DATA PROTECTION POLICY

September 2025

Policy No: 84
APPROVED BY GOVERNING BODY: 11.9.2025
DATE OF NEXT REVIEW: Autumn 2028
LEAD: Angela Macvie
GOVERNOR RESPONSIBLE: Governing Body

Contents

Data Protection Policy Details

Teacher Responsible: Mrs Angela Macvie

Data Controller: Chadsgrove School (Deb Rattley)

Data Protection Officer: Warwickshire Legal services (SLA in place)

1. Aims

1.1. Chadsgrove School aims to ensure that all personal data collected about staff, pupils, parent carers, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulations (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

1.2. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Purpose

2.1. The purpose of this policy is to explain how Chadsgrove School meets the requirements of the Data Protection Act 2018 with regard to how it collects, stores and processes personal data.

3. Legislation and Guidance

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

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

3.3. In addition, this policy complies with Regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parent carers the right of access to their child's educational record.

4. Definitions

4.1. The definitions used throughout this policy and when dealing with data at Chadsgrove School are as follows:

Personal Data

4.2. 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

4.3. Personal data may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special Categories of Personal Data

4.4. 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), where used for identification purpose
- Physical or mental health
- Sexual orientation.

Processing

4.5. 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

4.6. The identified or identifiable individual whose personal data is held or processed.

Data Controller

4.7. A person or organisation that determines the purposes and the means of processing of personal data.

Data Processor

4.8. 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

4.9. A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

5. The Data Controller

5.1. Chadsgrove School processes personal data relating to parent carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

5.2. The school is registered as a data controller with the ICO and has paid its data protection fee to the ICO, as legally required.

6. Roles and Responsibilities

6.1. This policy applies to all staff employed by Chadsgrove School, and to external organisations or individuals working on the school's behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Body

6.2. The Governing Body has overall responsibility for ensuring that Chadsgrove School complies with all relevant data protection obligations.

Head of School

6.3. The Head of School acts as the representative of the data controller on a day-to-day basis.

Data Protection Officer

6.4. The Data Protection Officer is responsible for overseeing the implementation of this policy, monitoring the school's compliance with data protection law, and developing related policies and guidelines where applicable.

6.5. The Data Protection Officer will provide an annual report of their activities directly to the Governing Body and, where relevant, report to the Governing Body their advice and recommendations on school data protection issues.

6.6. The Data Protection Officer is also the first point of contact for individuals whose data the school processes, and for the ICO.

6.7. Full details of the Data Protection Officers' responsibilities are set out in Appendix C

6.8. The Data Protection Officer can be contacted via 01926 476706 / sophiescullion@warwickshire.gov.uk

All staff

6.9. All school 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 Data Protection Officer 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 internationally
  - 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.

7. Data Protection Principles

7.1. The GDPR is based on data protection principles that Chadsgrove School must comply with.

7.2. 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.

8. Collecting Personal Data

Lawfulness, Fairness and Transparency

8.1. Whenever Chadsgrove School first collects personal data directly from individuals, those individuals will be provided with the relevant information required by data protection law. This information is sent out with the pre-admission forms.

8.2. Chadsgrove School will always consider the fairness of data processing. It will ensure that it does not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways that have unjustified adverse effects on them.

8.3. Chadsgrove School will only process personal data where there is one of six 'lawful bases' (legal reasons) to do so under data protection law. These lawful bases are as follows:

- 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, for example, to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task in the **public interest** or exercise its official authority
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent carer when appropriate in the case of a pupil) has freely given clear **consent.**

8.4. For special categories of personal data, Chadsgrove will also meet one of the special category conditions for processing under data protection law:

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

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

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

Limitation, Minimisation and Accuracy

8.6. Chadsgrove will only collect personal data for specified, explicit and legitimate reasons. These reasons will be explained to the individuals (or their parent carers) when their data is first collected.

8.7. If the school wants to use personal data for reasons other than those given when it was first obtained, the individuals concerned will be informed before the data is used and consent will be sought as necessary.

8.8. Staff will only process personal data where it is necessary in order to do their jobs.

8.9. When staff no longer need the personal data they hold, they will ensure that it is deleted, stored securely for the appropriate period of time, or anonymised. This will be done in accordance with the school's record retention schedule, a copy of which can be obtained from the school office.

9. Sharing Personal Data

9.1. Chadsgrove 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 school staff at risk
- It is necessary to liaise with other agencies – consent will be sought, as necessary, before doing this
- Suppliers or contractors need data to enable services to be provided to staff and pupils. When doing this, the school will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
  - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any data that is shared
  - Only share data that the supplier or contractor needs to carry out their service.

9.2. Chadsgrove will share personal data with law enforcement and government bodies where there is a legal requirement to do so.

9.3. Chadsgrove may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of its' pupils or staff.

9.4. If Chadsgrove transfers personal data internationally, this will be done in accordance with data protection law. However, the school does not currently do this.

10. Subject Access Requests and Other Rights of Individuals

10.1. 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.

