



**Data Management**

**The Forest CE Federation**

**General Data Protection Regulations Audit**

**Tony Kidd**

**Company Director**

BA (Hons), PGCE, APIOL, AHOEC, IOL

**Ruth Hawker**

**Company Director**

BSc (Hons), MBA, MSc HRM (Open), CMIOSH, SIIRSM, FCMI, Chartered FCIPD

**Becky Clark**

**Assistant Director**

MAAT, MInstLM



# Contents

<b>1.0 Overall Summary</b> .....	<b>3</b>
1.1 Date of Audit and Key Information .....	3
1.2 Summary of the Audit .....	3
<b>2.0 School Details</b> .....	<b>4</b>
<b>3.0 Explanation of the Audit</b> .....	<b>5</b>
3.1 Audit Purpose .....	5
3.2 Audit Remit .....	5
3.3 Audit Owner .....	5
3.4 Audit Distribution .....	5
3.5 Audit Review Schedule .....	5
<b>4.0 Audit Process</b> .....	<b>6</b>
<b>5.0 Main Report and Evidence</b> .....	<b>7</b>
5.1 Summary of Key Findings .....	7
5.2 School Audit Table .....	9
5.3 Summary of Main Recommendations .....	18
<b>6.0 Appendix</b> .....	<b>19</b>
6.1 Listings of documentary evidence .....	19
6.2 Listings of observations .....	19
6.3 Listings of interviews .....	19



# 1.0 Overall Summary

## 1.1 Date of Audit and Key Information

Date	April 2019
Auditor	Ruth Hawker and Becky Clark

## 1.2 Summary of the Audit


A data protection audit is a way of finding out if data management is taking place in line with the standards required by the General Data Protection Regulations. It lets organisations know where suitable and sufficient controls are in place, where improvements are required and areas of non-compliance.

The aim is; to allow quality improvement in systems and processes to reduce the likelihood of a data breach involving personal identifiable information; to ensure that in the event of a breach the organization can show that it has taken appropriate practical steps outlined as necessary by the Information Commissioners Office.



## 2.0 School Details

School Name	The Forest CE Federation
School Address	Whittlebury CE Primary, Tiffield VA Primary School, Stoke Burerne CE Primary and Gayton CE Primary
Chair of Governors	Mr Daniel Lister
Type of School	Academy
School Category	Primary
Age Range of Pupils	4-11
Number of Pupils on Roll	
School Description	

 (SEP)

The Forest CE Federation is made up of four small village rural primary schools based in the beautiful countryside surrounding the market town of Towcester.

The three schools, Whittlebury CE Primary School, Tiffield VA Primary School and Stoke Bruerne CE Primary School federated in 2012 and were the first federation of three schools in Northamptonshire. This union has enabled the trust to pool their strengths and experiences in the classroom, alongside leadership and governance to create a better quality learning experience for all of their pupils.

In September 2016 the trust welcomed Gayton CE Primary into the federation.

The trust is part of the Church of England Schools, closely affiliated with the Diocese of Peterborough.



## 3.0 Explanation of the Audit

**This audit does not supersede existing procedures or arrangements associated with GDPR.**

### 3.1 Audit Purpose

The audit provides an assessment of whether your organisation is following good data protection practice. The audit plays a key role in assisting organisations in understanding and meeting their data protection obligations. The audit looks at whether you have effective controls in place alongside fit for purpose policies and procedures to support your data protection obligations. We check if you are following data protection legislation as it applies to your organisation and will report with recommendations on how to improve.

### 3.2 Audit Remit

The audit must be perceived as a positive management tool for the employer. It should have unrestricted access to both external and internal auditors, keeping cost-effectiveness, independence and objectivity under review.

The audit will ensure the undertaking of the employers responsibilities outlined in section 1.1.

### 3.3 Audit Owner

The Headteacher is the owner of the audit and is responsible for it's distribution and action. The Governors have the responsibility to consider and act upon the findings in accordance with the General Data Protection policy and other related school policies.

### 3.4 Audit Distribution

The audit will be distributed to staff (teachers and support staff) and governors if applicable. New staff and governors will be informed of the actions of the audit during their induction as a positive management communication tool to embed the importance of GDPR into the schools culture.

### 3.5 Audit Review Schedule

The audit will be conducted on a annual basis, unless the audit has been activated or changes occur which then require a review.



