be processing on behalf of West Croft School. The result of this will inform the final decision as to whether or not the School contracts with that organisation.
- When procuring goods and services that require a formal procurement exercise, we will ensure that contractual provision is in place which clearly identifies the following: the identity of the data controller; the data being processed; the requirement for a record of processing activity (in accordance with article 30 of the GDPR); arrangements for how personal data will be disposed of or returned to the School at the end of the contract; contractual clauses which mandate conformance to the GDPR.

Records of processing activity

West Croft School will have measures in place to ensure that data processors responsible for processing personal data on behalf of the School will maintain records of processing as required by article 30 of the GDPR.

The school shall maintain a record of its processing activities in line with Article 30 of the GDPR. This inventory shall contain the following information:

- *Name and contact details of the school and its Data Protection Officer*
- *Description of the personal data being processed*
- *Categories of data subjects*
- *Purposes of the processing and any recipients of the data*
- *Information regarding any overseas data transfers and the safeguards around this*
- *Retention period for holding the data*
- *General description of the security in place to protect the data*

Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 UK data protection law*
- *Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share*
- *Only share data that the supplier or contractor needs to carry out their service*

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

We may 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 internationally, we will do so in accordance with UK data protection law.

Joint Controller Agreements

The school shall sign up to agreements with other data controllers where personal data is shared or otherwise processed on a regular basis, where it is necessary to do so.

Data Security and Storage of Records

Accuracy of data

The school shall take all reasonable efforts to ensure the personal data it holds is accurate and where necessary kept up to date. Where personal data is found to be inaccurate, this information will be corrected or erased without delay.

- *The school will send reminders, on at least an annual basis, to parents/carers, pupils and employees, to remind them to notify the school of any changes to their contact details or other information*
- *The school shall carry out sample checks of pupil and employee files containing personal data, to ensure the data is accurate and up to date. This will be carried out on an annual basis.*

Security incident management and notification

An information security incident can occur when the confidentiality, availability and/or integrity of personal data is put at risk. Examples of activities considered an information security incident might include: information being at risk of being, or actually being; lost; stolen; disclosed to the wrong recipient (accidentally or deliberately); accessed, or attempted to be accessed, unlawfully and/or without the permission of the School; sold or used without the permission of the School; irretrievable indefinitely or for a long period of time as the result of a malfunction of a system containing personal data or sensitive business data.

In accordance with article 33 of the GDPR, West Croft School is committed to notifying the Information Commissioner's Office or relevant supervisory authority within 72 hours of being notified of an information security incident that might adversely affect the rights and freedoms of a data subject.

Notifications of this nature are the responsibility of the Data Protection Officer, who will ensure that the risks associated with information security incidents are recorded, monitored and, where appropriate, escalated.

Data security and storage of records

West Croft School shall keep personal data for no longer than is necessary for the purpose(s) of the processing.

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 or incinerate 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 the UK data protection law.

The school shall adhere to the schools Record Retention Schedule and ensure the disposal of personal data securely and at the end of the retention period appropriately.

The school shall have appropriate security in place to protect personal data against unauthorised or accidental access, disclosure, loss, destruction or damage. This will be achieved by implementing appropriate technical and organisational security measures

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. 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

The school shall implement proportionate security measures to protect its network and equipment and the data they contain. This includes, but is not limited to:

- *having a Firewall, anti-virus and anti-malware software in place*
- *applying security patches promptly*
- *restricting access to systems on a 'need to know' basis*
- *use of strong passwords*
- *regularly backing up data*
- *regularly testing the school's disaster recovery and business continuity plans, to ensure data can be restored in a timely manner in the event of an incident*

Organisational security measures

The school will ensure additional measures to protect personal data:

- *Signed confidentiality clauses as part of their employment contract*
- *Data protection awareness training and GDPR updates*

- *Policies and guidance relating to the handling; access, storage and disposal of personal data whilst during and outside of school.*
- *Data protection compliance shall be a regular agenda item in governing body and Senior Leadership Team meetings.*
- *Appropriate equipment and secure systems in place to protect personal data.*
- *Procedures shall be in place for visitors coming onto the school's premises. These will include signing in and out at reception, wearing a visitor's badge and being escorted by a school employee (unless the visitor holds a valid Disclosure and Barring Service certificate, or it is otherwise appropriate for the person not to be escorted).*
- *Procedures in place to identify, report, record, investigate and manage personal data breaches in the event of a security incident.*
- *Subject Access Request procedures and management.*

Subject access requests (SAR) Handling requests

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing to West Croft School, Coronation Road, Bideford, Devon EX39 3DE or emailed to:

DPO link at: dpo@westcroft.devon.sch.uk or the school's DPO at: dpo@devonmoorsfederation.devon.sch.uk

Please include:

- *Name of individual*
- *correspondence address*
- *contact number and email address*
- *details of the information requested.*

Verbal Subject Access Requests; the school will write to confirm to ensure information requested is accurate following GDPR principles.

Staff who receive a subject access request in any form must immediately inform the DPO link officer or the school DPO.