10.2. 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:

- The name of the individual
- A correspondence address
- A contact number and email address
- Details of the information requested.

10.3. If staff receive a Subject Access Request they must immediately forward it to the Data Protection Officer.

11. Children and Subject Access Requests

11.1. Personal data about a child belongs to that child and not the child's parent carer. For a parent 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.

11.2. Children below the age of 12 and some (but not all) older pupils with learning difficulties 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 parent carers of pupils at Chadsgrove may be granted without the express permission of the pupil. However, this is not a rule and a pupil's ability to understand their rights, regardless of their age, will always be judged on a case-by-case basis.

12. Responding to Subject Access Requests

12.1. When responding to Subject Access Requests, the Data Protection Officer:

- May ask the individual to provide two 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 that the school will comply within three months of receipt of the request, where the request is complex or numerous. The school will inform the individual of this within one month, and explain why the extension is necessary.

12.2. Chadsgrove 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 a 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 the school couldn't reasonably anonymise, and the school doesn'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.

12.3. If a Subject Access Request is unfounded or excessive, the school may refuse to act on it, or charge a reasonable fee to cover administrative costs. The school will take into account whether the request is repetitive in nature when making the decision.

12.4. If a request is refused, the school 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.

13. Other Data Protection Rights of the Individual

13.1. In addition to the right to make a Subject Access Request (see above) and to receive information about how Chadsgrove collects, uses and processes data, individuals also have the right to:
- Withdraw their consent to processing at any time
- Ask the school to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)
- Ask for their personal data to be transferred to a third party in a structured, commonly

13.2. Individuals should submit any request to exercise these rights to the Data Protection Officers. If school staff receive such a request, they must immediately forward it to the Data Protection Officers.

14. Parent Carer Requests to See the Educational Record

14.1. Parent carers, 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.

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

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

14.4. 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

15. Biometric Recognition Systems

15.1. Chadsgrove School does not currently use biometric data.

15.2. If the school does begin to use biometric data, as part of an automated biometric recognition system, then:

- It will comply with the requirements of the Protection of Freedoms Act 2012
- Parent carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before any biometric data is taken from their child and first processed
- Parent carers and pupils have the right to choose not to use biometric systems should these been put into place at Chadsgrove. In such cases, the school will provide alternative means of accessing the relevant services for those pupils
- Parent carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and the school will make sure that any relevant data already captured is deleted
- As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, the school will not process that data irrespective of any consent given by the pupil's parent carer
- Where staff members or other adults use the school's biometric system(s), Chadsgrove will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

16. CCTV

16.1. Chadsgrove may use CCTV in various locations around the school site in order to ensure that it remains safe.

16.2. Should CCTV be used, the school will adhere to the ICO's Code of Practice for the use of CCTV.

16.3. Chadsgrove does not need to ask individuals' permission to use CCTV, but it will be made clear where/when individuals are being recorded. Any security cameras will be clearly visible and accompanied by prominent signs explaining that CCTV is in use.

16.4. Any enquiries about CCTV systems should be directed to Laura Slater, Office Manager, via the school office (01527 871511).

17. Photographs and Videos

17.1. As part of school activities, staff may take photographs and record images of individuals within the school.

17.2. The school will obtain written consent from parent carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. How the photographs and/or videos will be used will be clearly explained to both the parent carer and, where appropriate, the pupil.

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

17.4. Uses of photographs and videos may include:

- Within school on notice boards and in school magazines, brochures, newsletters, communication aids etc.
- Within school for assessment purposes
- Outside of school by external agencies such as the school photographer, or newspapers
- Online on the school website, social media pages or Class Dojo.

17.5. Consent can be refused or withdrawn at any time. If consent is withdrawn, the school will delete any photographs and videos and not distribute them further.

17.6. When using photographs and videos, outside of classroom areas, the school will not accompany them with any other personal information about the child, in order to ensure they cannot be identified.

17.7. Occasionally, school staff may use images/videos as part of training materials delivered to outside agencies. Consent, from parent carers, will always be sought before such materials are used.

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

18. Data Protection by Design and Default

18.1. Chadsgrove will put measures in place to show that it has integrated data protection into all of its' data processing activities, including:

- Appointing a suitably qualified Data Protection Officer via an SLA with Warwickshire Legal Services
- 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 Data Protection Officer 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 privacy measures and ensure compliance;
- Maintaining records of processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the Data Protection Officer and all of information the school is required to share about how it uses and processes personal data (via our privacy notices, which can be seen in Appendix 2)
    - 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 international transfers and the safeguards for those, retention periods and how we are keeping the data secure. At Chadsgrove, the document used for this purpose is called the GDPR spreadsheet.

19. Data Security and Storage of Records

19.1. Chadsgrove 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.

19.2. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept secure when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, 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 office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices
- Staff and pupils are reminded that they should not reuse passwords from other sites and should 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 the ICT policy)
- Where the school needs to share personal data with a third party, it carries out due diligence and takes reasonable steps to ensure that it is stored securely and adequately protected.

