Data Protection Policy

This Policy is to be used across the trust for all employees	Version	Date
CAMPFIRE EDUCATION TRUST Officer responsible for updating content – DPO	2	May 2020
Data approved by CAMPFIRE EDUCATION TRUST Board		
Effective date as determined by CAMPFIRE EDUCATION TRUST	2	Nov 2019
Statement to be reviewed annually from date last approved by CAMPFIRE EDUCATION TRUST Board	1	Annually

1. **Aims**

   Our trust 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 data protection law including the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 Data Protection Act 2018 (DPA 2018).

   This policy applies to all personal data regardless of whether it is in paper or electronic format and to all staff employed by the trust. It also applies to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

2. **Legislation and guidance**

   This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the information Commissioners office (ICO) on the GDPR.

   It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

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

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 - Health – physical or mental - Sexual 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 trust and its schools processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Trust which includes its' schools is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

5.1 Board of Trustees

The trustees have overall responsibility for ensuring that the Trust and all schools within the trust complies with data protection legislation.

5.2 Data Protection Officer (DPO)

The 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 for the trustees including recommendations where appropriate.

The DPO is also the first point of contact for individuals whose data the school processes and for the IC0.

Our DPO is Tracey Riches and is contactable via dpo@campfiretrust.co.uk.

5.3 Headteacher

The headteacher acts as a 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 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 and vote 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 trust and schools 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 it that ensures it is appropriately secure

This policy sets out how the trust and its schools 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 trust/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 that 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 trust/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. This will be done in accordance with the school's Record Retention Schedule/Records Management Policy

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 (SAR)

Our privacy statements provide an outline of the personal data we hold, why we hold it and who we share it with.

Individuals have a right to make a 'subject access request' to request a copy of the personal information that we hold about them.

To help individuals exercise this right we provide a form on our website. Hard copies of the form can be requested from the school reception. We ask that SARs are made using the form so that we can ensure that we provide the information requested however subject access requests can also be made verbally or by letter or email.

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 any of the trust's schools 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

On receipt of a SAR we may ask for 2 forms of identification, for example a passport and utility bill.

We will also:

- confirm the request in writing and our understanding of the information requested
- respond without delay and within 1 month of receipt. Where a request is complex or numerous we may extend this to 3 months. We will confirm this within 1 month, and explain why the extension is necessary

In certain circumstances we may not disclose information. When we refuse a request, we will explain why, and provide information on how to complain to the Information Commissioners Office.

There is generally no charge for a SAR. However, if the request is considered to be 'manifestly unfounded or excessive' we may charge an administration fee or refuse to provide the information. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

We maintain a register of SAR received to enable us to monitor this.

9.4 Other data protection rights of the individual

Individuals also have the right to:

- Withdraw their consent to processing at any time, where consent is used as the legal basis for processing.
- 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

There is no automatic parental right of access to a pupil's educational record. If a parent wishes to request a copy they should contact the Headteacher of the pupil's school by letter or email in the first instance explaining why the wish to receive it. If

the request is excessive and regular, the school may charge a reasonable fee which takes into account administrative costs.

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

11. CCTV

CCTV cameras are installed at the following sites:

- Bourton Meadow Academy
- Lace Hill Academy
- Moorland Primary School.

We will adhere to the ICO's code of practice for the use of CCTV.
We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DPO.

12. Photographs and videos

As part of the trusts and school activities, we may take photographs and record images of individuals within our trust/schools.

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.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on the trusts or school website or social media pages
- Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.
- When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified unless specific permission is received in writing from parents/carers for each new photograph or video

See our Use of Photos, Videos and Display Boards policy for more information on our use of photographs and videos.

13. 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.

14. 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 sign it in and out from the school via the office, from the trust via the DPO or deputy DPO.
- Passwords that are at least 12 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, tablets/ipads and USB devices. Mobile phones must have a passcode on them.

- Employees, governors, volunteers and visitors must not store personal data information on their personal devices (see our Acceptable Use Policy for Employees, Governors, Volunteers and Visitors)
- 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).

15. Disposal of records

Personal data that is no longer needed will be disposed of securely in line with our document retention schedule. 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.

16. Personal data breaches

The trust and its schools will make all reasonable effort 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 1.

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

- A non-anonymised dataset being published on the trust/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 trust/school portable device ie a laptop or other item containing non-encrypted personal data about pupils/staff or others.

17. Training

All staff and governors/trustees are provided with data protection/GDPR compliance training as part of their induction process followed by refresher training on an annual basis.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and shared with the Board of Trustees and then placed on the Trusts website.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Acceptable use Policy for Employees, Governors, Volunteers and Visitors
- Photos, Videos and Display Boards policy which provides more information on our use of photographs and videos.
- CCTV Use Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.
Each school has a designated Data Protection Lead (DPL) who is the first point of contact in the event of a Data Breach or "near miss". The list of DPLs can be found in Appendix 2.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the school Data Protection Lead (DPL) who will telephone the DPO and log the breach on the trust's secure GDPR portal.

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 DPL will alert the School Improvement Director of the Trust and the headteacher if the breach is within a school.

The DPO will advise on immediate actions to contain and minimise the impact of the breach. (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 to decide whether the breach must be reported to the ICO. This will be judged on a case-by-case basis.

In making the decision 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 trust's secure GDPR portal. Where necessary a paper copy is kept in a locked filing cabinet.

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 trust's secure GDPR portal, and where necessary a paper copy kept in a locked filing cabinet.

The DPO, CFOO and or headteacher will review what happened and how it can be stopped from happening again. This review 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.

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.
- If the sender is unavailable or cannot recall the email for any reason, the DPL will contact the ICT provider and ask that they 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 DPL 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.

Members of staff who receive personal data sent in error must:

- alert the sender and the school DPL as soon as they become aware of the error.
- delete the information immediately and empty their mailbox.

They must not deliberately read the data, share, publish, save or replicate it in any way.

Information being disclosed via social media – website, Facebook, Twitter and other platforms:

Where possible the item should be removed from social media as soon as the trust/school is made aware.

Information being shared that is non-anonymised that contains personal/sensitive data during meetings:

Any documents given out that contain non-anonymised information must be collected back in immediately, if additional copies have been distributed outside of the meeting, all recipients to be contacted and asked to return the paperwork, not to read if not already done so, and must not share the information with anyone else, with a record of who received the document and that all copies were returned and signed to confirm that the information had not been shared via any other means or to anyone else.

Document storage:

All paperwork that contains personal or sensitive information must be locked away at the end of each day.

The list is not exhaustive, but all breaches must be reported to the DPO immediately to ensure compliance of reporting to the ICO within 72 hours, the DPO will carry out the

necessary investigation and reporting as required under the legislation and detailed earlier in this document.

Appendix 2 – Data Protection Leads

The Data Protection Lead (DPL) is the person that staff would initially report a data breach or receipt of a Subject Access Report to in your school.

The DPL is the school's liaison point with the Data Protection Officer (DPO).

The DPO advises the DPL on next steps and prepares draft letters/emails as necessary. The DPO liaises with the Information Commissioners Office on behalf of the school/trust.

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this policy, please contact our data protection officer: Tracey Riches, dpo@campfiretrust.co.uk.