Castle Phoenix Trust

Data Protection Policy

Trust Level Policy

Date effective	01 September 2025
Review Cycle	Annually
Review Date	01 September 2026
Date of Approval by Trust Board	12 November 2025
Committee approved by	Trust Board
Author	Emma Phillips – Trust Data Protection Lead

Contents

1. Aims 3
2. Legislation and guidance 3
3. Definitions 3
4. The data controller 4
5. Roles and responsibilities 5
6. Data Protection Principles 6
7. Collecting personal data 6
8. Sharing personal data 7
9. Subject access requests and other rights of individuals 8
10. Parental requests to see the educational record 10
11. Biometric recognition systems 10
12. CCTV 10
13. Photographs and videos 11
14. Data protection by design and default 11
15. Data security and storage of records 12
16. Disposal of records 12
17. Personal data breaches 12
18. Training 13
19. Links with other policies 13
Appendix 1: Personal Data Breach Procedure 14
Appendix 2: Special Policy Document 16
Appendix 3: Internal Data Sharing Between Trust and Schools 22

1. Aims

Castle Phoenix Trust aims to ensure that all personal data collected about staff, pupils, parents, trustees, governors, visitors and other individuals is collected, stored and processed in accordance with the UK data protection law.

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

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

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

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

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes

	• Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Criminal Convictions Data	personal data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Privacy Notice	a separate notice setting out information that may be provided to Data Subjects when the organisation collects information about them.
Data Privacy Impact Assessment (DPIA)	tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data

4. The data controller

The Trust processes personal data relating to parents, pupils, staff, governors, volunteers, visitors and others, and therefore is a data controller.

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

5. Roles and responsibilities

This policy applies to **all staff** employed by Castle Phoenix Trust, and to external organisations, volunteers and other individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Academy Trust

The Board of Trustees has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

5.2 Data Protection Officer

The data protection officer (DPO) is responsible for providing advice and guidance to the Trust in order to assist the Trust to implement this policy, monitor compliance with data protection law, and develop related policies and guidelines where applicable.

The DPO will carry out an annual audit of the Trust's data processing activities and report to the Trust their advice and recommendations on school data protection issues.

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

Our DPO is the School DPO Service and is contactable via schooldpo@warwickshire.gov.uk or alternatively;

School Data Protection Officer
Warwickshire Legal Services
Warwickshire County Council
Shire Hall
Market Square
Warwick
CV34 4RL

5.3 Headteacher

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

5.4 Data Protection Lead

The Trust has nominated the following individuals as designated persons to be contacted internally in relation to all matters relating to data protection issues, and to make referrals, where necessary, to the Data Protection Officer:

Helen Harrison who is contactable via email - helen.harrison@castlephoenixtrust.org.uk

Emma Phillips who is contactable via email - emma.phillips@castlephoenixtrust.org.uk

5.5 All staff

All members of 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 designated Data Protection Leads in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area

- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

The UK GDPR is based on data protection principles that our Trust must comply with.

Castle Phoenix Trust has adopted the principles to underpin its Data Protection Policy:

The principles require that all personal data shall be:

(1) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');

(2) used for specified, explicit and legitimate purposes ('purpose limitation');

(3) used in a way that is adequate, relevant and limited to what is necessary ('data minimisation');

(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay ('accuracy');

(5) kept no longer than is necessary ('storage limitation');

(6) processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ('integrity and confidentiality').

This policy sets out how the Trust aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

Castle Phoenix Trust shall only process personal data where it has one of 6 'lawful bases' (legal reasons) available to the Trust to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school (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**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018:

- 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

For criminal offence data, we 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

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

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

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with guidance set out in the Trust's Retention Policy.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are circumstances where we are required to do so. These include, but are not limited to situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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

Where we transfer personal data internationally, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

The DPO will send the subject access request to the Trust Data Protection Lead, who will immediately forward to the school. If staff receive a subject access request they must immediately forward it to Helen Harrison, who will ensure that the DPO is informed.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the person should have parental responsibility for the child, and the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or carers of pupils at our school aged 13 and above may not be granted without the express permission of the pupil.

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or carers of pupils at our school [aged under 13] will in general be granted without requiring the express permission of the pupil. These are not fixed rules and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time, where processing is based on the consent of the pupil or parent
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing

- Object to processing which has been justified on the basis of public task, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the Data Protection Lead who may send it to the DPO for information purposes.