20. Disposal of Records

20.1. 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 it is not possible or there is no need to rectify or update it.

20.2. Chadsgrove will shred paper-based records and delete electronic files. The school may also use a third party (currently Shred-it) to safely dispose of records on the school's behalf. If this occurs, the school will require the third party to provide sufficient guarantees that it complies with data protection law. Shred-it destroys material on site under the supervision of a member of school staff.

20.3. Secure storage bins are available for documents waiting to be shredded. Should these become full, excess materials are stored in the locked archive store.

21. Personal Data Breaches

21.1. Chadsgrove will make all reasonable endeavours to ensure that there are no personal data breaches.

21.2. In the unlikely event of a suspected data breach, the school will follow the procedure set out in Appendix 1.

21.3. When appropriate, the school/DPO 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
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils.

22. Training

22.1. All staff will be provided with data protection and cyber security training as part of their induction process.

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

23. School Support Services and PD Outreach Provision

23.1. The School Support Service and PD Outreach provision (collectively known as 'Support Services for Your School' will comply with Chadsgrove policy regarding GDPR regulations.

23.2. All data held by the SST will be stored securely in the following manner:

- Paper – locked filing cabinets
- Electronic – secure password protected dedicated server and/or secure encrypted external drives

23.3. Data will be held and shared in accordance with GDPR regulations as detailed in the Data Privacy Statement. Data expiration dates will be logged and, when reaching this point, will be destroyed securely in line with GDPR guidelines.

23.4. Data will only be shared with persons and organisations detailed within the privacy notice. Data privacy notices are requested, and held on file, from any third party organisation with whom data is shared.

23.5. Staff (including associate staff, supply staff and employed staff) will ensure that data is handled in a secure manner in line with Chadsgrove policy. Where data is required to be used away from Chadsgrove, it will need to be held on a secure device (with adequate encryption – in line with Chadsgrove policy).

23.6. Data (e.g. reports) may only be shared via the Worcestershire Children's Services Portal, Egress or via secure remote server access. Where paperwork requires a physical signature rather than an electronic one (e.g. JCQ Form 8) staff are required to ensure that this is only completed onsite at Chadsgrove.

23.7. All recruitment and employment paperwork for staff will be held in line with the main Chadsgrove School staffing and recruitment policy. Staff will be expected to adhere to Chadsgrove policies whilst undertaking any work on behalf of the SST.

23.8. Staff are expected to hold a form of photographic ID whilst undertaking work for the SST. Chadsgrove Teaching School and/or Worcestershire County Council ID badges will be provided, however should staff not wish for their data to be held for this purpose, they will be responsible for seeking a suitable alternative form of photographic ID in line with Chadsgrove policy.

24. Monitoring Arrangements

24.1. The Data Protection Officer is responsible for monitoring and reviewing this policy.

24.2. This policy will be reviewed every two years.

25. Links with Other Policies

25.1. This data protection policy is linked to the following:

- Freedom of information (Policy Number 86)
- Online Safety and Acceptable Use (Policy Number 87)
- School Systems and Data Security (Policy Number 85)
- GDPR Information Spreadsheet
- Records Retention Schedule
- School Safeguarding and Child Protection (Policy Number 73)
- Safer Recruitment (Policy Number 101)

Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioners Office.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer.

- The Data Protection Officer will investigate the report, and determine whether a breach has occurred. In order to make this decision, the Data Protection Officer 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 Data Protection Officer will alert the Head of School and the Chair of Governors.

- The Data Protection Officer 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 Data Protection Officer will assess the potential consequences, based on how serious they are, and how likely they are to happen.

- The Data Protection Officer 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 Data Protection Officer 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 is likely that there will be a risk to people's rights and freedoms, the Data Protection Officer must notify the ICO.

- The Data Protection Officer 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 will be stored in the school office.

- Where the ICO must be notified, the Data Protection Officer will do this via the 'report a breach' page of the ICO website or through their breach report line (0303 123 1113) within 72 hours. As required, the Data Protection Officer will set out:

- A description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned
- The name and contact details of the Data Protection Officer
- 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 Data Protection Officer 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 Data Protection Officer expects to have further information. The Data Protection Officer will submit the remaining information as soon as possible.

- The Data Protection Officer 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 Data Protection Officer will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - A description, in clear and plain language the nature of the personal data breach
  - The name and contact details of the Data Protection Officer
  - 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 Data Protection Officer 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 Data Protection Officer 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 in the school office.

- The Data Protection Officer and Head of School will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

<u>Actions to Minimise the Impact of Data Breaches</u>

Chadsgrove 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.

