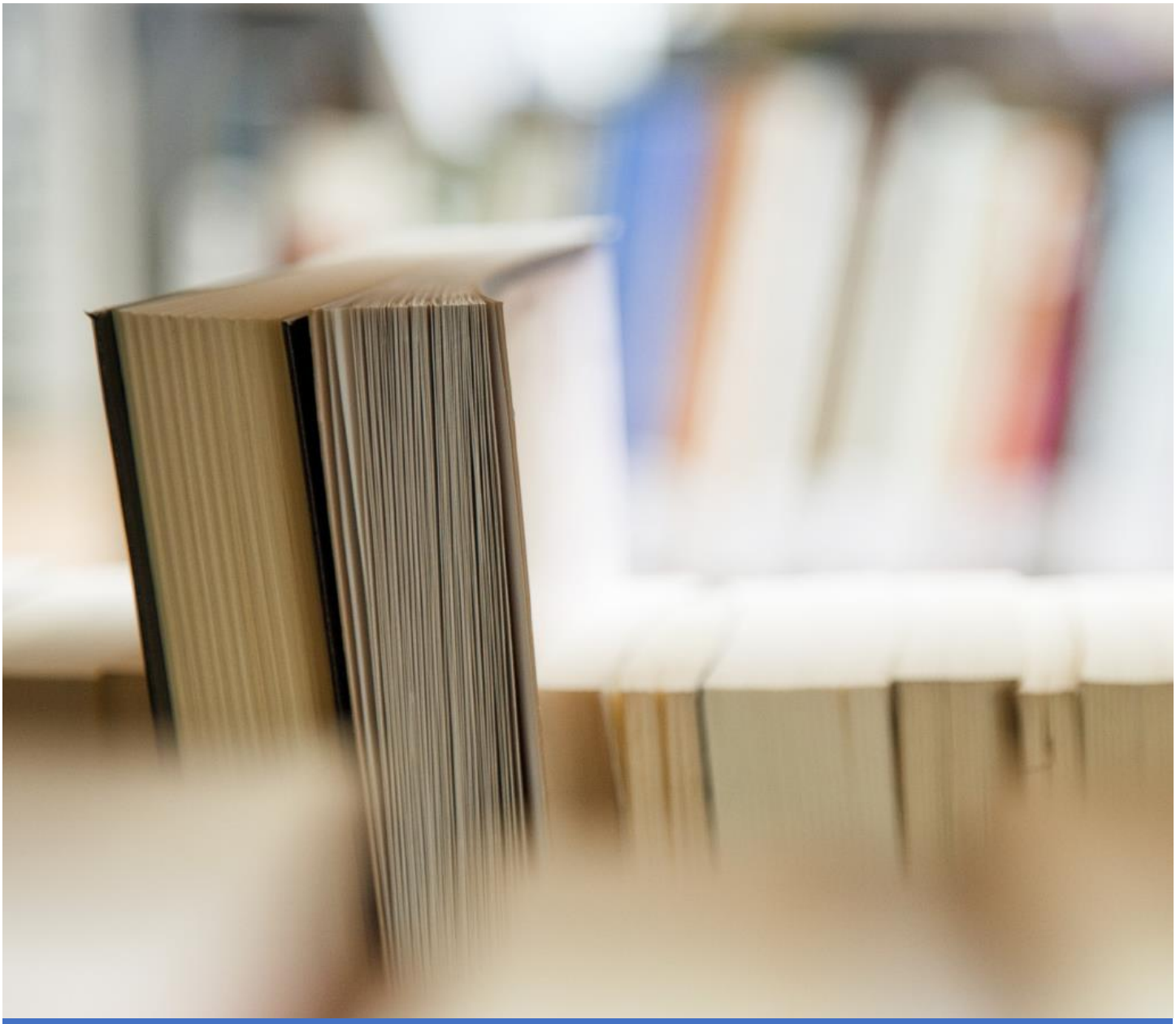


College Town Primary [109828] Data Protection Officer report to Governors

1st[th] September 2021

Author: Darren Rose CIPP/E

Table of Contents

Appendices

Executive summary

Over the last 12 months a comprehensive review has been carried out resulting in a large number of observations requiring action within the school. It is understood that there has been, and will continue to be, ongoing impact from the pandemic which will dictate school priorities and available resources to complete these actions moving forward. It is however advised, in order to demonstrate ongoing compliance, to continue to allocate resource to completing the actions, even if that resource is limited.

