One Community Trust

DATA PROTECTION POLICY

Author	**Tina Wiegand**
Approved by	**Trustees**
Approval Date	**02/02/2026**
Version Number	**3**
Status	**Approved**
Review Date	**Spring Term 2028**

CHANGE RECORD FORM

Version	Date of change	Date of release	Changed by	Reason for change
1	30/03/2021	30/03/2021		New Policy
2	18/09/2023	16/10/23	AH	Update format and policy review
3	29/01/26	02/02/26	TW	Policy review based on Brown Jacobson Template. Updated to reflect additional primary schools information and added further detailed information as recommended by The Key Policies.

Contents

1 Policy statement

- Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as a Trust/School we will collect, store and **process personal data** about our pupils, **workforce**, parents and others. This makes us a **data controller** in relation to that **personal data**.
- We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.
- The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.
- All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

2 Aims

- Our Trust aims to ensure that all personal data collected about staff, pupils, parents and carers, 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.

3 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 UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

4 About this policy

- The types of personal data that we may be required to handle include information about pupils, parents, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation ('GDPR'), the [Data Protection Act 2018], and other regulations (together '**Data Protection Legislation**').

- This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.
- This policy does not form part of any employee's contract of employment and may be amended at any time.
- This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

5 Definition of data protection terms

- All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in the Annex to this policy.

6 The data controller

- Our Trust processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore is a data controller.
- The Trust has paid its data protection fee to the ICO, as legally required.

7 Roles and responsibilities

- This policy applies to **all staff** employed by One Community Trust (OCT), and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Board of Trustees

It is the responsibility of the OCT Trust Board to:

- Produce, regularly review and monitor the effectiveness of all GDPR policies
- monitor Trust compliance with GDPR legislation

This is achieved by:

- Ensuring sufficient competent persons are in place to advise our schools on GDPR issues.
- Ensuring policies and procedures are provided and implemented in accordance with the requirements of GDPR legislation
- Identifying a lead Trustee for GDPR who will:
    - actively monitor and promote GDPR across the Trust by raising matters with senior leaders or meeting with the DPO and CFO as necessary
    - provide input and comment on Trust GDPR policies and procedures when necessary
    - feedback to Trustees via the Business Risk and Audit Committee
- Providing adequate training and resources to meet the Trust's legal responsibilities as well as compliance with all GDPR policies

Data Protection Officer

- As a Trust we are required to appoint a Data Protection Officer ("DPO"). Our DPO is Tina Wiegand, and she can be contacted by calling Birchwood Community High School on 01925 853500.
- The DPO is responsible for ensuring compliance with the Data Protection Legislation and overseeing the implementation of this policy.
- The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection.
- Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO. Any concerns that the policy has not been followed should be referred, in writing, to the Chair of Trustees. For further guidance, please also refer to our complaints procedure which is available on the Trust website.
- The DPO will provide an annual report of activities directly to the board of trustees via the CFO briefing and, where relevant, report to the board their advice and recommendations on data protection issues.
- The DPO is also the first point of contact for individuals whose data the schools process, and for the ICO.
- Full details of the DPO's responsibilities are set out in their job description.

Headteacher

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

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 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

- The GDPR Lead at each school and their contact details are as follows:

○ Birchwood	Tina Wiegand	01925 853500
○ Croft	Michelle Culliford	01925 764276
○ Gorse Covert	Gillian Poole	01925 825070
○ Oakwood Avenue	Annie O'Brien	01925 635565
○ Woolston	Craig Burgess	01925 837764
○ Locking Stumps	Jane Hill	01925 819076
○ Brook Acre	Jo Holmes	01925 815827
○ Culcheth	Reina Fazackerley	01925 764312

8 Data protection principles

- Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:
    - **Processed** fairly and lawfully and transparently in relation to the **data subject**;
    - **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;
    - Adequate, relevant and not excessive for the purpose;
    - Accurate and, where necessary, kept up to date;
    - Not kept for any longer than is necessary for the purpose; and
    - **Processed** securely using appropriate technical and organisational measures.
- Personal Data must also:
    - be **processed** in line with **data subjects'** rights;
    - not be transferred to people or organisations situated in other countries without adequate protection.
- We will comply with these principles in relation to any **processing** of **personal data** by the Trust/School.