Special category data being disclosed via email (including safeguarding records)

- If special category data 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

Non-anonymised data being published electronically

- Remove/take down the document immediately
- Alert the DPO
- Carry out on internet search to check if the information has been posted elsewhere and request removal from the publisher if this is the case

A school laptop containing non-encrypted sensitive personal data being stolen or hacked

- Report the theft to the police
- Alert the DPO
- Alert the Senior IT Manager in school to advise re remotely wiping the laptop
- Change all passwords

Appendix 2: Privacy Statements

Privacy Notice for Parent Carers – Pupil Information

Under data protection law, individuals have a right to be informed about how Chadsgrove School uses any personal data that is held about them. We comply with this right by providing 'Privacy Notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

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

This privacy notice applies whilst we believe your child is not capable of understanding and exercising their own data protection rights. Once your child is able to understand their rights over their own data (generally considered to be age 12, but this has to be considered on a case-by-case basis, particularly for children with learning difficulties), you should instead refer to our privacy notice for pupils to see what rights they have over their own personal data. This can be found on the school website.

We, Chadsgrove School, Meadow Road, Catshill, Bromsgrove, are the 'data controller' for the purposes of data protection law.

Our Data Protection Officer is Warwickshire Legal Services (01926 476706)

The Personal Data we Hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

a) Contact details, contact preferences, date of birth, identification documents
b) Results of internal assessments and externally set tests
c) Pupil and curricular records
d) Exclusion information
e) Attendance information
f) Safeguarding information
g) Details of any support received, including care packages, plans and support providers

We may also collect, use, store and share (when appropriate) information about your child that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to, information about:

h) Any medical conditions we need to be aware of, including physical and mental health
i) Photographs and CCTV images captured in school
j) Characteristics, such as ethnic background or special educational needs

We may also hold data about your child that we have received from other organisations, including other schools and social care services.

Why we use this data

We use the data listed above to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Ensure the continuity of the services that we offer to support pupils
- Communicate with parent carers and other organisations such as health and social care

- Carry out research – specific consent would be gained if data was to be used in this way
- Comply with the law regarding data sharing

Where you have given us consent to do so, we may send your child marketing information by email or text promoting school events, campaigns, charitable causes or services that may be of interest to them. You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by clicking on the 'Unsubscribe' link at the bottom of any such communication, or by contacting us (see 'Contact us' below).

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Our Legal Basis for Using this Data

Our lawful bases for processing your child's personal data for the purposes listed in section 3 above are as follows:

- For the purposes of (a, b, c, d, e, f, h) above, in accordance with the 'public task' basis – we need to process data to fulfil our statutory function as a school as set out here:
    - Safeguarding and Welfare of pupils
    - Facilitating educational visits
    - Teaching, supporting and learning
    - Reporting to the Governing body

- For the purposes of (a, b, c, d, e,) above, in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law as set out here:
    - Maintaining admission and attendance records
    - Free school meal information
    - Pupil premium information
    - Pupil behaviour and exclusion information

- For the purposes of (g, i) above, in accordance with the 'consent' basis – we will obtain consent from you to use your child's personal data

- For the purposes of (d, f,) above, in accordance with the 'vital interests' basis – we will use this personal data in a life-or-death situation

- For the purposes of(a, b)above, in accordance with the 'contract' basis – we need to process personal data to fulfil a contract with your child or to help them enter into a contract with us

- For the purposes of (a,) above, in accordance with the 'legitimate interests' basis – where there's a minimal privacy impact and we have a compelling reason, including:
    - Communicating with parent carers

Where you have provided us with consent to use your child's data, you may withdraw this consent at any time. We will make this clear when requesting.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

Most of the data we hold about your child will come from you, but we may also hold data about your child from:

- Local authorities
- Government departments or agencies
- Police forces, courts, tribunals

How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. Our record retention schedule sets out how long we keep information about pupils.

You may request a copy of our Record Retention Schedule by contacting the school office (office@chadsgrove.worcs.sch.uk), telephoning school (01527 871511) or calling in to the school office.

We have put in place appropriate security measures to prevent your child's personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your child's personal data securely when we no longer need it.

Who we Share Data With

We do not share information about pupils with any third party without consent unless the law 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 personal information about pupils with:

- The relevant Local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- Your Own Local Authority (e.g. Dudley, Solihull), as above, if your child is educated out of authority
- Government Departments or agencies
- Our youth support services provider
- Our regulator, Ofsted
- Financial organisations
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.
The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with third party organisations, which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data.
You can also contact the Department for Education with any further questions about the NPD.

Transferring Data internationally
We do not currently transfer personal data to a country or territory outside the European Economic Area. If we needed to do so, we will do this in accordance with data protection law.

Your Rights
You have a right to make a 'subject access request' to gain access to personal information that we hold about your child.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact our data protection officer. If you would like to make a request, please contact us (see 'Contact us' below).
Once your child is able to understand their rights over their own data (generally considered to be age 12, but this has to be considered on a case-by-case basis, particularly if an individual has learning difficulties), we will need to obtain consent from your child for you to make a subject access request on their behalf.

Your Right to Access your Child's Educational Record
Parent carers, or those with parental responsibility, also have the right to access their child's educational record (which includes most information about a pupil). This right applies as long as the pupil 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.