In parallel to the ongoing review, the program of training, began in the autumn term will continue and be expanded to ensure good practice is instilled and supported within the school and help reduce any possibility of a data breach as a result of an avoidable common mistake by a staff member.

Overview of data protection incidents within the school (Sept 2020 – Sept 2021).

Data Breach Incidents

The school has not recorded any data breach incidents during this period. All staff awareness training, including an element on how to identify and report a data breach, has been provided to the school for distribution. This will ensure that all data breaches are correctly identified and support the number reported.

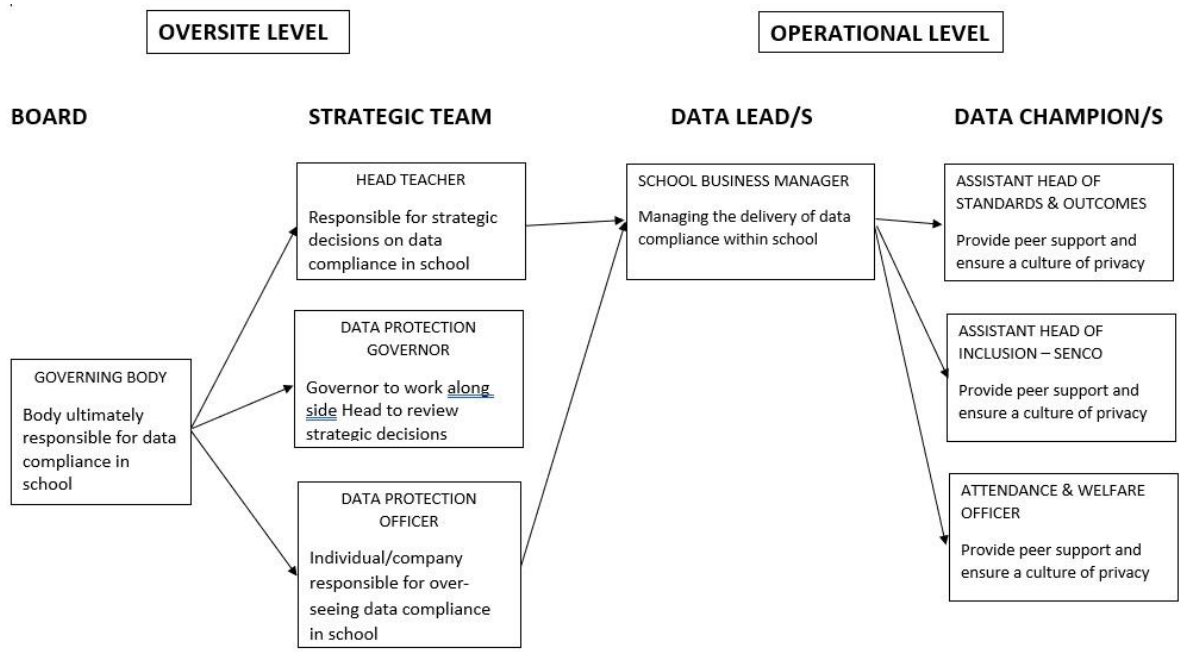
Subject Access Requests

The school has not received any subject access requests during this period. All staff awareness training, including an element on how to identify a subject access request, has been provided to the school for distribution. This will ensure that all subject access requests are correctly actioned and support the number reported.

Other Subject Requests

The school has not received any subject requests (including withdrawal of consent, objection to processing etc) during this period. The focus of the current policy and procedures review, and suggested school progress check, is to ensure that the school would be able to receive and action such a request.

An overview of the school data protection organisational structure.



This structure was created to provide the school with the required levels of strategic oversight from the board of governors and head teacher, operational implementation by line managers and remote support, training, procedural support, legal oversight and sign off from DHR Consultancy. The role of the Data Protection Lead is to act as a point of contact between the school and the Data Protection Officer as well as organise and co-ordinate the implementation of any required action identified by the Oversight group or Data Protection Officer.

This organisational structure fulfils the requirements of the Information Commissioner's Office as detailed in the recent accountability framework. [A copy of the ICO interactive Excel accountability framework tool has been provided with this report].

Summary of resources provided as part of the Data Protection Officer support package.

The remote DPO support package, currently provided by DHR Consultancy, contains unlimited levels of email and scheduled telephone support as well as free resources including:

1-day onsite consultancy visit

Can be used for either group training sessions, compliance audit [as detailed in Appendix 1], or other onsite actions involving meetings or breach investigations.