9 Fair and lawful processing

- Data Protection Legislation is not intended to prevent the **processing** of **personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the **data subject**.
- For **personal data** to be **processed** fairly, **data subjects** must be made aware:
    - that the **personal data** is being **processed**;
    - why the **personal data** is being **processed**;
    - what the lawful basis is for that **processing** (see below);

- whether the **personal data** will be shared, and if so with whom;
- the period for which the **personal data** will be held;
- the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and
- the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

- We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any **processing**.
- For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally **process personal data** under the following legal grounds:
  - where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;
  - where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g the Education Act 2011);
  - where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest; and
  - where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data.**
- When **special category personal data** is being processed then an additional legal ground must apply to that processing. We will normally only **process special category personal data** under following legal grounds:
  - where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;
  - where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
  - where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and
  - where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **special category personal data**.
- We will inform data subjects of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.
- If any **data user** is in doubt as to whether they can use any **personal data** for any purpose then they must contact the DPO before doing so.

Vital Interests

- There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not in a position to give consent to the **processing**.

We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

- Where none of the other bases for **processing** set out above apply then the Trust/School must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.
- There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**
- When pupils or our Workforce join the Trust/School a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.
- In relation to all pupils under the age of 12/13 years old we will seek consent from an individual with parental responsibility for that pupil
- If consent is required for any other **processing** of **personal data** of any **data subject** then the form of this consent must:
    - Inform the **data subject** of exactly what we intend to do with their **personal data**;
    - Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and
    - Inform the **data subject** of how they can withdraw their consent.
- Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent.
- The DPO must always be consulted in relation to any consent form before consent is obtained.
- A record must always be kept of any consent, including how it was obtained and when.

10 Processing for limited purposes

- In the course of our activities as a Trust/School, we may collect and **process** the **personal data** set out in our Schedule of Processing Activities. This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our **workforce**).
- We will only **process personal data** for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

11 Notifying data subjects

- If we collect **personal data** directly from **data subjects**, we will inform them about:
    - our identity and contact details as **Data Controller** and those of the DPO;
    - the purpose or purposes and legal basis for which we intend to **process** that **personal data**;

- the types of third parties, if any, with which we will share or to which we will disclose that **personal data**;
- the period for which their **personal data** will be stored, by reference to our Retention and Destruction Policy;
- the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making; and
- the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

- Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter, informing them of where the **personal data** was obtained from.

12 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 who 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.

13 Adequate, relevant and non-excessive processing

- We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

14 Accurate data

- We will ensure that **personal data** we hold is accurate and kept up to date.

- We will take reasonable steps to destroy or amend inaccurate or out-of-date data.
- **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

15 Timely processing

- We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required.

16 Processing in line with data subject's rights

- We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:
    - request access to any **personal data** we hold about them;
    - object to the **processing** of their **personal data**, including the right to object to direct marketing;
    - have inaccurate or incomplete **personal data** about them rectified;
    - restrict **processing** of their **personal data**;
    - have **personal data** we hold about them erased
    - have their **personal data** transferred; and
    - object to the making of decisions about them by automated means.

17 Subject Access Requests and other rights of individuals

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.

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 13 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 our school 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.

Children aged 13 and above are generally 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 our school may not 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.

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 (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 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 or they can seek to enforce their subject access right through the courts.

Parental requests to see the educational record

- Parents, or those with parental responsibility, can request 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.

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, 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 that 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.