10. Parental requests to see the educational record

There is no automatic parental right of access to the educational record and any requests from parents should be treated as subject access requests in accordance with the above.

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/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 we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the School's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we 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, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we 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.

12. CCTV

We use CCTV in various locations around the school sites to oversee the management and security of the site, monitoring health and safety and safeguarding of the pupils, parents, visitors and employees on site. We will adhere to the ICO's guidance for the use of CCTV.

Our lawful basis for using CCTV is public task. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use and how you can contact us if you have any queries relating to the use of CCTV on our premises. See also our CCTV Policy for more information.

CCTV camera locations will vary by site, depending on individual needs and layouts. The Trust Head of Estates is responsible for identifying and approving the most suitable camera positions at each school, in consultation with site leaders. Footage is retained for 30 days and is deleted on a rolling basis. We may keep data for longer where we are required to review footage for an investigation. In such a case we will delete the footage once we no longer need it and in line with our retention schedule.

We have undertaken a data protection impact assessment in relation to our CCTV system to comply with our legal obligations. Our assessment is reviewed every year.

Only authorised staff are permitted to access the system. Any enquiries about the CCTV system should be directed to the Trust Head of Estates.

See our CCTV Policy for more information.

13. Photographs and videos

As part of our school activities, the Trust may take photographs and record images of individuals within the School.

The School will obtain written consent from parents/carers for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where the School needs parental consent, it shall clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where the School doesn't need parental consent, it shall clearly explain to the pupil how the photograph and/or video will be used.

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

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way, unless we have consent, we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

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

14. Data protection by design and default

The Trust shall put measures in place to show that it has integrated data protection into all of its data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Consideration of whether a data protection impact assessment needs to be undertaken. The school will consider this if any of the following kinds of processing plan to be undertaken:
    - Use of systematic and extensive automated processing
    - Large scale processing of data, particularly where it involves special category or criminal offence data
    - Systematic monitoring of publicly accessible areas and any other form of surveillance
    - Processing of biometric or genetic data
    - Transfer of data outside of the European Economic Area
    - Profiling, evaluation or scoring
    - Automated decision making with legal or significant effects
    - Matching or combining datasets
    - Processing of data concerning vulnerable data subjects

- Implementation of new technology or solutions
- If processing would prevent a data subject from exercising a right or using a service or contract

On reviewing these criteria, if the school finds that the processing personal data presents a high risk to the rights and freedoms of individuals we will undertake a data protection impact assessment.

- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

The School will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Staff must ensure passwords are hard for anyone else to guess by incorporating numbers and mixed case into it.
- Encryption software is used to protect all portable devices and removable media on which personal information is stored, 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 Online Safety and Cyber Security policy/acceptable use agreement)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, the School will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

The Trust shall take all reasonable steps to ensure that there are no personal data breaches.

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

When appropriate, the Trust shall report the data breach to the ICO within 72 hours. Such breaches in a Trust context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. Training

All staff and governors are provided with data protection training as part of their induction process.

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

19. Links with other policies

This data protection policy is linked to our:

- Information Security Policy
- Record Retention Schedule
- Child Protection and Safeguarding Policy
- Online Safety and Cyber Security Policy
- Schools Subject Access Request Policy

Appendix 1: Personal Data Breach Procedure

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it in accordance with this procedure.

When appropriate, the Trust will report the data breach to the ICO within 72 hours in accordance with the requirements of the GDPR.

1. Data protection breaches occur where personal data is lost, damaged, destroyed, stolen, misused and/or accessed unlawfully.

2. Examples of how a breach may occur include:

    a. Theft of data or equipment on which data is stored;
    b. Loss of data or equipment on which data is stored;
    c. Inappropriate access controls allowing unauthorised use;
    d. Accidental Loss;
    e. Destruction of personal data;
    f. Damage to personal data;
    g. Equipment failure;
    h. Unlawful disclosure of personal data to a third party;
    i. Human error;
    j. Unforeseen circumstances such as fire or flood;
    k. Hacking attack; or
    l. 'Blagging' offences where information is obtained by deceiving the organisation which holds it.