## 4.0 Audit Process

The audit reflects ICO guidance for leading GDPR at work. It also audits the employer's performance of legal duties placed on the employer under the General Data Protection Regulation which was introduced in May 2018.



## 5.0 Main Report and Evidence

### 5.1 Summary of Key Findings

Compliance Indicator	Main Findings
<p><b>PLAN:</b></p> <p>How does the school demonstrate the governing body/trustee's commitment to GDPR?</p>	<p>the Governors have agreed the GDPR policy.</p>
<p><b>DO:</b></p> <p>What has the school done to ensure the organisation, at all levels including the governing body/trustees receives competent GDPR advice?</p> <p>How is the school ensuring all staff – including the governing body/trustees – are sufficiently trained and competent in their GDPR responsibilities?</p> <p>How confident is the school that their workforce, particularly data controllers and processors are made aware of their responsibilities for data protection.</p> <p>What systems are in place to ensure the schools organisation's risks are assessed and that sensible control measures are established and maintained?</p>	<p>Staff are aware of GDPR, but further training is required to ensure all staff are fully aware of their responsibilities.</p> <p>Staff have been informed of GDPR, but the school need to implement further training. This can be completed by adding the GDPR information video to the staff area available on the Plumsun website.</p> <p>The staff are aware of GDPR and data controllers have taken ownership of their responsibilities.</p> <p>The school has taken out measures to ensure that data is kept safe, secure and up to date. This includes locks on doors, screens moved so members of the public are unable to view potentially sensitive data.</p>
<p><b>CHECK:</b></p> <p>How well do the Governing Body/Trustees and Senior Managers know what is happening on the ground, and what audits or assessments are undertaken to inform the Governing Body/Trustees about what the school and contractors actually do?</p> <p>Where significant changes in data processing arrangements are intended Governing Bodies/Trustees are made aware of the results of data protection impact assessments.</p>	<p>The Senior Managers and Governing Body are aware of GDPR.</p> <p>It is recommended to the school that GDPR is on the agenda of the Full Governing Body as a standing item, even if there is nothing to report.</p>

**ACT:**

What does the organisation do to ensure appropriate senior management and Governing Body/Trustee review requirements of general data protection and act upon findings of audits and privacy impact assessments.

It is recommended that the SLT and the governing body review progress in addressing vulnerabilities or adopting recommendations at regular intervals. SLT and Governors conduct periodic checks to ensure that processes and work place practices do not compromise data protection.



## 5.2 School Audit Table

Data Held	
Questions	Answers
<b>Core Actions</b>	
Undertake a data audit of information held and processed by the school in consultation with stakeholders.	Examples Consult with staff, governors and other stakeholders.
<b>Process (How can it be done)</b>	
What Data Formats do the school use for data: (Computers, photographs, paper, video, audio)	Computer, paper, photographs (video – eg school plays, pupil performances?)
Which data subjects do the school hold data on: (Staff, pupils, parents, volunteers, supply staff, customers, suppliers)	Staff, Pupils, Parents, Volunteers, Supply Staff, Customers
Which data classes do the school hold: (Personal details, lifestyle, employment details etc.)	Personal details, Employment Details
Which Data Sources do the school hold: (Third party information)	Examples; Information form Nursery Schools, Information from NHS (care plans)
Who does the school share data with: (Data Subjects themselves, Relatives, guardians or other persons associated with the data subject, current, past or prospective employers of the Data subject, Healthcare, social and welfare advisers or practitioners, Education, training establishments and examining bodies, Business associates and other professional advisers, Employees, Suppliers, providers of goods and services, Persons making an enquiry, Trade Unions, Police Forces, Local Government)	The school has completed an information audit and is available to view on the Trust and School's website.

Plan	
Questions	Answers
Core Actions	
Process (How can it be done)	
Have Governors/Trustees been informed of their responsibilities under GDPR	Yes – The GDPR policy has been agreed by the Academy Trust.
Do Governor agendas detail the number of subject access requests, possible breaches, privacy impact assessments	It is recommend that data protection be a standing item on the agenda

Do	
Questions (School)	Answers (School)
Process (How can it be done)	
Is there evidence that the school has identified a lawful basis for processing and documenting personal data?	Yes The information audit has been completed and available on the school website.
Has the school documented what personal data is held, where it came from, who you share it with and what you do with it?	Yes The information audit has been completed and available on the school website.
Is there evidence that the school has identified a lawful basis for processing and documenting personal data?	Yes The information audit has been completed and available on the school website.
How has the school recorded consent?	Yes Answer: The school ask for consent currently, suggest that the schools issue a statement of how they will use photographs and personal data going forward.
How does the school record and manage on going consent?	Answer:

