Data Protection Policy

Cantell SCHOOL

2020/21

Data Protection Policy

Statutory/Non-Statutory:	Statutory
Approval Level:	Whole Governing Body
Approved by Governing Body on:	
Author:	Keith Pinney School Business Manager

Review Date: May 2020

Next Review Date: May 2022

Cantell – An exceptional school experience:
Academic excellence / Exciting teaching & learning
Life-changing opportunities / A richly diverse community

Contents

1. Aims

Cantell 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.

2. 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 (ICO) 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 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, 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 to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, 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.

5. 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.

5.1 Governing board

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

5.2 Data protection officer

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

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

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

Our DPO is Keith Pinney and is contactable via email at keith.pinney@cantell.co.uk

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 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, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;

- 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.

6. 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 specified, 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.

7. Collecting personal data

7.1 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 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 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 (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**.

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 get parental consent (except for online counselling and preventive services).

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

7.2 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.

8. 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;
    - 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 that 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 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 to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 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;
- 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 or email to the DPO. They should include:

- Name of 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 DPO.

9.2 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. Therefore, most subject access requests from parents or carers of pupils at this 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.

9.3 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 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.

9.4 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, 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 (decisions 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. 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.

11. Privacy Notices

When information is collected about individuals, they must be made aware of the Privacy Notices (see **Appendix 1 and 2**). The Privacy Notice provides information about what, why and how information is processed. You should make yourself aware of the Privacy Notice, which should be read in line with this policy.

12. 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.

Any enquiries about the CCTV system should be directed to Keith Pinney, School Business Manager.

13. 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, etc.

- Outside of school by external agencies such as the school photographer, newspapers, Aspire Trust
- Online on our School website

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.

See our child protection and safeguarding policy for more information on our use of photographs and videos.

14. 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 section 6);
- 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 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

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.

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;
- Where personal information needs to be taken off site, staff must protect it and keep it with them at all times;

- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals;
- Encryption software is used to protect all 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 Acceptable Use policy)
- 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 (see section 8).

16. 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.

17. 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** and complete the reporting form found in **Appendix 4.**

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 unauthorized person;
- The theft of a school laptop containing non-encrypted personal data about pupils.

18. 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.

19. Monitoring arrangements

The DPO is 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 board.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information policy
- Child protection and safeguarding policy
- Acceptable Use policy

Appendix 1: Privacy Notice (Staff)

Privacy Notice
(Staff)
How we use School Workforce information

Introduction

1. This notice is to help you understand **how** and **why** we collect personal information about you and **what** we do with that information. It also explains the decisions that you can make about your own information.

2. Cantell School is ultimately responsible for how the School handles your personal information. In this privacy notice, we use the term School to mean Cantell School.

3. If you have any questions about this notice, please contact the Data Protection Officer (DPO), Keith Pinney, School Business Manager.

4. This notice is aimed at all staff (including Governors, volunteers and certain contractors), Supply/agency staff and applicants for employment vacancies. This privacy notice does not form part of your contract of employment and the School may amend this notice at any time.

What is personal information?

5. Personal information is information which is about you and from which you can be identified.

6. This includes your contact details, next of kin and financial information. We may also hold information such as your religion or ethnic group. CCTV, photos and video recordings of you are also personal information.

What personal information does the School hold about you and how is this obtained?

7. We set out below examples of the personal information the School holds about you and where this personal information comes from.

8. Information about you is gathered during the recruitment process:

Such as information about your education, qualifications and professional achievements;

You will provide certain information to us, for example, on your application form and during any interviews;

We may obtain information from publicly available sources such as your social media profiles;

We will receive your personal information (from you and third parties) when we carry out pre-employment checks, for example, when we receive references, confirmation of your fitness to work, your right to work in the UK and criminal records checks.

9. We will hold information about your job performance. This includes information about skills, achievements, career progression, performance and disciplinary related matters and information relating to the School's appraisal procedure.

10. We hold and use your financial information, such as, your bank details, your salary and pension details.

11. We will hold information about any physical or mental health condition you may have, which is disclosed to the School during the recruitment process or at any stage during your employment.

12. We will hold information about any protected characteristics you may have (e.g. a disability) which you provide, for example on the Equal Opportunities Monitoring Form.

13. Your personal information may be created internally by the School during the course of your employment. An email from the Head to a member of staff complimenting them on class management would be an example of this.

14. Your personal information may be acquired from outside of the School such as from Occupational Health practitioners or from public authorities such as the Police or the Local Authority Designated Officer.

15. Pupils may provide us with your personal information, for example, if a pupil emails their tutor to say how much you are helping them with their work.

Why does the School use your personal information?