To make a request, please contact us (see 'Contact us' below).

Your Other Rights Regarding your Child's Data

Additionally, you have the right to:

- Object to our use of your child's personal data
- Prevent your child's data being used to send direct marketing
- Object to and challenge the use of your child's personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected
- In certain circumstances, have the personal data we hold about your child deleted or destroyed, or restrict its processing
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact us (see 'Contact us' below).

Once your child is able to understand their rights over their own data (generally considered to be age 12, but this has to be considered on a case-by-case basis, particularly if an individual has learning difficulties), we will need to obtain consent from your child for you to make these requests on their behalf.

Complaints

We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **Data Protection Officer**:
Warwickshire Legal Services
01926 476706

Privacy Notice for Parent Carers

Introduction

Under data protection law, individuals have a right to be informed about how Chadsgrove School uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **parent carers of pupils at our school**.

We, Chadsgrove School, Meadow Road, Catshill, Bromsgrove, are the 'data controller' for the purposes of data protection law.

Our Data Protection Officer is Warwickshire Legal Services (01926 476706)

The Personal Data we Hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

a) Contact details and contact preferences (such as your name, address, email address and telephone numbers)
b) Bank details
c) Details of your family circumstances
d) Details of any safeguarding information including court orders or professional involvement
e) Records of your correspondence and contact with us
f) Details of any complaints you have made

We may also collect, use, store and share (when appropriate) information about you that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to, information about:

g) Any health conditions you have that we need to be aware of
h) Photographs and CCTV images captured in school

We may also hold data about you that we have received from other organisations, including other schools and social care services.

Why We Use this Data

We use the data listed above to:

- Report to you on your child's attainment and progress
- Keep you informed about the running of the school (such as emergency closures) and events
- Process payments for school services and clubs
- Provide appropriate pastoral care
- Protect pupil welfare
- Administer admissions waiting lists
- Assess the quality of our services
- Carry out research
- Comply with our legal and statutory obligations

Use of your Personal Data for Marketing Purposes

Where you have given us consent to do so, we may send you marketing information by email or text promoting school events, campaigns, charitable causes or services that may be of interest to you.

You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by clicking on the 'Unsubscribe' link at the bottom of any such communication, or by contacting us (see 'Contact us' below).

Use of your Personal Data in Automated Decision Making and Profiling

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Our Lawful Basis for Using this Data

- For the purposes of (a, b, c, d, e, f, h) above, in accordance with the 'public task' basis – we need to process data to fulfil our statutory function as a school as set out here:
    - Safeguarding and Welfare of pupils
    - Facilitating educational visits
    - Teaching, supporting and learning
    - Reporting to the Governing body

- For the purposes of (a, b, c, e, f) above, in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law as set out here:
    - Maintaining admission and attendance records
    - Free school meal information
    - Pupil premium information
    - Pupil behaviour and exclusion information

- For the purposes of (a, g) above, in accordance with the 'vital interests' basis – we will use this personal data in a life-or-death situation

- For the purposes of (a, b, e)above, in accordance with the 'contract' basis – we need to process personal data to fulfil a contract with you

- For the purposes of (a) above, in accordance with the 'legitimate interests' basis – where there's a minimal privacy impact and we have a compelling reason, including:
    - Communicating with you

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our Basis for Using Special Category Data

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in data protection law:

- We have obtained your explicit consent to use your personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation

- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation

Collecting this Data

While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily. Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Government departments or agencies
- Your children
- Police forces, courts, tribunals

How we Store this Data

We keep personal information about you while your child is attending our school. We may also keep it beyond their attendance at our school if this is necessary. Our Record Retention Schedule sets out how long we keep information about parent carers. A copy of this can be obtained from the school office.

We have put in place appropriate security measures to prevent your personal information being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

Who We Share Data With

We do not share information about you with any third party without consent unless the law 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 personal information about you with:

- The relevant Local authority– to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about exclusions
- Government departments or agencies
- Our regulator, [specify as appropriate, e.g. Ofsted, Independent Schools Inspectorate]

- Suppliers and service providers:
- List the specific types of providers (e.g. catering, HR)
- Financial organisations
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals

Transferring Data Internationally

We do not currently transfer personal data internationally. If we needed to do so, we will do this in accordance with data protection law.

Your Rights

You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that may apply):

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

Your Other Rights Regarding your Data

Under data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- Object to our use of your personal data
- Prevent your data being used to send direct marketing
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected
- In certain circumstances, have the personal data we hold about you deleted or destroyed, or restrict its processing
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact us (see 'Contact us' below).

Complaints

We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:
Warwickshire Legal Services
01926 476706

Privacy Notice for Pupils

Introduction

You have a legal right to be informed about how Chadsgrove School uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This notice explains how we collect, store and use personal data about **pupils at our scho**ol, like you.

We, Chadsgrove School, Meadow Road, Catshill, Bromsgrove, are the 'data controller' for the purposes of data protection law.