	In most cases consent is not used as the legal basis for processing. Where consent is requested, this is locked in the school office.
Has the school provided privacy information to individuals?	Yes  Answer: Privacy Notices are on the Trust and school website. They are also available on request from any of the schools in the trust.
Does the school have a policy/procedure in place to respond to requests for access and to view personal information	Yes  Answer: The policy is available to view on the trust/schools website.
How does the school ensure that the data remains accurate and up to date?	Answer: The schools hand the pupil data sheets direct to the parents/carers to ensure that they are handed to the correct person.
How does the school dispose of personal data that is no longer required or where an individual has asked for it to be erased?	Answer: The school currently shreds all documentation that this no longer required.
Has the school an appropriate data protection policy?	Yes  Answer: The policy is available on the trust/schools website.
Has the school made all employees aware of GDPR and how?	Partial Yes  Answer: The staff are aware of GDPR but further training is required to ensure all staff in the trust are fully aware of their responsibilities.
Does the school have a written contract with processors?	Yes  Suggestion: Complete a list of data sharing companies with their ICO registration number.
The school has identified an effective process to report any data breach?	Yes  Answer:

The policy is available on the trust/schools website.

## Check

Questions (School)	Answers (School)
Has the data subject been informed of the processing?	Yes
Has the schools data audit been uploaded to website?	Yes
Does the website contain a specific privacy notice covering the information collected as a data subject when accessing the organisations website?	Yes
Has the data subject been informed of the people or organisations their data may be passed onto?	Yes
Has the data subject given their consent to the processing?	N/A in most cases – permission sought to upload pupil images to websites and social media.
If the data subject has not given their consent, can the processing be justified on the basis of necessity?	Yes – Public Interest
If the data collection includes sensitive data, has the data subject given their explicit consent to process such data?	No – Required by other legislation specified in parents/carers policy
Is the processing of data legal? (The legality of the processing must not be in question. Eg. It is unlawful to use a person’s National Insurance number as a personal identifier)	Yes
Has it been made clear to the data subject what the data will be used for?	Yes
Have any ‘non-obvious’ uses of the data been made clear to the data subject. i.e. things that the data subject would not have realised you were doing from a general description of the processing	N/A

Is there a clear reason for processing each item of data?	Yes
Has it been verified that the same outcome could not be achieved, safely and effectively, with less data?	Yes
Where information is collected on a form, does it indicate to the data subject that information which is essential and that which is voluntary to give?	Yes
Is the information that is being processed adequate for the purpose? (For example, if information is collected with the intention of using it later to prove the identity of individuals, a first and last name may not be enough.)	Yes
Is the information that is being processed no more than is necessary? (For example, in collecting information for identification purposes it may be excessive to request a person's last three addresses.)	Yes
Have steps been taken to ensure the accuracy of the data?	Yes
Is there a system of rolling reviews of data to keep the data up to date? (Note: if data is inaccurate or out of date it would not only breach the fourth principal, but it could breach the third as well because the data might not be adequate for the purpose)	Yes  Answer: Parents and staff are asked to check data sheets on an annual basis. Where information comes to light this is recorded in pupil files and SIMS.
Are the data being kept for no longer than is necessary to comply with relevant laws and regulations that define minimum periods of retention?	Yes  Suggestion: Ensure that both hard and soft copies of personal data is reviewed and being kept in line with the schools retention document.

If data are being kept for periods longer than the legal minimum is there a good reason for doing so?	Yes
Are files periodically 'weeded' of irrelevant data?	Yes
Is there a clear justification for the length of time the data are retained?	Yes
Can it be confirmed that data are not being kept on a 'just in case' basis?	Yes
Does the data subject know that their personal data are being processed?	Yes
Does the data subject know why their personal data are being processed?	Yes
Does the data subject know how their personal data are being processed?	Yes
Has the data subject been informed of their rights of access?	Yes
Is the level of security adopted appropriate to the risks represented by the processing and the nature of the data to be protected? (Consideration should be given to the measures taken to guard against theft, malicious damage or corruption (including computer viruses), unlawful access, accidental disclosure, loss and destruction.)	Yes  Answer: Governors view documents via the Governor Hub.  Recommendation: In the Code of Conduct include a section regarding downloading and deletion of any files that may contain personal data if applicable.
Do the school conduct periodic checks for insecure personal information in classrooms, offices and meeting rooms	Yes
Has the school ensured that IT equipment shuts down after a specified idle time	No  The trust/school use encrypted hard drives, the laptops are not encrypted. Idle time is not enabled on the computers/laptops.