16. We commonly use personal information for:

Ensuring that we provide a safe and secure work environment;

Providing employment services (such as payroll and references);

Providing training and support;

Protecting and promoting the Schools' interests and objectives (including fundraising);

Personnel, administrative and management purposes and to enable us to meet our legal obligations as an employer. For example, to pay staff and to monitor their performance;

Safeguarding and promoting the welfare of all staff and pupils;

Fulfilling our contractual and other legal obligations.

17. Some specific examples of when the School uses your personal information are set out below:

We use your personal information to consider your suitability to work in your role at the School;

We will check that you have the right to work in the UK by reviewing your identification documents and keeping copies on your personnel file;

We may use your personal information in addressing performance or disciplinary concerns;

We will use information relating to any medical condition you may have in order to verify fitness to work, monitor sickness absence and comply with our duty of care towards you;

We may use your information when dealing with complaints and grievances (e.g. from other staff and parents);

We may use information about you and photographs and video recordings of you for marketing and promotion purposes including in School publications, in social media and on the School website;

We may use your information to enable the development of a comprehensive picture of the workforce and how it is deployed;

We may use your information to inform the development of recruitment and retention policies;

We may also allow external publication of certain media where appropriate (for example, a photograph or article in a local newspaper);

We may also make recordings for teaching purposes, for example, recording a drama lesson to provide feedback to you or pupils. We may also record lessons for pupils who were not able to attend in person;

We use CCTV recordings for the purposes of crime prevention and investigation and also in connection with our obligation to safeguard the welfare of pupils, staff and visitors to the School site;

The School regularly monitors and accesses its' IT system for purposes connected with the operation of the School. The IT system includes any hardware, software, email account, computer, and device or telephone provided by the School or used for School business. The School may also monitor staff use of the telephone system and voicemail messages. Staff should be aware that the School may monitor the contents of a communication (such as the contents of an email).

The purposes of such monitoring and accessing include:

To help the School with its day to day operations. For example, if a member of staff is on holiday or is off sick, their email account may be monitored in case any urgent emails are received;

To check staff compliance with the School policies and procedures and to help the School fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to send abusive or inappropriate messages.

Monitoring may be carried out on a random basis or it may be carried out in response to a specific incident or concern.

The School may use software which automatically monitors the IT system (for example, it would raise an alert if a member of Staff visited a blocked website or sent an email containing an inappropriate word or phrase).

The monitoring is carried out by the School. If anything of concern is revealed as a result of such monitoring, then this information may be shared with the Headteacher/Line Manager and this may result in disciplinary action. In exceptional circumstances concerns may need to be referred to external agencies such as the Police.

How does the School share staff personal information with third parties?

18. We may need to share your information with the Disclosure and Barring Service (**DBS**) or the National College for Teaching and Leadership (**NCTL**) when carrying out safer recruitment checks or in making a referral to the DBS or the NCTL.

19. We may need to share your information with UK Visas and Immigration **(UKVI)** in order to sponsor you as an employee if you are from outside of the European Economic Area and to meet the School's sponsorship duties.

20. Occasionally we may use consultants, experts and other advisors (including legal advisors) to assist us in fulfilling our obligations and to help run the School properly. We might need to share your information with them if this is relevant to the work they carry out.

21. In accordance with our legal obligations, we may share information with Ofsted, for example, during the course of an inspection and may need to share your information with the Department for Education.

22. We may share some of your information with our insurance company or benefits providers, for example, where there is a serious incident.

23 If the School is dealing with a complaint or grievance (e.g. from a parent) we may share your information with other parties, for example, the appropriate staff at the School, the parents making the complaint and governors.

24. We may share your information with individuals connected to the School who are exercising their data protection rights, for example, when responding to a Subject Access Request.

25. We may share personal information about staff with the relevant statutory agencies who may need this information to investigate allegations of misconduct.

26. We may need to share your information with the police for the prevention and investigation of crime and the prosecution of offenders.

27. CCTV recordings may be disclosed to third parties such as the police.

28. We may share your information with parents and pupils where this is related to your professional duties.

29. We may need to share your information if there is an emergency, for example, if you are hurt in an accident.

30. We sometimes use contractors to handle personal information on our behalf. The following is an example:

Strictly Education – our Payroll Provider.

For how long does the School keep staff personal information?

31. We keep your information for as long as we need to in relation to your employment. We will keep some information after you have left the School in case this is needed, for example, in relation to our legal obligations and provide references.

Processing in line with your rights

32. From May 2018 data protection legislation gives you a number of rights regarding your information. Some of these are new rights whilst others build on your existing rights. Your rights are as follows:

If information is incorrect you can ask us to correct it;

You can also ask what information we hold about you and be provided with a copy. We will also give you extra information, such as why we use this information about you, where it came from and what types of people we have sent it to;

You can ask us to delete the information that we hold about you in certain circumstances. For example, where we no longer need the information;

You can ask us to send you, or another organisation, certain types of information about you in a format that can be read by computer;

Our use of information about you may be restricted in some cases. For example, if you tell us that the information is inaccurate we can only use it for limited purposes while we check its accuracy.