Data subjects who request a copy of their personal data (known as making a Subject Access Request) may be asked to provide identification to satisfy the school of their identity, particularly where the data subject is no longer a pupil, employee or governor at the school. These requests shall be responded to within 1 month, upon receipt of receiving a valid request and appropriate identification (required to confirm identity where requested).

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.

The Information Commissioners' Office (ICO) and the Department of Education (DofE) guidance, suggests that children aged 13 years and above, may have sufficient maturity in these situations, however it is up to the school to decide this on a case by case basis.

Parents/carers can make a request for their child's information when their child is 12 years and under. If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

Where the child attends a maintained school, a parent can request a copy of their child's educational record. The parent/carer does not need consent from the child to access this information. This type of request is governed by the Education (Pupil Information) (England) Regulations 2005.

Responding to subject access requests

When responding to Subject Access Requests or pupil information requests, the school shall redact the information the data subject or parent/carer is not entitled to receive, in accordance with the exemptions set out in the Data Protection Act 2018.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

The school shall consult with the Data Protection Officer upon receipt of a Subject Access Request or pupil information request, and again prior to making disclosures in response to these 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 (or receipt of the additional information needed to confirm identity, where relevant)*
- *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 may not disclose information for a variety of reasons, such as if it:

- *Might cause serious harm to the physical or mental health of the pupil or another individual*
- *Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests*
- *Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it*
- *Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts*

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will consider whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

Other data protection rights of the individual

In addition to the right to make a subject access request and to receive information when we are collecting their data about how we use and process it, 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 (in certain circumstances)*
- *Prevent use of their personal data for direct marketing*
- *Object to processing which has been justified on the basis of public interest, official authority or legitimate interests*
- *Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)*
- *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 DPO link or DPO. If staff receive such a request, they must immediately forward it to the DPO school link or DPO.

Parental requests to 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 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

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.

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 explain how the photograph and/or video will be used to both the parent/carer and pupil. (Publicity Permissions and Educational Activities Consent Form)

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the school takes photographs and videos, uses may include:

- *Within school on notice boards and in school magazines, brochures, newsletters, etc.*
- *Outside of school by external agencies such as the school photographer, newspapers, campaigns*
- *Online on our school website 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 child, to ensure they cannot be identified.

Data protection by design and default

The school shall have appropriate technical and organisational measures in place which are designed to implement the data protection principles in an effective manner, and will ensure that by default, it will only process personal data where it is necessary to do so. The school's Data Protection Policy and supplementary policies, procedures and guides, explain how the school aims to achieve this. We will put measures in place by:

- *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 UK data protection law (see section 6)*
- *Completing data protection 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*
- *Training members of staff on UK data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance*
- Passwords to meet current guidance of numeric and letter characters to be used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- *Conducting reviews and audits to test our privacy measures and make sure we are compliant*
- *Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different UK data protection laws will apply*
- *Maintaining records of our processing activities, including:*
- *For the benefit of data subjects, making available the name and contact details of our school DPO link and DPO and all information we are required to share about how we use 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure*

Data processors

The school shall carry out checks with prospective data processors (e.g. suppliers providing goods or services which involve the processing of personal data on the school's behalf) to assess they have appropriate technical and organisational measures that are sufficient to implement the requirements of the data protection legislation and to protect the rights of data subjects.

The school's Data Protection Officer, IT Manager and Data Protection Link Officer shall assess the appropriateness of data processors before the school purchases their services. A record will be kept of their findings.

The school shall ensure there are appropriate written contracts/Terms of Service in place with data processors, which contain the relevant clauses listed in Article 28 of the GDPR.

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 3.

The school shall have procedures in place to identify, report, record, investigate and manage personal data breaches (i.e. security incidents involving personal data). These include security incidents resulting in the:

- *unauthorised or accidental disclosure or access to personal data*
- *unauthorised or accidental alteration of personal data*
- *accidental or unauthorised loss of access or destruction of personal data*

Personal Data breach procedure - Appendix 3

All incidents will be recorded in the school's data breach log and investigated by GDPR school link officer under the support and direction of the school's Data Protection Officer.

Notification to the ICO and Data Subjects

- The Data Protection Officer shall determine whether the school must notify the Information Commissioner's Office and data subjects.

- Where a breach is likely to result in a risk to the data subject, for example if they could suffer damage, discrimination, disadvantage or distress as a result of the breach, the school shall notify the Information Commissioner's Office (ICO) *within 72hrs* of becoming aware of the breach.

- If the breach is likely to result in 'high risks' to data subjects, for example if the breach could lead to identity theft, psychological distress, humiliation, reputational damage or physical harm, the school shall inform the data subject promptly and without delay.