10 Hrs of remote training via either Zoom or MS Teams

Can be used as either part of a training program for the data protection lead(s) or used as separate topic sessions or workshops, such as subject access requests, for individuals or a group.

Online training package for up to 150 staff

Select Skills online training package allows a school to invite staff, via email, to complete a course selected from a library of available courses as well as provide individual or group reports on completed and outstanding courses. The package provided as part of the support contract accommodates up to 150 candidates (members of staff) to sit a training course, refresher course or open a link to a school policy, up to 6 times per year. [Screen prints of the platform, current courses and staff reporting, can be seen in Appendix 2]

Over the previous academic year, the pandemic had an impact on the works completed plus access to these resources, due to other understandable priorities.

It is the aim of this report to raise awareness of the resources included within the package and ensure they are utilised as staff availability and school calendar allow.

Overview of actions completed to date.

Review of the School data protection policies

A full review has been made of the following school policies:

- Data Audit Log
- Data Protection Policy
- Data Security Framework
- eSafety and Data Security Policy
- Acceptable Use Agreements (Appendix 2 of the eSafety and Data Security Policy)
- The use of digital images and video (Appendix of the eSafety and Data Security Policy)

Amended versions, complete with comments, have been provided to the school data protection lead (Cath Wadsworth). A summary of the reviews can be seen in the **Compliance Review Summary 2021** in Appendix 3, with actions which are currently under discussion for actioning over the coming months.

For clarification it is my opinion that in their current state they would satisfy an initial inspection by the Information Commissioners Office, the recommendation of further actions is to further refine them as part of ongoing and constant review.

Review of the School privacy notices.

A full review has been made of the following school privacy notices:

- Privacy notice Pupil and Parents
- Privacy notice for Governors
- Privacy Notice for School Workforce

Amended versions, complete with comments, have been provided to the school Data Protection Lead (Cath Wadsworth). A summary of the reviews can be seen in the **Compliance Review Summary 2021** in Appendix 3, with actions which are currently under discussion for actioning over the coming months.

For clarification, amendments were made to ensure the privacy notices met the requirements of Article 13 of the GDPR. Full detailed Art13 review grids were completed and shared with the school Data Protection Lead for inclusion into the school compliance records.

Please Note: At this stage, no processing activity has been identified which would require an Article 14 privacy notice i.e. where personal data is obtained from a source other than directly from the data subject or representative and which would not reasonably be expected (an example of this would be a purchased marketing list).

Review of the School Article 30 record of processing activity.

A full review of the school data audit log was completed against Article 30 of the GDPR. Full details provided in the **Article 30 RoPA Review Grid for processing activities as a Data Controller** in Appendix 4.

While the existing data audit log does meet the Article 30 requirements the additional information, required for the Data Protection Act 2018, is recommended to be reported in the same place i.e., within the record of processing activity of RoPA.

Review of the schools Information Security Management Systems (ISMS).

A review of the school's data protection security measures was conducted using the policy documents and conversation with the schools Data Protection Lead (Cath Wandsworth).

An ISMS self-audit template, compiled from resources and guidance provided by the Information Commissioners Office and the National Cyber Security Centre (NCSC) was completed and is visible in Appendix 5.

The initial review and discussion did provide enough evidence to demonstrate it fulfilled certain requirements but there are some follow on conversations to be had with the schools IT provider which will be completed over the coming months.

Staff training.

Over the last 12 months staff training has been completed through training videos provided on the SelectSkills Vimeo channel provided by the DHR Consultancy; including:

- **Preventing common data processing mistakes in your school** – aimed at SLT
- **Avoiding common mistakes when processing personal data** – aimed at non SLT staff
- **Understanding and managing a SAR** – aimed at the school Data Protection Lead
- **The impact of insufficient technical & Organisational measures** – also aimed at DPL's
- **Secure handling of SEND records** = aimed at all staff who process SEND records.

In the recently released Information Commissioners Officer accountability framework a requirement has been added for more accurate training records as well as a proof of understanding from those individuals completing the training. In answer to this DHR has added an online training tool to the support package, as detailed previously, as well as an additional "**All Staff data protection awareness**" course available for new starters and staff refresh training.

Overview of next recommended actions.

Continuation of the policies and privacy notice review.

