



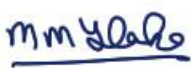
**Shires**  
Multi Academy Trust

**Shires Multi Academy Trust**

1366 Evesham Rd, Astwood Bank, Redditch, B96 6BD

hello@shiresmat.org.uk | www.shiresmat.org.uk

# Data Protection Policy

<b>Policy Name: Data Protection Policy</b>	<b>Policy Reference: MAT-OP10</b>
<b>Owner/Reviewer: COO</b>	<b>Review Date: 19<sup>th</sup> May 2025</b>
<b>Approved by: COO</b>	<b>Approval Date: 19<sup>th</sup> May 2025</b>
<b>Chair of Trust Board</b>  	<b>Review Frequency: Annually</b>
	<b>Date of Next Review: Summer Term 2026</b>

## 1. Aim

Shires Multi Academy 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 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). It is based on guidance published by the Information Commissioner’s Office (ICO) on the GDPR and the ICO’s code of practice for subject access requests.

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

It also reflects the ICO’s code of practice 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
<b>Personal data</b>	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual’s:</p> <ul style="list-style-type: none"> <li>• Name (including initials)</li> <li>• Identification number</li> <li>• Location data</li> <li>• Online identifier, such as a username</li> </ul> <p>It may also include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural or social identity.</p>
<b>Special categories of personal data</b>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual’s:</p>

	<ul style="list-style-type: none"> <li>• Racial or ethnic origin</li> <li>• Political opinions</li> <li>• Religious or philosophical beliefs</li> <li>• Trade union membership</li> <li>• Genetics</li> <li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li> <li>• Health – physical or mental</li> <li>• Sex life or sexual orientation</li> </ul>
<b>Processing</b>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
<b>Criminal Convictions Data</b>	<p>Personal data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings</p>
<b>Data subject</b>	<p>The identified or identifiable individual whose personal data is held or processed.</p>
<b>Data controller</b>	<p>A person or organisation that determines the purposes and the means of processing of personal data.</p>
<b>Data processor</b>	<p>A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.</p>
<b>Personal data breach</b>	<p>A breach of security leading to the accidental or unlawful destruction, loss, alteration,</p>

	unauthorised disclosure of, or access to personal data.
<b>Privacy Notice</b>	A separate notice setting out information that may be provided to Data Subjects when the organisation collects information about them.
<b>Data Privacy Impact Assessment (DPIA)</b>	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

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

Shires Multi Academy Trust is registered 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 Shires Multi Academy 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 The Shires Multi Academy Trust Board

The Trust Board has overall responsibility for ensuring that Shires Multi Academy 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 Shires Multi Academy 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 all schools' in the Shires Multi Academy Trust data processing activities and report to the Trust Board their advice and recommendations on school data protection issues.

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

Our DPO is Warwickshire DPO Service and is contactable via [schooldpo@warwickshire.gov.uk](mailto: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 at each school acts as the representative of the data controller on a day-to-day basis.

### **5.4 Data Protection Champions**

Shires Multi Academy Trust has nominated individuals at each school 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:

Please contact the relevant school office for this information or the COO

### **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 trust of any changes to their personal data, such as a change of address
- Contacting the designated Data Protection Champions 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 Shires Multi Academy Trust must comply with.

Shires Multi Academy Trust has adopted the principles to underpin its Data Protection Policy:

The principles require that all personal data must be:

- (1) Processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')
- (2) Collected for specified, explicit and legitimate purposes ('purpose limitation')
- (3) Adequate, relevant and limited to what is necessary ('data minimisation')
- (4) accurate and, where necessary, kept up to date ('accuracy')
- (5) kept no longer than is necessary ('storage limitation')
- (6) processed in a manner that ensures it is safe and secure, ensuring the measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ('integrity and confidentiality')

This policy sets out how Shires Multi Academy Trust aims to comply with these principles.

## 7. Collecting personal data

### 7.1 Lawfulness, fairness and transparency

Shires Multi Academy Trust shall only process personal data where it has one of 6 'lawful bases' (legal reasons) available to the Shires Multi Academy 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 or another person 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, 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**

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**

## Shires Multi Academy Trust

1366 Evesham Rd, Astwood Bank, Redditch, B96 6BD

hello@shiresmat.org.uk | www.shiresmat.org.uk

- 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 **Shires Multi Academy Trust's GDPR compliant records management policy**

## 8. Sharing personal data

We will not normally share personal data with anyone else except as set out in Shires Multi Academy Trust's Privacy Notice. There are certain circumstances where we maybe 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 that 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 Data Protection Champion. If staff receive a subject access request they must immediately forward it to Designated Data Protection Champions, who will ensure that the DPO is informed.