- When informing a data subject of a personal data breach involving their personal data, the school shall provide in clear, plain language the:

    - *nature of the incident*
    - *name and contact details of the Data Protection Officer*
    - *likely consequences of the breach*
    - *actions taken so far to mitigate possible adverse effects*

Actions to minimise the impact of data breaches Appendix 3

Data Protection Impact Assessments

The school shall carry out Data Protection Impact Assessments (DPIAs) for the processing of personal data, where this is likely to result in high risks to the rights and freedoms of data subjects, particularly when using new technologies. This includes, but is not limited to the following activities:

- *Installing and using Closed Circuit Television (CCTV)*
- *Sharing personal data or special category data with other organisations*
- *Using mobile Apps to collect or store personal data, particularly about children*
- *Storing special category data in the 'Cloud'*
- *Using systems that record large volumes of personal data, particularly where data processors are involved*

The results from DPIAs shall be recorded and shared with the Data Protection Officer, who will advise on any privacy risks and mitigations that can be made to reduce the likelihood of these risks materialising. The Data Protection Officer will monitor the outcome of the DPIA, to ensure the mitigations are put in place.

Appendix 2

Appointment of a Data Protection Officer

The school shall appoint a Data Protection Officer to oversee the processing of personal data within the school, in compliance with Articles 37-38 of the GDPR. This person shall be designated on the basis of professional qualities and in particular, expert knowledge of the UK data protection law and practices and the ability to fulfil the tasks referred to in Article 39 of the GDPR.

The school shall publish the contact details of the Data Protection Officer and communicate these to the Information Commissioner's Office.

14. Policy history

Policy Version and Date	Summary of Change	Amended by	Implementation Date
Version 1.1 25th May 2018	This policy replaces the school's existing Data Protection Policy	K D K.D	25th May 2018 25th May 2020 25th May 2021

Declaration

I confirm that I have read, understood and shall adhere to West Croft Schools Data Protection Policy Version 1.0, dated 25 May 2021 and the supporting policies and procedures referred to in this policy.

Name:	
Job title:	
Date:	
Signature:	

Instructions for school admin

This declaration must be kept in an easily retrieval file. In the case of an employee, this should be kept on their personnel file.

Appendix 1

Data Protection Policy Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living 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 living 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 to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

West Croft School

Title: [*Insert short description of the proposed activity involving personal data]* **Assessment carried out by:** [*Insert name*]

Part 1 – DPIA Overview

1. **Explain why you believe the proposed activity requires a DPIA?** N.B Refer to the '*Do you need a DPIA*' document if relevant	
2. Describe the personal data that will be processed during this activity and the number of living individuals that will be identifiable.	
3. Who have you consulted as part of this DPIA? N.B It may be useful to consult the opinion of IT; Legal; Human Resources or Senior Management Team (as required) when considering the potential risks to the proposed activity.	
4. Explain why the proposed activity is considered necessary and list the business or other benefits of carrying it out.	
5. What are the potential risks associated with this activity? N.B Refer to the '*Identifying privacy and other risks'* document and the answers you provided in your DPIA Questionnaire.	
6. What steps do you propose to take to reduce the likelihood of the risks you have identified? N.B Refer to the *'Reducing Privacy Risks'* document and the answers given in your DPIA Questionnaire.	

Part 2 – Data Protection Officer's analysis

Part 3 – Agreed actions

Actions	Owner
1.	
2.	
3.	
4.	

Appendix 3: 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 or data processor must immediately notify the DPO link officer. (dpo@westcroft.devon.sch.uk Tel No: 01237 473548) or if unavailable dpo@devonmoorsfederation@devon.sch.uk .

The DPO link will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether 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*

Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation

If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors

- The DPO 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 DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will determine 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*
    - *Identify theft or fraud*
    - *Financial loss*
    - *Unauthorised reversal of pseudonymisation (for example, key-coding)*
    - *Damage to reputation*
    - *Loss of confidentiality*
        - *Any other significant economic or social disadvantage to the individual(s) concerned*

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

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 on the school's computer system, and/ or paper copies in locked admin cupboard.

Where the ICO must be notified, the DPO will do this via the 'report a breach' self-assessment tool of the ICO website, or through their breach report line (0303 123 1113), 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 report 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 all individuals whose personal data has been breached. This notification will set out:

- *A description, in clear and plain language, of the nature of the personal data breach*
- *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*
- *As above, any decision on whether to contact individuals will be documented by the DPO.*
- *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 based on the investigation*
- *The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:*
- *Facts relating to the breach*
- *Effects*
- *Action taken 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 held by the DPO or stored on the school's computer system, and/ or paper copies in locked admin cupboard and recorded in the school's data breach log.*
- *The DPO link will review the data breach incident with recommendations to prevent and reduce the risk of happening again as soon as reasonably possible.*
- *The DPO and headteacher will liaise to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches*

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO school link or DPO as soon as they become aware of the error*
- *In any cases where the recall is unsuccessful or cannot be confirmed, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*

- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy for evidence)*
- *The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*
- *If safeguarding information is compromised, the DPO will inform, the designated safeguarding lead and discuss whether to inform other safeguarding partners.*

Other types of breach may include:

- *Details of pupil premium interventions for named children being published on the school website*
- *Non-anonymised pupil exam results or staff pay information being shared with governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's cashless payment provider being hacked and parents' financial details stolen*
- *Hardcopy reports sent to the wrong pupil families.*