Our Data Protection Officer is Warwickshire Legal Services (01926 476706).

The Personal Data we Hold

We hold some personal information about you to make sure we can help you learn and look after you at school.

For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.
Personal information that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

a) Your contact details
b) Your test results
c) Your attendance records
d) Details of any behaviour issues or exclusions

We may also collect, use, store and share (when appropriate) information about you that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to:

e) Information about your characteristics, like your ethnic background or any special educational needs
f) Information about any medical conditions you have
g) Photographs and CCTV images

Why we Use this Data

We use the data listed above to:

- Get in touch with you and your parent carers when we need to
- Check how you're doing in exams and work out whether you or your teachers need any extra help
- Track how well the school as a whole is performing
- Look after your wellbeing

Use of your Personal Data for Marketing Purposes

Where you have given us consent to do so, we may send you messages by email or text promoting school events, campaigns, charitable causes or services that you might be interested in.

You can take back this consent or 'opt out' of receiving these emails and/or texts at any time by clicking on the 'Unsubscribe' link at the bottom of any such communication, or by contacting us (see 'Contact us' below).

Use of your Personal Data in Automated Decision Making and Profiling

We do not currently put your personal information through any automated decision-making or profiling process. This means we do not make decisions about you using only computers without any human involvement.

If this changes in the future, we will update this notice in order to explain the processing to you, including your right to object to it.

Our Lawful Basis for Using this Data

Our lawful bases for processing your child's personal data for the purposes listed in section 3 above are as follows:

- For the purposes of (a, b, d, e, f) above, in accordance with the 'public task' basis – we need to process data to fulfil our statutory function as a school as set out here:
    - To protect your safety and Welfare
    - To enable you to go out on visits and take part in other educational activities
    - To teach, support you and help you to learn
    - To report to other agencies such as the governors

- For the purposes of (b, d, e,) above, in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law as set out here:
    - Maintaining admission and attendance records
    - Free school meal information
    - Pupil premium information
    - Pupil behaviour and exclusion information

- For the purposes of (g,) above, in accordance with the 'consent' basis – we will obtain consent from you to use your personal data

- For the purposes of (a, f,) above, in accordance with the 'vital interests' basis – we will use this personal data in a life-or-death situation

- For the purposes of(a, b)above, in accordance with the 'contract' basis – we need to process personal data to fulfil a contract with you

- For the purposes of (a,) above, in accordance with the 'legitimate interests' basis – where there's a minimal privacy impact and we have a compelling reason, including:
  Communicating with you

Where you have provided us with consent to use your child's data, you may withdraw this consent at any time. We will make this clear when requesting.

Our Basis for Using Special Category Data

For 'special category' data (more sensitive personal information), we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in data protection law:

- We have obtained your explicit consent to use your information in a certain way
- We need to use your information under employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The information has already been made obviously public by you
- We need to use it to make or defend against legal claims

- We need to use it for reasons of substantial public interest as defined in legislation
- We need to use it for health or social care purposes, and it's used by, or under the direction of, a professional obliged to confidentiality under law
- We need to use it for public health reasons, and it's used by, or under the direction of, a professional obliged to confidentiality under law
- We need to use it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the use is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made obviously public by you
- We need to use it as part of legal proceedings, to obtain legal advice, or to make or defend against legal claims
- We need to use it for reasons of substantial public interest as defined in legislation

Collecting this Data

While most of the information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we want to collect information from you, we make it clear if you have to give us this information (and if so, what the possible consequences are of not doing that), or if you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local councils
- Government departments or agencies
- Police forces, courts, tribunals

How we Store this Data

We keep personal information about you while you are attending our school. We may also keep it beyond your attendance at our school if this is necessary. Our Record Retention Schedule sets out how long we keep information about pupils. A copy of this can be requested from the school office.

We have security measures in place to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

Who we Share Data With

We do not share information about you with any third party without your consent unless the law 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 personal information about you with:

- The relevant Local authority– to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about exclusions
- Government departments or agencies
- Our youth support services provider

- Our regulator, Ofsted
- Financial organisations
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals

National Pupil Database

We have to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.

Some of this information is then stored in the National Pupil Database, which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research.

The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations, such as organisations that promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

You can find more information about this on the Department for Education's webpage on how it collects and shares research data.

You can also contact the Department for Education if you have any questions about the database.

Transferring Data Internationally

We do not currently transfer personal data internationally. If we needed to do so, we will do this in accordance with data protection law.

Where we transfer your personal data to a country or territory outside the European Economic Area, we will follow data protection law.

In cases where we have safeguarding arrangements in place, you can get a copy of these arrangements by contacting us.