3. If any member of staff of the Trust, or Governor / Trustee, discovers that data has been lost, or believes that there has been a breach of the data protection principles in the way that data is handled, you must immediately or no later than within 24 hours of first coming to notice, inform the Trust's Data Protection lead.

4. Upon being notified, the Trust's Data Protection lead will assess whether a breach of personal information has occurred, and the level of severity. If a breach has occurred but the risk of harm to any individual is low (for example, because no personal information has left the control of the Trust), then the Trust's Data Protection lead will undertake an internal investigation to consider whether the Information Security Policy was followed, and whether any alterations need to be made to internal procedures as a result.

5. In all other cases, the incident must be notified to the Data Protection Officer immediately, who must follow the Information Commissioner's Office guidelines on notification and recording of the breach. The Data Protection Officer will provide advice and support on managing and responding to the data breach and advise whether they consider the incident to be reportable to the ICO. The priority must then be to close or contain the breach to mitigate / minimise the risks to those individuals affected by it.

All Trust staff and Governors / Trustees are expected to work in partnership with the Data Protection lead and the Data Protection Officer in relation to the following matters

Notification of Breaches

Any member of staff or Governor / Trustee who becomes aware of a personal information breach should provide full details to the Data Protection lead for the Trust within 24 hours of being made aware of the breach. The Data Protection lead will then complete the Data Breach Record Form and Incident Log. When completing the form details should be provided of the reporter's name, the date/time of the breach, the date/time of detecting the breach, and basic information about the type of breach and information about personal data concerned. Details of what has already been done to respond to the risks posed by the breach should also be included.

Containment and Recovery

The initial response is to investigate and contain the situation and a recovery plan including, damage limitation. You may need input from specialists such as IT, HR and legal and in some cases contact with external third parties.

- Seek assistance in the containment exercise. This could be isolating or closing a compromised section of the network, recovery of released documents, finding a lost piece of equipment or simply changing any related access codes
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
- As well as the physical recovery of equipment, this could involve the use of backup records to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Consider whether any individual affected by the data breach should be notified

Assessing the Risks

Levels of risk can be very different and vary on an individual breach of data security depending what is lost/damaged/stolen. For example, if a case file is lost then risks are different depending on type of data and its sensitivity with potential adverse consequences for individuals. The Data Protection lead should consider the following points:

- What type of data is involved?
- How sensitive is the data?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?
- If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate? If it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data has been affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals?
- Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to life?
- Loss of public confidence in the Trust?

All staff and Governors / Trustees should establish whether there is anything they can do to recover any losses and limit the damage the breach can cause.

Appendix 2: Appropriate Policy Document

1. About this policy

The Data Protection Act 2018 sets out the requirement to have an appropriate policy document when processing special category data and criminal offence data.

To fulfil our duties and function as a Trust, we need to process personal information that is listed within Schedule 1 of the Data Protection Act 2018. Most of the processing within Schedule 1 of the Data Protection Act 2018 is required to have an appropriate policy document in place.

This is the appropriate policy document for Castle Phoenix Trust setting out how we will protect special categories of personal data and criminal convictions data.

1. Why we process Special Categories of Personal Data and Criminal Convictions Data

1.1 We process Special Categories of Personal Data and Criminal Convictions Data for the following purposes:

1.1.1 assessing an employee's fitness to work;

1.1.2 complying with health and safety obligations;

1.1.3 complying with the Equality Act 2010;

1.1.4 checking applicants' and employees' right to work in the UK;

1.1.5 verifying that candidates are suitable for employment or continued employment; and

1.1.6 To safeguard pupils, staff, and the community.

1.1.7 To support pupils, staff, and visitors who have a medical condition or disability.

1.1.8 To support pupils with special educational needs

1.1.9 To meet our legal and ethical duties for the provision of education.

1.2 Where we process special categories of personal data and criminal convictions data, we will identify our lawful basis under both Article 6 and Article 9 of the UK GDPR and, where appropriate, identify the condition with schedule 1 that allows for the processing.