You also have the right to:

Object to processing of personal data that is likely to cause, or is causing, damage or distress;

Prevent processing for the purpose of direct marketing;

Object to decisions being taken by automated means;

In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and claim compensation for damaged caused by a breach of the Data Protection regulations.

Our legal grounds for using your information

33. This section contains information about the legal basis that we are relying on when handling your information as described above.

Contractual obligation

We will need to use your information in order to comply with our contractual obligations. For example:

- We need your name and bank details so that we can pay you your salary;
- We may need to provide your personal information to a pension provider;
- We also need to use your personal information to provide contractual benefits.

Legal obligation

We have to comply with various laws and this entitles us to use your information where necessary. For example:

- We have to make sure that you have the right to work in the UK;
- To fulfil our duty of care to you and your colleagues;
- We have to fulfil our safeguarding duties towards pupils;
- We may be legally obliged to disclose your information to third parties such as the DBS, local authorities or the police.

Performance of a task carried out in the public interest

We use your information for a variety of reasons in the public interest, for example:

- Facilitating our teaching requirements, for example, to help us decide which member of staff will teach a particular class based on skills, experience, qualifications etc.;
- Looking after your welfare and development and the welfare and development of others;
- Safeguarding and promoting the welfare of our pupils;
- Ensuring the security of the School site, which may involve issuing you with a photocard;
- Making sure that you are complying with your employment obligations;

If you object to us using your information when we are relying on the grounds above please speak to the DPO.

34. The School must also comply with an additional condition where it processes special categories of personal information. These special categories are as follows: personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic information, biometric information, health information, and information about sex life or orientation. The grounds that we are relying on to process special categories of personal data are set out below:

Employment, social security and social protection

The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the staff in the field of employment, social security or social protection.

Vital interests

To protect the vital interests of any person where that person cannot give consent, for example, if they are seriously hurt and are unconscious.

Legal claims

The processing is necessary for the establishment, exercise or defence of legal claims. This allows us to share information with our legal advisors and insurers.

Medical purposes

This includes medical treatment and the management of healthcare services.

35. We may ask for your consent to use your information in certain ways. If we ask for your consent to use your personal information you can take back this consent at any time. Any use of your information before you withdraw your consent remains valid. Please speak to the DPO if you would like to withdraw any consent given.
In some cases, we will rely on more than one of the grounds above for a particular use of your information. For example, we may rely on legitimate interests and public interest grounds when using your information to safeguard our pupils.

Further information

36. **Contact:** If you would like any further information about anything within this notice please contact the School's Data Protection Officer, Keith Pinney, School Business Manager.

37. Please speak to the Data Protection Officer if:

- You object to us using your information for marketing purposes e.g. to send you information about school events;
- You would like us to update the information we hold about you;
- You would prefer that certain information is kept confidential.

38. **If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us, in the first instance with the DPO, secondly with the Headteacher and lastly with the Chair of Governors, but if you consider that we have not acted properly when using your personal information, or responded adequately to your concerns, you may contact the Information Commissioner's Office at ico.org.uk.**

Appendix 2: Privacy Notice (Pupils)

Privacy Notice (How we use pupil information)

Under Data Protection law, individuals have a right to be informed about how the School uses any personal data that we hold about them. We comply with this right by providing access to 'privacy notices' where we are processing personal data.

This privacy notice explains how we collect, store and use personal data about pupils.

We, Cantell School, Violet Road, Southampton, Hants SO16 3GJ are the 'data controller' for the purposes of data protection law.

Our Data Protection Officer is Keith Pinney, School Business Manager (see 'Contact us' below).

Why do we collect and use pupil information?

We collect and use pupil information under:

General Data Protection Regulation (EU) 2016/679 (from 25th May 2018)

- Article 6(1)(e) – the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Article 9(2)(g) – the processing is necessary for reasons of substantial public interest.

We use the pupil data:

- to support pupil learning;
- to monitor and report on pupil progress;
- to assess pupils;
- to provide appropriate pastoral care;
- to protect pupil welfare and carry out safeguarding activities;
- to assess the quality of our services;
- to comply with the law regarding data sharing.

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number, address, date of birth, identification documents);
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility);
- Attendance information (such as sessions attended, number of absences and absence reasons);
- Eligibility information, such as for Free School Meals and Pupil Premium;
- Academic progress / assessment data;
- Relevant medical information;
- Special Educational Needs information;
- Exclusions / behavioural information;
- Safeguarding information;

- Fingerprints for those who wish to be included in the Cashless Catering system;
- Photographs, CCTV images and videos.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis in support of exercising our official tasks. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school in accordance with the Southampton City Council Records and Retention Schedule: http://www.southampton.gov.uk/Images/RRRS-version-9.000_tcm63-389236.pdf

Who do we share pupil information with?