Your Rights

You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (unless there is a really good reason why we should not):

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data (decisions made by a computer or machine, rather than by a person), and any consequences of this
- Give you a copy of the information in an understandable form

You may also have the right for your personal information to be shared with another organisation in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

Your Other Rights Regarding your Data

Under data protection law, you have certain rights regarding how your personal information is used and kept safe. For example, you have the right to:

- Say that you don't want your personal information to be used
- Stop it being used to send you marketing materials
- Say that you don't want it to be used for automated decisions (decisions made by a computer or machine, rather than by a person)
- In some cases, have it corrected if it's inaccurate
- In some cases, have it deleted or destroyed, or restrict its use
- In some cases, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation if the data protection rules are broken and this harms you in some way

To exercise any of these rights, please contact us (see 'Contact us' below).

Complaints

We take any complaints about our collection and use of personal information very seriously.
If you think that, our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:
Warwickshire Legal Services
01926 476706

Privacy Notice for School Workforce

Introduction

Under data protection law, individuals have a right to be informed about how Chadsgrove School uses any personal data that we hold about them. We comply with this right by providing 'Privacy Notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use your personal data .about individuals we employ or otherwise engage to work at our school

We, Chadsgrove School, Meadow Road, Catshill, Bromsgrove, are the 'data controller' for the purposes of data protection law.

Our data protection officer is Warwickshire Legal Services (01926 476706)

The Personal Data we Hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

a) Contact details
b) Date of birth, marital status and gender
c) Next of kin and emergency contact numbers
d) Salary, annual leave, pension and benefits information
e) Bank account details, payroll records, National Insurance number and tax status information
f) Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
g) Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
h) Performance information
i) Outcomes of any disciplinary and/or grievance procedures
j) Absence data
k) Copy of driving licence
l) Photographs and video recordings
m) Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Any health conditions you have that we need to be aware of
    n) Sickness records
    o) Photographs and CCTV images captured in school
    p) Trade union membership

We may also collect, use, store and share (when appropriate) information about criminal convictions and offences.

We may also hold data about you that we have received from other organisations, including other schools and social services, and the Disclosure and Barring Service in respect of criminal offence data.

Why We Use this Data

We use the data listed above to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable equalities monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

Use of your Personal Data in Automated Decision Making and Profiling

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Our Lawful Basis for Using this Data

Our lawful bases for processing your personal data for the purposes listed above are as follows:

- For the purposes of (a,b,d,e,j,m,n) above, in accordance with the 'public task' basis – we need to process data to fulfil our statutory function as a school as set out here:
    - To protect your health, safety and welfare
    - To facilitate the reporting of the functions of the school
    - To support teaching and learning
    - To report to other agencies such as the governors
    - To enable you to be paid

- For the purposes of (a,b,d,f,g,h,I,j,m,n) above, in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law as set out here:
    - Maintaining employment records
    - Maintaining accident records
    - Performance management obligations
    - Disciplinary procedures

- For the purposes of (o, p) above, in accordance with the 'consent' basis – we will obtain consent from you to use your personal data

- For the purposes of (b, c) above, in accordance with the 'vital interests' basis – we will use this personal data in a life-or-death situation

- For the purposes of(a,b,)above, in accordance with the 'contract' basis – we need to process personal data to fulfil a contract with you

- For the purposes of (a,b) above, in accordance with the 'legitimate interests' basis – where there's a minimal privacy impact and we have a compelling reason, including:
  Communicating with you

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our Basis for Using Special Category Data

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in data protection law:

- We have obtained your explicit consent to use your personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation

Collecting this Information

While the majority of information we collect from you is mandatory, there is some information that can be provided voluntarily

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Government departments or agencies
- Police forces, courts, tribunals

How we Store this Data

We keep personal information about you while you work at our school. We may also keep it beyond your employment at our school if this is necessary. Our Record Retention Schedule sets out how long we keep information about staff.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

You may request a copy of our Record Retention Schedule by contacting the school office (office@chadsgrove.worcs.sch.uk), telephoning school (01527 871511) or calling in to the school office.

Who we Share Data With

We do not share information about you with any third party without your consent unless the law 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 personal information about you with:

- The relevant Local authority– – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- Government department and agencies
- Our regulator, Ofsted
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll
- Financial organisations
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals

Transferring Data Internationally

Should we transfer personal data internationally, we will do so in accordance with data protection law. However, we do not current do this. In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Your Rights

How to access personal information we hold about you

You have a right to make a **'Subject Access Request'** to gain access to personal information that we hold about you

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact the relevant data protection officer.

Your Other Rights Regarding your Data

Under data protection law, you have certain rights regarding how your personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress

- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected
- In certain circumstances, have the personal data we hold about you deleted or destroyed, or restrict its processing
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:
Warwickshire Legal Services
01926 476706

Appendix 3 – Warwicksire Legal Sevices DPO Role

UKGDPR for Schools & Academies

All organisations need to comply with the UK General Data Protection Regulation (UKGDPR). The ICO has issued guidance on how you can demonstrate compliance, including that you must :

- implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training;
- internal audits of processing activities, and reviews of internal HR policies;
- maintain relevant documentation on processing activities; ● where appropriate, appoint a data protection officer.

What do you need to do?