1.3 Processing subject to Schedule 1 of the Data Protection Act 2018:

Processing condition for Special Categories of Personal Data	**Description of Processing**
Schedule 1, Part 1 – Conditions relating to employment, social security and social protection.	Processing data concerning health where we have a duty outlined under employment law. Processing data concerning criminal convictions under Article 10 of the UK GDPR where we have a duty under employment law for recruitment,

	discipline, and dismissal. To comply with statutory guidance for safer recruitment Processing information relating to Trade Union Membership to facilitate your right and preference to participate as a member of any trade union, and where there is industrial action that may impact the function of the school.
Schedule 1, Part 2 – Substantial Public Interest Conditions	**Statutory etc. And Government Purposes:** • Compliance with legal obligations and support the provision of education such as completing the school census, providing a common transfer file, to support pupils with medial conditions, to support pupils with special educational needs. • Compliance with legal obligations in connection with legal proceedings • We may also process criminal offence data under this condition.
	Equality of Opportunity and Treatment • To provide equal access to education • Compliance with legislation such as the Equality Act 2010. • To ensure equality of treatment.
	Preventing and detecting unlawful acts • To comply with our duty to safeguard pupils and the community. • To reduce risk to pupils, staff and visitors. • Sharing information with relevant and authorised agencies to support the prevention or investigations of unlawful acts.
	Protecting the Public against Dishonesty • Assisting other agencies in connection with regulatory requirements. • To protect and safeguard pupils and the community.
	Support for Individuals with a Disability or Medical Condition • To ensure we keep pupils and staff safe. • To ensure all pupils can access education and other services in school. • To ensure our employees are properly supported and able to do their job.
	Counselling • To allow for individuals to access confidential counselling services as arranged through occupational health or other support services.
	Safeguarding of Children and Individuals at risk • To protect and safeguard pupils from physical and emotional harm, neglect, or abuse. • To support the wellbeing of pupils at our school.

	Insurance • To process data that is required for insurance purposes.
	Occupational Pensions • To meet our legal obligation to provide a pension scheme for our workforce.
Schedule 1, Part 3 – Additional Conditions Relating to Criminal Convictions, etc.	We process data criminal offence data for the purposes of recruitment and employment vetting. We may also process criminal offence data to protect and safeguard pupils, staff, and the community.

2. Personal data protection principles

2.1 The UK GDPR requires personal data to be processed in accordance with the six principles set out in Article 5(1). Article 5(2) requires controllers to be able to demonstrate compliance with Article 5(1).

2.2 We comply with the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

2.2.1 Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

2.2.2 collected only for specified, explicit and legitimate purposes (Purpose Limitation);

2.2.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

2.2.4 accurate and where necessary kept up to date (Accuracy);

2.2.5 not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation); and

2.2.6 Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

2.3 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

3. Compliance with data protection principles

3.1 Lawfulness, fairness and transparency

Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

We will only Process Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. We can Process Special Categories of Personal Data and Criminal Convictions Data only if we have a legal ground for Processing and one of the specific Processing conditions relating to Special Categories of Personal Data or Criminal Convictions Data applies. We will identify and document the legal ground and specific Processing condition relied on for each Processing activity.

When collecting Special Categories of Personal Data and Criminal Convictions Data from Data Subjects, either directly from Data Subjects or indirectly (for example from a third party or publicly available source), we will provide Data Subjects with a Privacy Notice setting out all the information required by the UK GDPR which is concise, transparent, intelligible, easily accessible and in clear plain language which can be easily understood.

3.2 Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. They must not be further Processed in any manner incompatible with those purposes.

We will only collect personal data for specified purposes and will inform Data Subjects what those purposes are in a published Privacy Notice. We will not use Personal Data for new, different, or incompatible purposes from those disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

3.3 Data minimisation

Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

We will only collect or disclose the minimum Personal Data required for the purpose for which the data is collected or disclosed. We will ensure that we do not collect excessive data and that the Personal Data collected is adequate and relevant for the intended purposes.

3.4 Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We will ensure that the Personal Data we hold and use is accurate, complete, kept up to date, and relevant to the purpose for which it is collected by us. We check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

3.5 Storage limitation

We only keep Personal Data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where we have a legal obligation to do so. Once we no longer need Personal Data it shall be deleted or rendered permanently anonymous.

We maintain a Data Retention Policy and related procedures to ensure Personal Data is deleted after a reasonable time has elapsed for the purposes for which it was being held, unless we are legally required to retain that data for longer.

We will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

3.6 Security, integrity, confidentiality

Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

We will implement and maintain reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of or damage to Personal Data.

