Data Protection Policy 2019/20

Signed	

Chair of the Board of Directors

Date approved:	
Approved by:	
Version:	**1.2**
Date for Review	**November 2020**

Version History

Version	Date Issued	Brief Summary of Change	Owners Name
0.1	**3-05-18**	New Policy	Russell Muir
1.1	**11-11-19**	Policy Updated	Salima Khan

1. Context and Overview

This Policy sets out The Complete Works commitment to handling personal data in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

This policy applies to the processing of personal data held by The Complete Works. This is collected about staff, pupils, parents, governors, visitors and other individuals is collected,

The Complete Works is the data controller for the personal data it processes and is registered with the Information Commissioner's Office (ICO). This registration will be renewed annually or as otherwise legally required. Details about this registration can be found at www.ico.org.uk.

2. Legislation and guidance

The Complete Works needs to gather and use certain personal information about individuals. This can include learners, parents, staff and Governors.

All data must be collected, stored and managed in accordance with UK and EU law, and in line with our school ethos and values. Individuals retain the rights over their own data at all times. Our use of their data must be fair and lawful, and we must be open and honest about what we do with people's data.

All data we process is in accordance with the rules as laid down in statute, including the General Data Protection Regulations, the Data Protection Act 2018, all Education Acts and Regulations, and the Apprenticeship, Skills, Children and Learning Act 2009.

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

It 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.

3. 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 individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and 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.

4. Roles and responsibilities

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

4.1 Board of Directors

The Board of Directors has overall responsibility for ensuring that The Complete Works implements this Policy and continues to demonstrate compliance with data protection legislation.

4.2 Headteacher

The Head Teacher has day-to-day responsibility for ensuring this policy is adopted and adhered to by staff and other individuals processing personal data on behalf of their school.

4.3 Data Protection Officer

The Data Protection Officer (DPO) is responsible for carrying out the tasks set out in Article 39 of the General Data Protection Regulation (the GDPR). The DPO is responsible for:

- informing and advising the school of their obligations under the data protection legislation;
- monitoring compliance with data protection policies;
- raising awareness and delivering training to employees;
- carrying out audits on the school's processing activities;
- providing advice regarding Data Protection Impact Assessments and monitoring performance;
- co-operating with the Information Commissioner's Office;
- acting as the contact point for data subjects exercising their rights.

They will provide an annual report of their activities directly to the Board of Directors and, where relevant, report to the Board their advice and recommendations on school data protection issues.

The DPO for The Complete Works is Tim Bridger who can be contacted via email at timbridgerconsulting@gmail.com

4.4 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;
- Contacting the DPO 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 need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
    - If there has been an actual or potential 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.

5. Key principles

- Individuals retain rights over their data
- Data should be collected fairly and lawfully and used only in ways that the individual would expect
- Data should only be kept for as long as is necessary
- Data integrity and security is paramount

- Data governance will be actively managed at all levels of the organisation, to minimise risks to both the individual and the organisation
- All collection and use of data will be open and honest

6. Why this Policy exists

This policy will help ensure that The Complete Works respects the rights of all individuals whose data it collects, including learners, parents, staff and Governors. It encompasses legal responsibilities and best practice. By being open and honest with individuals we will demonstrate that people can trust our organisation and that we handle personal data with integrity. Routine application of these principles will also help protect The Complete Works from the risk of data breaches and unauthorised access to personal information.

7. Our Privacy Notice

The Complete Works will take all reasonable steps to ensure that individuals are aware their data is being processed. This will include telling individuals what is being used, how it is being used, how long it will be kept for, and how they can exercise their rights in respect of that data.

Our Privacy Notice sets out how we collect data, what data we collect, the lawful basis for that, and how long we retain it. It includes information on who we share data with and the lawful basis for such sharing. It also sets out how people can request copies of data we hold about them. The Notice will be included in any marketing or information literature we produce. It will also be available on request, and on our website.

8. Keeping Personal Data Secure

Once personal data has been lawfully and fairly collected and processed, it must be safely stored, kept up to date, and safely accessed. Storing data in a way that complies with the regulations is a mix of common sense, clear processes and application of strong IT solutions.