As part of the ongoing review of compliance documentation, it is advised that the school allocated ongoing resource, or agenda items, to review the observations and recommendations made in the recent policies and privacy notice review. Inclusion of a single policy per term, possibly into the existing scheduled meeting structure as an agenda item, would allow realistic allocation of resource and ensure completion.

Just for clarification and to help establish priorities, the policies and notices in their current state would pass challenge by the Information Commissioner's Office, therefore discussion, is recommended as demonstration of best practice and ongoing review.

Review of new suppliers appointed by the LA.

During the Summer term termly DPO meeting several new suppliers who are appointed by the Local authority to provide core services to schools, were discussed. As part of the school statutory compliance, the new suppliers, once confirmed by the Local Authority, who process or share personal data, will require a due diligence process to be completed. That is if the LA information governance team has not already done so, as part of their central procurement process.

Continuation of training

It is recommended for the school, unless other capability exists, to use the SelectSkills package provided by DHR with the initial rollout of the All-staff awareness course and establish a reportable baseline for the school compliance records.

It is also recommended that the school review and establish additional training required for staff who are members of the operational group (SENDCo, Safeguarding Lead, Deputy etc.) and plan interactive sessions using the included elements of the remote package.

Discussion of available courses and identified training requirements are scheduled for the next termly DPO meeting on the 12th November 2021.

Review of data mapping and process flows

If resource and other priorities allow, it is recommended that a review of school process flows, and data mapping be completed. The review of the processes can either be completed as part of the progress visit (if no existing flows exist) or as a remote review if already available.
The review would identify additional data items to be added to the existing data audit log and move the school closer to the expectations of the Information Commissioner's Office under the new accountability framework.

Appendix 1 Details of a school progress check

The school progress check uses the Information Commissioners Officer Accountability Tracker and experience of school operations to provide a high-level review of your existing position on the current data protection laws including the UK General Data Protection Regulation, Data Protection Act 2018 and the Privacy in Electronic Communication Regulations.

Delivery method.

The review is completed via a 45-minute interview, per section, conducted in a questioning friend, non-intimidating atmosphere to encourage engagement and obtain the best outcome.

Sections covered within a school progress check:

1/ Procurement

Areas discussed:

- Suppliers / other 3rd Party compliance review
- Data sharing agreements
- Data transfers and safeguards
- Evidence of technical and organisation measures taken by suppliers
- Sub processor/sub-contractor notifications

2/ HR

Areas discussed:

- General record keeping
- Staff contracts
- Pre-employment medical questionnaire
- Staff training
- Staff induction process
- Staff leaver process
- Right to work documentation
- Unsuccessful applications – retention and destruction
- Security measures (electronic/Physical)
- Archiving
- Data taken/sent out of the school grounds

3/ Safeguarding

Areas discussed:

- General record keeping
- Notice causes of concern process
- Onward school document transfers
- Record handling during home visits
- Medical alert sheets/SSIP's in the classroom
- Record handling on school trips
- Volunteers
- Security measures (electronic/Physical)
- Archiving
- Data taken/sent out of the school grounds

4/ Communications

Areas discussed:

- General record keeping
- Parent / Pupil portal
- Texting services
- Parent photo and image consent form
- Website
- Social media
- Photography at events
- Security measures (electronic/Physical)
- Archiving
- Data taken/sent out of the school grounds

5/ Admissions

Areas discussed:

- General record keeping
- Source of new pupils - Applications, Prospectus or school visits
- Registration form/Data Collection sheets
- Admissions process
- Prospective parents
- Prospective parents - Who do not take the offer
- Security measures (electronic/Physical)
- Archiving
- Data taken/sent out of the school grounds

6/ SEND

Areas discussed:

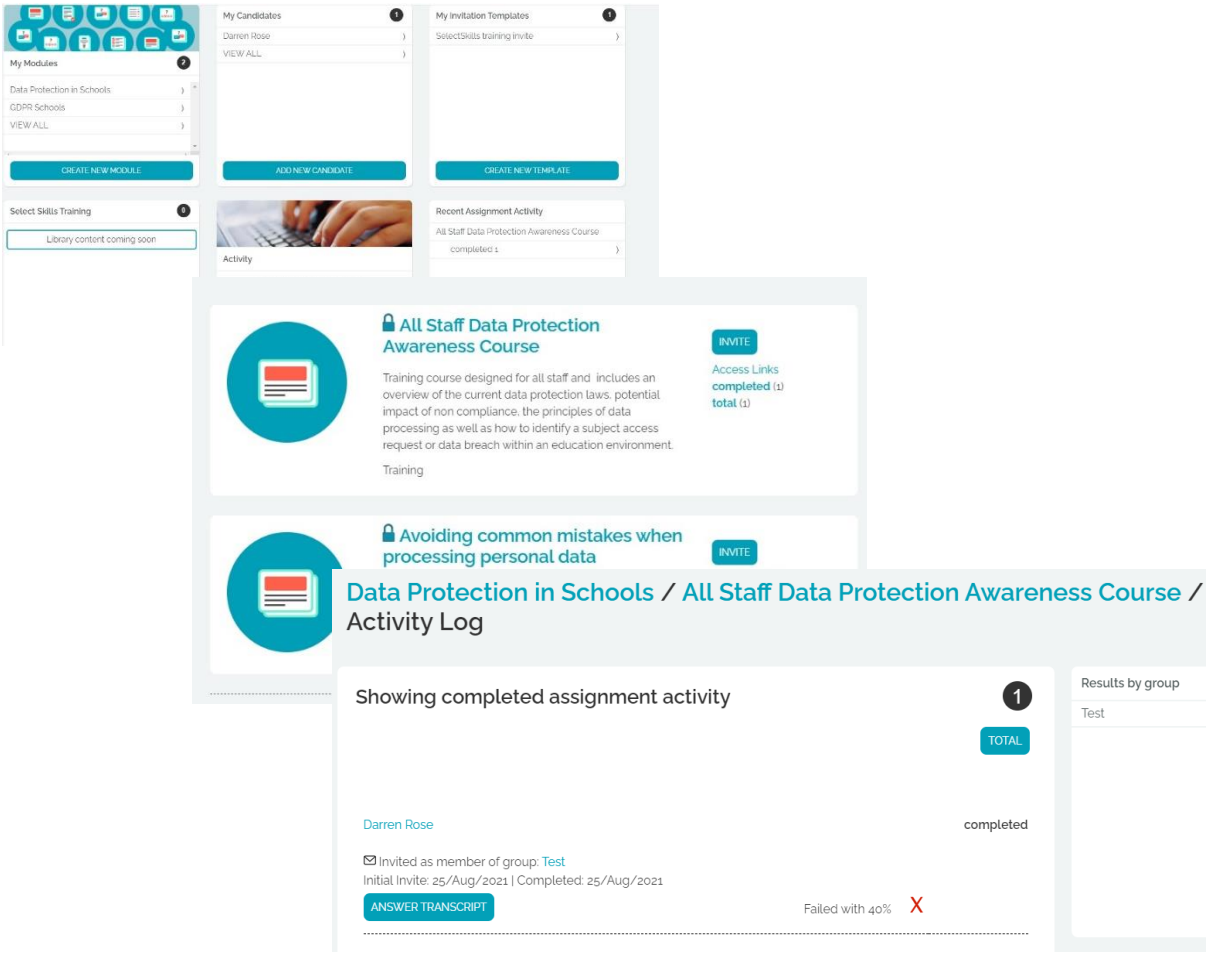
- Learning support staff
- EHCP's storage, processing and transit
- EHCP sharing as part of a review panel
- Security measures (electronic/Physical)
- Archiving
- Data taken/sent out of the school grounds

7/ IT

Areas discussed:

- User acceptance policy
- User account creation and management
- User access control
- BYOD – Mobile devices and removable storage
- ISMS Documentation and record keeping
- Online sharing / Cloud services
- External support
- Hardware repairs
- Hardware; end of life processing
- Email
- Backups
- Anti-Virus Software
- Security of IT equipment

Appendix 2 Online training package – SelectSkills



Appendix 3 College Town Primary Compliance Review Summary 2021

A full compliance review was carried out for College Town Primary against the latest Data Protection Laws and guidance from the Information Commissioners Office and the National Cyber Security Centre with detailed comments made in each document and a summary of overall actions/observations and onward actions required of the school below.