3.7 Accountability principle

We are responsible for, and able to demonstrate compliance with these principles. Our DPO is responsible for ensuring that we are compliant with these principles. Any questions about this policy should be submitted to the DPO.

We will:

3.7.1 Ensure that records are kept of all Personal Data Processing activities, and that these are provided to the Information Commissioner on request.

3.7.2 Carry out a DPIA for any high-risk Personal Data Processing to understand how Processing may affect Data Subjects and consult the Information Commissioner if appropriate.

3.7.3 Ensure that a DPO is appointed to provide independent advice and monitoring of Personal Data handling, and that the DPO has access to report to the highest management level.

3.7.4 Have internal processes to ensure that Personal Data is only collected, used or handled in a way that is compliant with data protection law.

4. Controller's policies on retention and erasure of personal data

We take the security of Special Categories of Personal Data and Criminal Convictions Data very seriously. We have administrative, physical, and technical safeguards in place to protect Personal Data against unlawful or unauthorised Processing, or accidental loss or damage. We will ensure, where Special Categories of Personal Data or Criminal Convictions Data are Processed that:

4.1.1 The Processing is recorded, and the record sets out, where possible, a suitable time for the safe and permanent erasure of the different categories of data in accordance with our Records Retention Policy

4.1.2 Where we no longer require Special Categories of Personal Data or Criminal Convictions Data for the purpose for which it was collected, we will delete it or render it permanently anonymous as soon as possible.

4.1.3 Where records are destroyed, we will ensure that they are safely and permanently disposed of.

Data Subjects receive a Privacy Notice setting out how their Personal Data will be handled when we first obtain their Personal Data, and this will include information on how we determine retention periods. The Privacy Notice is also available on our Trust website.

5. Review

5.1 This policy on Processing Special Categories of Personal Data and Criminal Convictions Data is reviewed annually.

5.2 The policy will be retained where we process Special Categories of Personal Data and Criminal Convictions Data and for a period of at least six months after we stop carrying out such processing.

5.3 A copy of this policy will be provided to the Information Commissioner on request and free of charge.

Further information:

For further information about our compliance with data protection law, please contact our Data Protection Lead:
emma.phillips@castlephoenixtrust.org.uk / helen.harrison@castlephoenixtrust.org.uk

Or our Data Protection Officer at the School DPO Service, Warwickshire Legal Service, Shire Hall, Warwick – Email schooldpo@warwickshire.gov.uk (when contacting our DPO, please state which school your query relates to).

Appendix 3: Internal Data Sharing Between Trust and Schools

Link to Main Policy

This appendix forms part of the Castle Phoenix Trust Data Protection and Information Governance Policy and should be read alongside Section 5: Data Sharing and Processing.
It provides additional guidance on how pupil, staff, and school performance data may be shared between schools and the Trust's central team for legitimate educational, operational and improvement purposes.

Purpose

This appendix outlines how data may be accessed and shared internally within Castle Phoenix Trust to support school improvement, performance analysis and the effective delivery of education across all schools.

Scope

This appendix applies to:

- All schools within the Trust
- All Trust employees with cross-school responsibilities
- Any platforms or systems used to collect and analyse performance or pupil, staff or governance data (e.g. SISRA, Arbor, FFT Aspire, Power BI dashboards, Every, Governorhub, etc.)

Legal Basis

Internal data sharing within the Trust is based on the following lawful bases under the UK GDPR:

- **Article 6(1)(e)** – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- **Article 9(2)(g)** and **Schedule 1, Part 2, Paragraph 6** of the Data Protection Act 2018 – Processing of special category data is permitted for reasons of substantial public interest, including statutory and government purposes.

Principles

All data shared between schools and the Trust must be:

1. Necessary and proportionate for the intended purpose.
2. Accessed securely through approved Trust systems.
3. Restricted to authorised staff with a clear professional need.
4. Used solely for educational, operational or improvement purposes.
5. Handled in accordance with the Trust's Data Protection, Information Security and Retention policies.

Authorised Access

All members of the Trust Central Team are authorised to access school-level data, including but not limited to pupil, staff, finance and governance data, without requiring separate headteacher permission, provided access is for legitimate Trust functions and within the remit of their role.

Data Security

- Access must be via named user accounts with appropriate permissions and multi-factor authentication where available.
- Access permissions will be reviewed annually and revoked immediately when roles change or employment ends.