The only people who will have access to personal data at The Complete Works are those who need it for their work. Our IT systems and file storage will have granular levels of permission, and we will ensure that people only see personal data if required for operational reasons and for the benefit of teaching and learning.

Strong passwords must be used to access electronic resources and IT systems. These should never be shared with other people, or written down. The Complete Works will set an appropriate password policy and require passwords to be changed on an annual basis.

Personal data must only be disclosed to those who are authorised to see it, both within and outside the organisation. If there is any doubt about the identity the person requesting access to information, or doubt as to whether they should be allowed to see it, we will not disclose information.

Data will only be shared with those people who are authorised to see it. This will be in line with our legal obligations and with the lawful and legitimate requirements of the business. Our Privacy Notice explains who we might share data with, the lawful basis for that, and the circumstances in which data subjects can object to data being shared.

Full training for all staff will be available. This will help them understand their responsibilities under data protection legislation. Staff should ask their line manager or the Data Protection Officer for guidance if they are unsure about any aspect of data protection.

Data use and transfer

Data must only be used for the purpose it was first obtained. Personal data should not be shared informally, either internally or externally to the organisation.

Staff should follow simple checks when transferring data outside the organisation via post or email, to ensure that personal data goes to the correct recipient. The Complete Works will use a simple checklist when sending personal data by post, to add an extra layer of security and checking to our data transfers.

Extra care will always be taken when sharing data via email. The Complete Works uses encrypted email and a secure email client to ensure that data is shared securely and appropriately.

School data is never stored on personal IT devices. In particular staff must not email school documents to their personal email addresses. If data needs to be transferred outside of the secure school environment, staff should use their school email account or secure cloud storage solution provided by the ICT department.

9. Getting your Consent to Process Personal Data

There may be times where we would like to process your data in a way that requires your consent. This could include taking photographs or images of you engaging in school activities, or adding your contact details to any marketing or promotional mailing lists

SCHOOL will ensure that we obtain your consent in a positive and clear way. You will be able to refuse consent, and that will not impact your ability to join in the full range of activities and opportunities within the school. We will also ensure that you can withdraw consent quickly and easily, should you change your mind about us processing your data in these ways.

10. 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, and we will allow parents and carers to choose what use should be made of these images.

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.

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.

11. Subject access requests and other rights of individuals

11.1 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;
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing;
- The right to lodge a complaint with the ICO or another supervisory authority;
- 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;
- The safeguards provided if the data is being transferred internationally.

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 and include:

- Name of individual;
- Correspondence address;
- Contact number and email address;
- Details of the information requested.

If staff receive a subject access request in any form they must immediately forward it to the DPO.

11.2 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.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Most subject access requests from parents or carers of pupils of primary school age may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Parents, as defined under Education Law, have a right to be involved in decisions related to their child's education. This includes receiving an annual report of progress in the main subjects taught. As an independent school, The Complete Works is not legally obliged to provide parental access to student's School Record, but may agree to do so in certain circumstances, upon request, such as if a student is being excluded.

11.3 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 30 days of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant);
- 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 30 days, 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 take into account 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.

11.4 Other data protection rights of the individual

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 section 7), 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. If staff receive such a request, they must immediately forward it to the DPO.

12. Parental requests to see the educational record

As an independent school there is no automatic parental right of access to the educational records of a pupil. However, all reasonable requests will be considered by the Headteacher. Requests will need to be made in writing directly to the Headteacher.

13. CCTV

We may use CCTV in some locations around our education establishments to ensure they remain 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.

Any enquiries about the CCTV system should be directed to the Data Protection Officer.

14. Sharing Personal Data

We will not normally share personal data with anyone else's 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 may 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;
    - 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 data protection law.

15. 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 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 data protection law.

Document retention guidance can be found in Appendix 2.

16. 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 an appropriate data breach procedure, as advised by the ICO.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it.

17. Training

All Staff and Directors 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.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and shared with the Board of Directors.