Summary of reviewed documents:

Document reviewed:	Actions/Observations:	Onward Actions:
Data Audit Log	Actions and observations detailed in a separate Article 30 review log which can be found in the compliance review folder published with this summary.	Consider the recommendations made in the review log.
Data Protection Policy	Versioning added (V3). Updated to latest UK Data Protection Laws (Data Protection Act 2018, UK General Data Protection Regulation) including Principles of data processing, categories of personal data, Subject Access request response times and potential charges.	Update highlighted elements (time out period for auto screen lock of workstations etc.) Pass to governing body for final approval and school adoption.
Data Security Framework	Versioning added (V3). The Information Security Management Systems (ISMS) audit, produced by the National Cyber Security Centre www.ncsc.gov.uk, was completed using this policy and placed in the compliance review folder. Observations. No mention is made of the process to monitor ongoing adherence to the stated procedures. Consider using data walks to demonstrate accountability and a strong culture of privacy. A copy of the template can be seen in the compliance folder.	Update highlighted elements (time out period for auto screen lock of workstations, references to DCSF changing to DfE etc.) Review the ISMS audit Action the ongoing elements Pass to S&F for final approval and school adoption. Complete a random data walk either after school or at lunch time, for a sample location containing sensitive or confidential information such as admin office, SENCO office, Classroom etc, and add them to the school compliance folder.

Document reviewed:	Actions/Observations:	Onward Actions:
E-Safety and Data Security Policy	Versioning added (V3). ➢ Emphasis moved from loss of reputation of the school to undermine the data subject's perception of the school. ➢ Highlighted of webmail restrictions for discussion and possible removal. ➢ Highlighted the 5minutes for auto screen lock. Appears to be low as based on experience of other schools 10 or 15 minutes is more common. ➢ Comment made on document labelling and disposal based on the document label given. Is it used extensively within school at least enough to base a policy on it? ➢ Highlighted webcams for review as usage may have changed to accommodate distance learning during the recent pandemic. ➢ Question asked regarding the restrictions for volunteers using their own mobile phones when attending a school trip as a responsible adult. ➢ Further detail added on the possible penalties under the Computer Misuse Act to provide understanding and gravity of possible implications. ➢ Updated Appendix 1 Current legislation… with PECR description as it is a key component of the data protection laws.	Review the highlighted sentences on non-permitted use of internet-based webmail services to access work email or send sensitive information as the commonly used email services today, such as office 365 or Google mail are classed as Internet based webmail services. How are staff, not directly involved in data processing, trained? Review the highlighted sentence on Webcams and never used to contain images of staff pupils. Review the controls in place for personal mobile use of volunteers on school trips. Possibly consider guidance and "**only for personal use**" declaration form. Recommend a separate exercise is carried out to review the school's compliance with the PECR in communications and the school website.

Document reviewed:	Actions/Observations:	Onward Actions:
Acceptable Use Agreements (Appendix 2 of the E-Safety and Data Security Policy).	8/ Title and link updated for the Guidance for safer working to the latest 2020 version to include remote learning during COVID. 19/ Note added as the declaration states “Any electronic personal or sensitive data taken off-site will be password protected.” And yet the body of the policy states “Any equipment where personal data is likely to be stored must be encrypted”.	Review 19/ and update. Advised to update the AUP to match the policy body text i.e. …must be encrypted as Article 32 of the GDPR expects safeguards are adopted appropriate to the category of personal data being processed. Sensitive (special category of personal data defined under Article 9) and criminal conviction/prosecutions (defined under Article 10) high the highest elevation due to the potential impact and therefore the strongest safeguard is expected.
The use of digital images and video (Appendix of the E-Safety and Data Security Policy).	Recommend a review of image consent capture as internal and external school use appear missed. ➢ Link updated to ThinkYouKnow website CEOP safety.	Recommend discussion and review of this process.
Privacy Notice Pupil & Parents	Version updated to version 3. Audit completed to the GDPR Article 13 requirements and included in the compliance review folder as a separate document. ➢ Confirmation of College Town Primary as the Data Controller added. ➢ Details of the Data Protection Officer added.	Review the Article 13 review document and consider the amendments or additions proposed. Add further detail to international transfers if available. Review and add details of any legitimate interests of the school. Review and add to the 3rd Party software list.

	➢ Additional purposes, common to schools added to Why we collect and use information. ➢ Change of purpose declaration added as required under UK GDPR. ➢ Lawful basis information updated to the latest data protection laws. ➢ Data Protection Act Schedule 1 conditions of processing added. ➢ Added staff training information to create perception of processing within the school. ➢ International data transfers added as required under the UK GDPR. ➢ Automated decision-making declaration added as required under the UK GDPR. ➢ Additional information, including charge, response times and legal capacity of a child to give consent, to the subject access request section. ➢ Details of how to request access changed to recognise that a request can be made in any form but to guide the requester to make it in writing. ➢ Additional rights added and title changed to additional rights of a data subject to meet UK GDPR. ➢ Contact details of the Data Protection Officer added to allow the exercising of the additional rights. ➢ School details updated with correct school name.	