The Right to Object

- In certain circumstances **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.
- An objection to **processing** does not have to be complied with where the Trust/School can demonstrate compelling legitimate grounds which override the rights of the **data subject**.
- Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

- In respect of direct marketing any objection to **processing** must be complied with.
- The Trust/School is not however obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

The Right to Rectification

- If a **data subject** informs the Trust/School that **personal data** held about them by the Trust/School is inaccurate or incomplete then we will consider that request and provide a response within one month.
- If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the **data subject** within one month of their request that this is the case.
- We may determine that any changes proposed by the **data subject** should not be made. If this is the case then we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

- **Data subjects** have a right to "block" or suppress the **processing** of **personal data**. This means that the Trust/School can continue to hold the **personal data** but not do anything else with it.
- The Trust/School must restrict the **processing** of **personal data**:
    - Where it is in the process of considering a request for **personal data** to be rectified (see above);
    - Where the Trust/School is in the process of considering an objection to processing by a **data subject**;
    - Where the **processing** is unlawful but the **data subject** has asked the Trust/School not to delete the **personal data**; and
    - Where the Trust/School no longer needs the **personal data** but the **data subject** has asked the Trust/School not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the Trust/School.
- If the Trust/School has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.
- The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

- **Data subjects** have a right to have **personal data** about them held by the Trust/School erased <u>only</u> in the following circumstances:
    - Where the **personal data** is no longer necessary for the purpose for which it was originally collected;
    - When a **data subject** withdraws consent – which will apply only where the Trust/School is relying on the individuals consent to the **processing** in the first place;

- When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object;
- Where the **processing** of the **personal data** is otherwise unlawful;
- When it is necessary to erase the **personal data** to comply with a legal obligation.

- The Trust/School is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:
  - To exercise the right of freedom of expression or information;
  - To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;
  - For public health purposes in the public interest;
  - For archiving purposes in the public interest, research or statistical purposes; or
  - In relation to a legal claim.
- If the Trust/School has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.
- The DPO must be consulted in relation to requests under this right.

Right to Data Portability

- In limited circumstances a **data subject** has a right to receive their **personal data** in a machine readable format, and to have this transferred to other organisation.
- If such a request is made then the DPO must be consulted.

18 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:
  - Papers containing confidential personal data will not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
  - Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices as outlined in our Acceptable Use Policy.
  - Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
  - Staff, pupils or governors should not store personal information on their personal devices.
  - 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

- Specific security procedures include:
    - **Entry controls.** Any stranger seen in entry-controlled areas should be reported to a member of Trust/School staff.
    - **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
    - **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.
    - **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
    - **Medical Plans.** Will be displayed in rooms throughout the school where they are deemed necessary. Care must be taken that the information cannot be seen by passer-by.
    - **Oakwood Avenue Pupil Reports.** Will be stored electronically via the school's secure cloud-based solution.
    - **Working away from the Trust/School premises – paper documents.**
        - **Birchwood Community High School** – Pupil information taken off site for an educational visit is returned to the trip leader who will refile or dispose of accordingly.
        - Paperwork taken offsite by the DSL to attend offsite meetings is held in enclosed files and never left unattended.
        - **Brook Acre Community Primary School**
        - Pupil information taken off site for an educational visit is the responsibility of the trip leader who will store in a closed folder on their person or in a locked room only. All information must then be refiled or securely disposed of on return to school .
        - Paperwork taken offsite by the DSL or safeguarding team member to attend offsite meetings is held in enclosed files and never left unattended.
        - **Croft & Oakwood Avenue** – Documents taken off site containing personal data such as pupil records, assessment data, reports, etc MUST be kept in a closed folder and kept securely.
        - Pupil information taken off site for an educational visit must be returned to the trip leader who will refile or dispose of accordingly.
        - Staff should avoid leaving documents in their cars as this creates a higher risk of them being stolen.
        - When returning documents to school, staff should take them immediately to their original storage place.

- **Culcheth Community Primary School**

- Pupil information taken off site for an educational visit is the responsibility of the trip leader who will store in a closed folder on their person or in a locked room only. All information must then be refiled or securely disposed of on return to school .

- Paperwork taken offsite by the DSL or safeguarding team member to attend offsite meetings is held in enclosed files and never left unattended.

- **Gorse Covert** – Paper copies of personal information must only be removed from site with the permission of the DPO. Where it is necessary to remove paper documents, such as residential trips, there will be one lead person to keep all the personal documentation in a safe place (with a lock if possible).

- **Woolston** – Documents should always be securely stored and in no circumstances should the documents be left in a car or lying around the home. When confidential documents are taken off site they should be signed out on the data protection log (situated in the school office) and signed back in on the same log.