Is the school registered with the ICO, including the notifying the ICO of the appointed DPO	Yes
Are there clear lines of responsibility for the processing operations?	Yes
Are staff that deal with personal data aware of the purposes for which it has been collected?	Yes
Are staff that deal with personal data aware of the parties to who they can legitimately disclose the data?	Yes
Are staff that deal with personal data aware of the parties to who they can legitimately disclose the data?	Yes
Has the school developed a process and checklist to be used by staff when a subject access request is received	Yes
Has the school checked that it is able to meet a data access request within the legal timeframe for pupil/staff member	Partial Yes – suggest that all schools simulate a data access request around a specified individual as a means of establishing a procedure.
Has the school undertake checks to ensure that staff are not using duplicate passwords. (e.g. the same password is used to access the school website is also used to access SIMS)	Yes  Suggestion - The IT technician requests all admin access, SIMS etc. passwords to be changed. Staff should be prohibited from enabling machines to 'auto fill' passwords.
Are non-school personnel and students who handle personal data adequately supervised?	Yes
Where consultants/contractors have access to or process data is there a data protection statement in place in the contract setting out their obligations with regard to the security and use of data? e.g. Computer service engineers	Yes  Contractors have sent Data sharing agreements.
Are appropriate measures in place for the secure disposal and/or destruction of personal data that are longer required?	Yes – documentation is securely shredded.
Where applicable, has the consent of the data subject been obtained to transfer personal data to countries outside the EEA which are not designated as 'adequate' by the Information Commissioner?	N/A

To the best of your knowledge has it been determined whether any other legal or regulatory conditions apply to the processing of the personal data?	Yes
Where such conditions apply please state the applicable legislation and/or regulations.	N/A
Where such other conditions apply, are appropriate procedures and controls in place to ensure compliance?	N/A

Act	
Questions (School)	Answers (School)
Core Actions	
Process (How can it be done)	
Is there a sufficient process/policy in place to assess the likely risk to individuals as a result of a breach	Yes
Are staff aware who the relevant supervisory authority is for their processing activities	Yes
Does the school have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet?	Yes
Does the school know what information they must give to the ICO about a breach	Yes
The school has a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms	Yes
The school knows they must inform affected individuals without undue delay	Yes
The school knows what information about a breach they must provide to individuals, and that they should provide advice to help them protect themselves from its effects	Yes
The school documents all breaches, even if they don't all need to be reported	Yes



## 5.3 Summary of Main Recommendations

Observations	Recommendations
<b>General</b>	<ul style="list-style-type: none"><li>• Review the information audit periodically, ensure it is kept up to date.</li><li>• Complete a 'dummy' data subject request for one pupil to ensure staff are fully aware of the procedure.</li><li>• GDPR to form part of governor agenda's.</li><li>• Change the 4 in the information audit to include 'Public Task'.</li></ul>
<b>Website</b>	<ul style="list-style-type: none"><li>• Ensure that any updates to the information audit are uploaded to the school website.</li></ul>
<b>Physical Data</b>	<ul style="list-style-type: none"><li>• Is the trip documentation necessary to be taken on a trip, for example use the Plumsun app to ensure limited paperwork is taken on school visits.</li><li>• Ensure Idle time is enabled onto all the trust/schools laptops.</li></ul>
<b>Staff Training</b>	<ul style="list-style-type: none"><li>• Ensure staff lock their computers/laptops when they leave their computers/laptops</li><li>• Staff should be directed not to save passwords onto their systems. (Especially using 'auto fill' facility).</li></ul>

## 6.0 Appendix

### 6.1 Listings of documentary evidence

- Parent's /Carers privacy notice
- Staff privacy notice
- Information Audit
- Schools GDPR Policy

### 6.2 Listings of observations

- Sample visits to main school office, staffroom, and document storage area, sample classroom.
- Review of public face of website with specific reference to documentation related to GDPR.

### 6.3 Listings of interviews

- Meeting with Trust Business Manager and Administrative Staff.
- Spoke to school workforce.