Maintained Schools and Academies are required to designate a Data Protection Officer (DPO) to take responsibility for monitoring and advising on data protection compliance. An important part of the DPO's role will be to shape the "data culture" of the organisation, ensuring that all staff have access to appropriate levels of training and support on matters of data protection and leading on embedding this practice within the organisation.

The DPO is required to report directly to the most senior level of management in the organisation (Headteachers / Governors / Directors) and cannot be dismissed for undertaking duties in relation to their job. In doing so, they will also be expected to monitor compliance, offer independent scrutiny and advice on decision making.

Our Data Protection Officer Service

We will provide a comprehensive service, provided by trained and knowledgeable staff, to meet the requirements of GDPR. Working in partnership with your senior leadership team and all staff who manage your data, our service will deliver all the tasks of the Data Protection Officer, fully covering what WLS considers the core service:

- Audits and compliance checks
- Data breach advice
- ICO complaint handling
- Data subjects' complaints (stage before ICO involvement)
- Template policies and procedures
- Bulletins (including advice notes)
- Access to our School DPO Handbook
- Training – live events, on demand, and access to eLearning

The service also provides subscribers with 4 hours of pre-paid time per term for support on areas supplementary to the core service:

- Data rights requests, including subject access requests and advice on exemptions.
- Advice on information sharing:

- Processors/software providers o Local authority/DfE o Law enforcement
- Insurers o External agents (e.g., NHS)

- Reviewing schools' policies and procedures – e.g., updated privacy notices, data mapping tool, DP policy/info security policy etc.
- Reviewing agreements and contracts for data protection compliance (requirement under Article 28 of UKGDPR)
- Support with screening for and conducting DPIAS
- Reviewing and signing off DPIAs
- Retention queries (e.g., how long should we keep x file)
- General enquiries – e.g., consent for photos, can we ask for X and share Y etc. CCTV (installation, storage, retention, policies), data collection/checking and best practice guides.

Should subscribers exceed their pre-paid time in any one term, they can continue to buy more and will be charged at our very competitive, subscriber hourly rates. Any buy-as-you-go charges will be charged termly in arrears. For all work over pre-paid time we will give provide a quote.

What's included? – Service Deliverables

We will provide:

- Regulatory advice from our team of data protection specialists, via the dedicated DPO hotline and mailbox.
- Three bulletins per year, which will aim to provide help and support with your Data Protection compliance.
- Advise on sharing personal data lawfully. We will also provide you with draft template agreements where appropriate.
- Supply you with exemplar policies required to ensure Data protection compliance.
- Monitor your compliance with the UK GDPR and other data protection law, including support for managing internal data protection activities, advising on data protection impact assessments, training staff.
- Act as the first point of contact for supervisory authorities and for individuals whose data is processed
- Access to eLearning for your staff. In addition, we will provide resources to enable you to deliver refresher training in your school or trust.
- Annual refresher training events for your school's Data Protection Lead/named contact for data protection matters.
- Annual compliance check, which will result in recommendations and overall feedback on your school or trust's data protection compliance.
- Unlimited support on the core service DPO work and termly pre-paid support time for areas extra to the core service
- Send you termly updates on your use of our services

Client Responsibilities

The appointment of an external DPO does not change your responsibilities relating to the management of data within your school or academy. You will still be required:

- to own and process data according to your own policies & procedures.
- to act as the Data Controller, and data protection compliance remains the responsibility of the Controller.
- to provide a nominated point of contact for the school / federation / MAT.
- to disseminate guidance and advice to school / federation / MAT staff.
- to process subject access requests.
- to undertake data audits.
- to report data breaches to the Information Commissioner's Office.
- to implement action plans and steps identified by data protection officer in compliance checks and reviews.

How to buy more

Additional Hours

If your requirement for extra support outside of the core service exceeds your pre-paid time within a term, or at any time you require additional support outside the scope of our service (ie legal representation), you can continue to buy more and will be charged at our very competitive, subscriber hourly rates. For all matters over your subscription hours we will give you a quote. Our hourly rates are available on the WES website at www.warwickshire.gov.uk/wes

If you want to discuss buying additional DPO or legal services or you want to talk to someone about your DPO or other legal requirements either telephone us on 01926 412859 or email us at schooldpo@warwickshire.gov.uk .

Service Managers

The following manager leads the business arrangements should you have any comments or wish to discuss your service requirements in more detail.

Contact	**Telephone / Email**
Tim Seedhouse Business Manager – Legal Services	01926 412762 timseedhouse@warwickshire.gov.uk
Sophie Scullion Team Leader – School DPO	01926 476706 sophiescullion@warwickshire.gov.uk

If something goes wrong

For any queries about service delivery please contact our Schools Hotline on 01926 412361 between 8.30am to 4.30pm Monday to Friday. We aim to respond to 95% of problems raised within 5 working days.

We look to resolve service issues within a 90 day period and in most instances expect to resolve issues much quicker than this. If however, we miss the 90 day deadline, we will escalate the issue to WES Customer Care.