We do not share information about pupils with any third party without consent unless the laws and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share pupil information with:

- Schools / other education providers;
- our Local Authority;
- the Department for Education (DfE);
- the NHS;
- other Local Authorities;
- our regulator (Ofsted);
- Police forces, courts and tribunals.

For further details, please see “Why do we collect and use pupil information?” above.

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils’ data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our Local Authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information about Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform

independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Keith Pinney, School Business Manager who will make the necessary arrangements.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;

- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and;
- claim compensation for damages caused by a breach of the Data Protection regulations.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance and if not satisfied, directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact:

If you would like to discuss anything in this privacy notice, please contact:

- The Data Protection Officer Keith Pinney, School Business Manager – finance@cantell.co.uk

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

www.youngsouthampton.org/privacynotice.aspx and
http://media.education.gov.uk/assets/files/doc/w/what%20the%20department%20does%20with%20data%20on%20pupils%20and%20children.doc
http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

- If you are unable to access these websites we can send you a copy of this information.

Please contact the LA or DfE as follows:

- **Solicitor for Education:** Legal Services, Southampton City Council, Ground Floor, Civic Centre, SO14 7LY

- **Public Communications Unit:** Department for Education, Sanctuary Buildings, Great Smith Street, London, SW1P 3BT

  Website: www.education.gov.uk

  Email: www.education.gov.uk/help/contactus
  Telephone: 0370 000 2288

School postal address	Cantell School, Violet Road, Southampton, Hants, SO16 3GJ
School e-mail address	info@cantell.co.uk
School telephone number	02380 323111

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
- The DPO 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
- 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 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
    - 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 stored on the schools computer system.
- 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 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, 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 of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - 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 stored on the school's computer system. The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, 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.

For example:

Sensitive information being disclosed via email (including safeguarding records)

- 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 as soon as they become aware of the error;
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it;
- In any cases where the recall is unsuccessful, the DPO will 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;
- The DPO will ensure we receive 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.

Other types of breach that you might want to consider could 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.

Summary of Actions to take once an incident has been identified:

	Action	Responsibility	Timelines
1	Report the incident to the Data Protection Officer	Member of staff who was first made aware of the incident	**Immediately after the incident is identified**
2	Investigate and identify the full details of the incident to identify the cause	Data Protection Officer for the school (with the assistance of the colleague who reported the incident)	**As soon as possible following the incident being reported**
3	Identify any remedial action (see section 4, below)	Data Protection Officer for the school	**As soon as possible following the incident being reported**
4	Complete a formal Personal Data Breach Form and return it to the Data Protection Officer	Data Protection Officer for the school	**Within 48 hours of the incident being identified**
5	Review the Personal Data Breach Form and determine whether the incident constitutes a personal data breach or a 'near miss' (i.e. an incident which does not meet the definition of a personal data breach)	Data Protection Officer for the school	**As soon as possible following step 4**
6	If necessary, decide whether to notify (i) the ICO; and/or (ii) individual data subjects, of the personal data breach (see section 5, below)	Data Protection Officer for the school	**As soon as possible following step 4**
7	If necessary, notify the ICO of the personal data breach	Data Protection Officer for the school	**Within 72 hours of the incident being identified**
8	If necessary, notify individual data subjects of the personal data breach	Data Protection Officer for the school	**Without undue delay (in practice this should be done as soon as possible)**

Appendix 4: Personal Data breach reporting form

Part 1: Summary (To be completed by Data protection officer)	
Name and department of person reporting	
Date of completion	
Time and day of incident first identified by staff member	
Time and date of incident occurred (if different)	
Circumstances of the incident (What actually happened)	
Part 2: Details of the personal data incident (To be completed by the Data Protection Officer)	
Nature of incident (e.g. which rules/procedures were breached and how did it happen?)	
Categories of Data subject affected (e.g. Pupils, parents, staff others)	
Approximate number of data subjects affected (if known)	
Possible consequences of the incident for Data subjects	
Part 3: Actions taken in response to the incident (To be completed by the Data Protection	

Officer)	
What mitigating action was taken or will be taken in response to the incident?	
Follow up action to prevent similar incidents	
Part 4: DPO actions	
Does the incident constitute a near miss or a personal data breach?	
If it is a personal data breach, is it notifiable to the ICO?	If Yes – Date notified to ICO If No – Reason for not notifying?
If it is a personal data breach, is it notifiable to the data subjects?	If Yes – Date notified to ICO If No – Reason for not notifying?
Date incident closed	
Signature of DPO	