Information to be released will be collated by Shires Multi Academy Trust and then sent to the DPO for checking and sending out to the applicant.

## **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 those with parental responsibility 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 those with parental responsibility for 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 (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous, or where it is impractical to comply within a month due to school closure. 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 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 the 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.

## Shires Multi Academy Trust

1366 Evesham Rd, Astwood Bank, Redditch, B96 6BD

hello@shiresmat.org.uk | www.shiresmat.org.uk

- 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 Champion who will 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 thus any requests from parents will be treated as subject access requests and dealt as detailed in point 9.3.

### 11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints 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. Shires Multi Academy Trust will get written consent from at least one parent/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 Shires Multi Academy Trust's biometric system(s). We will provide an alternative swipe card which they can use in order to access 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.

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

*If your school uses CCTV, insert the text below. If not, delete this whole section and re-number the remaining sections.*

We use CCTV in various locations around the school site to: [e.g. ensure it remains safe insert any other reasons– ensure these are consistent with those set out in your DPIA]. We will adhere to the ICO's guidance for the use of CCTV.

Our lawful basis for using CCTV is [legitimate interest/public task – check your privacy notice and DPIA]. 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.

Our cameras are situated in [state the areas where the cameras are located]. Footage is retained for [give details e.g. 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 [x] year/s.

Only [insert staff names] are permitted to access the system. Any enquiries about the CCTV system should be directed to [name/job title].

## 13. Photographs and videos

As part of all of our school's activities, Shires Multi Academy Trust may take photographs and record images of individuals within the School.

Shires Multi Academy Trust will obtain written consent from parents/carers of pupils for photographs and videos to be taken of pupils for communication, marketing and promotional materials via the admissions form in their admissions year of entry. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

The [School / Academy Trust] will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where the School's need 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's don'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.

The permission section for images outlines where this may be used or displayed.

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, local newspapers, theatre programs,
- sporting programs and in and around the community
- 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.

#### **14. Data protection by design and default**

Shires Multi Academy 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 (detailed in 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
- Appropriate safeguards being put in place if we transfer personal data outside of the UK, where different data protection laws may apply
- 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**

Shires Multi Academy Trust will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school 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
- Encryption software is used to protect all portable devices and removable media such as laptops and USB devices

## Shires Multi Academy Trust

1366 Evesham Rd, Astwood Bank, Redditch, B96 6BD

hello@shiresmat.org.uk | www.shiresmat.org.uk

- Staff, pupils, trustees or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- 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, Shires Multi Academy Trust 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

Shires Multi Academy 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, Shires Multi Academy Trust shall report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a Shires Multi Academy 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, trustees and governors are provided with data protection training as part of their induction process.

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

### 19. Monitoring Arrangements

This policy will be annually and approved by the full governing board.

### 20. Links with other policies

This data protection policy is linked to our:

- Information Security Policy



## Shires Multi Academy Trust

1366 Evesham Rd, Astwood Bank, Redditch, B96 6BD

hello@shiresmat.org.uk | www.shiresmat.org.uk

- Security Incidents and Breach Reporting Policy
- GDPR Compliant Records Management Policy
- ICT Policy
- Child Protection & Safeguarding

## **Appendix 1: Personal data breach procedures**

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, Shires Multi Academy 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 Shires Multi Academy Trust, Trustees or Governors 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 Data Protection Champion at the school in which the breach relates to within the trust.
4. Upon being notified, the individual school's Data Protection Champion 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 Shires Multi Academy Trust, then the school's or trust Data Protection officer 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 Shires Multi Academy Trust staff, Trustees and Governors are expected to work in partnership with the Data Protection Champion and the Data Protection Officer at each school in relation to the following matters

### **Notification of Breaches**

Any member of staff, trustee or Governor who becomes aware of a personal information breach should provide full details to the Data Protection Champion for the relevant school within 24 hours of being made aware of the breach. The Data Protection Champion 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 Champion 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

### Shires Multi Academy Trust

1366 Evesham Rd, Astwood Bank, Redditch, B96 6BD

hello@shiresmat.org.uk | www.shiresmat.org.uk

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 Shires Multi Academy Trust?

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