- **Locking Stumps**

- Staff may, where there is a need, take personal data away from the school premises. However these instances are kept to a minimum and when done so, the data user will keep paper documents safe and secure. For trips, one person is responsible for personal documentation in a safe place and then disposed of securely on the return to school.

- Paperwork taken offsite by the DSL or safeguarding team member to attend offsite meetings is held in enclosed files and never left unattended.

- **Working away from the Trust/School premises – electronic working**

  - **Birchwood Community High School** – Electronic documents are stored within Office 365, a secure online platform. These can be accessed across multiple devices but only by using authorised credentials and the user must have the appropriate permissions. Certain users are required to use multi-factor authentication. Users are not to download personal data to unauthorised devices. The use of USB drives is permitted but they must be encrypted.

  - **Croft & Oakwood Avenue** – Electronic documents containing substantial personal data must be stored on an encrypted pen drive or a secure cloud base solution. The use of laptop hard drives to store this type of data is NOT permitted.

  - **Gorse Covert** – Electronic devices must be password protected and kept in a safe place. Only the use of encrypted USBs are authorised.

  - **Woolston** – Staff can access documents via the shared google drive (which has password protected access) but information should not be downloaded onto personal computers/devices under any circumstances. Staff must not disclose their password to anyone.

  - **Brookacre** – Electronic documents are stored within Office 365, a secure online platform. These can be accessed across multiple devices but only by using authorised credentials and the user must have the appropriate permissions. Multifactor

authentication is set up on all users. Information should not be downloaded to personal devices.

- **Locking Stumps** – Electronic documents are stored within Office 365, a secure online platform. Data can be access across multiple platforms using two factor authentication and appropriate permissions. Information should not be downloaded to personal devices.
- **Cu**lcheth - Staff can access documents via the shared google drive (which has password protected access) but information should not be downloaded onto personal computers/devices. They have personal OneDrive through 365 which is a secure online platform.

Document printing. Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

19 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.

20 Data Protection Impact Assessments

- The Trust takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.
- In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.
- The Trust/School will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.
- The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

21 Disclosure and sharing of personal information

- We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, Education and Skills Funding Agency "ESFA", Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

- The Trust/School will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.

- In some circumstances we will not share safeguarding information. Please refer to our Safeguarding Policy.

22 Data Processors

- We contract with various organisations who provide services to the Trust/Schools, including:

- Warrington Borough Council (WBC) Catering, WBC Payroll, Parent Pay, Arbor, DBPrimary, Target Tracker, etc.

  Note: This list is not exhaustive.

- In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

- **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust/School. The Trust/School will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

- Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.

23 Images and Videos

- Parents and others attending Trust/School events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a Trust/School performance involving their child. The Trust/School does not prohibit this as a matter of policy.

- The Trust/School does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust/School to prevent.

- The Trust/School asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

- As a Trust/School we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering Trust/School events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

- Whenever a pupil begins their attendance at the School they (Year 8 onwards), or their parent (nursery to Year 7 inclusive) where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

24 CCTV

- Some of the Schools within the Trust operate CCTV systems. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.
- We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded.
- Please refer to the School's CCTV Policy where applicable. Any enquiries about the CCTV system should be directed to the relevant headteacher.
- Currently this section does not apply all schools within the Trust, but may do so in the future.

25 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
- 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
- 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- 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, 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

26 Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. One Community Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, One Community Trust will treat this as a data breach, and will follow the Trust's data breach procedure.

27 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 our Data Breach Notification Policy.
- When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:
    - A non-anonymised dataset being published on the school website, which shows the exam results of pupils eligible for the pupil premium
    - Safeguarding information being made available to an unauthorised person
    - The theft of a school laptop containing non-encrypted personal data about pupils

28 Training

All staff and governors are provided with data protection training as part of their induction process and will complete an online training course at the beginning of every academic year.

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

29 Changes to this policy

- We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

30 Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Privacy notices
- AI Policy
- Child Protection and Safeguarding Policy

31 ANNEX DEFINITIONS

Term	Definition
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our workforce (including Governers and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Workforce	Includes, any individual employed by Trust such as staff and those who volunteer in any capacity including governors, trustees, members and parent helpers
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.