Document reviewed:	Actions/Observations:	Onward Actions:
Privacy Notice for Governors	Version updated to version 3. Audit completed to the GDPR Article 13 requirements and included in the compliance review folder as a separate document. ➢ Confirmation of College Town Primary as the Data Controller added. ➢ Contact details of the Data Protection Officer added to allow the exercising of the additional rights. ➢ Change of purpose declaration added as required under UK GDPR. ➢ Lawful basis information updated to the latest data protection laws. ➢ Added staff training information to create perception of processing within the school. ➢ International data transfers added as required under the UK GDPR. ➢ Automated decision-making declaration added as required under the UK GDPR. ➢ Additional information, including charge, response times and legal capacity of a child to give consent, to the subject access request section. ➢ Details of how to request access changed to recognise that a request can be made in any form but to guide the requester to make it in writing. ➢ Additional rights added and title changed to additional rights of a data subject to meet UK GDPR.	Review the Article 13 review document and consider the amendments or additions proposed. Add further detail to international transfers if available. Review and add details of any legitimate interests of the school. Discuss and review if Consent will ever be used for processing of Governor's information such as photos/images etc. on school prospectus or social media accounts.

Document reviewed:	Actions/Observations:	Onward Actions:
Privacy Notice for School Workforce	Version updated to version 3. Audit completed to the GDPR Article 13 requirements and included in the compliance review folder as a separate document. ➢ Confirmation of College Town Primary as the Data Controller added. ➢ Contact details of the Data Protection Officer added to allow the exercising of the additional rights. ➢ Change of purpose declaration added as required under UK GDPR. ➢ Lawful basis information updated to the latest data protection laws. ➢ Data Protection Act Schedule 1 conditions of processing added. ➢ Added staff training information to create perception of processing within the school. ➢ International data transfers added as required under the Data Protection Act 2018. ➢ Automated decision-making declaration added as required under the UK GDPR. ➢ Additional information, including charge, response times and legal capacity of a child to give consent, to the subject access request section. ➢ Details of how to request access changed to recognise that a request can be made in any form but to guide the requester to make it in writing.	Review the Article 13 review document and consider the amendments or additions proposed. Add further detail to international transfers if available. Review and add details of any legitimate interests of the school. Discuss and review if Consent will ever be used for processing of school staff such as photos/images etc. on school prospectus or social media accounts. Review and add to the 3rd Party software list for HR functions, Payroll, training etc.

Appendix 4 - Article 30 Compliance Review Grid for processing activities as a Data Controller

Article 30(1) of the UK GDPR is very prescriptive on what must be documented within a Record of Processing Activity (RoPA) for personal data collected and processed as a Data Controller.

Article 30(1) states that: "*Each Controller, and where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility…".*

The following grid provides a observations and recommended actions on the Record of Processing Activity under review.

Please note: The review will only comment on the presence of the required elements and will not comment on the lawful basis or additional conditions used by the organisation.

School Name:	**College Town Primary School**
Date of Review:	**17/05/2021**

The following colours are used for ease of reference and action:

	Not applicable – no further action required.
	Compliant: Legally required and present – no further action required.
	Compliant or Partially compliant but review recommended: Either legally required and partially fulfilled or recommended and not present – review recommended and documented in the organisations compliance records.
	Non-Compliant: Legally required and but not present – Immediate action required.

Mandatory information		
Information required:	Present: Yes/No/NA	Notes/Recommendations:
Art.30(1)(a) …the name and contact details of the controller;	Yes	
Art.30(1)(a) …the name and contact details of the controller's representative/s (if applicable);	N/A	Not applicable as the organisation does not provide services or carry out profiling of any residents in the European Union or any other country or territory requiring a representative under either the UK GDPR or EU GDPR.
Art.30(1)(a) …the name and contact details of any joint controller's (if applicable);	To be established	Not present however yet to be established with the organisation if applicable. Action set for next termly update meeting.

Art.30(1)(a) …the name and contact details of the data protection officer (if applicable);	Yes	
Art.30(1)(b) …the purpose of processing;	Yes	
Art.30(1)(c) …a description of the categories of data subjects;	No	Information such as Staff, Ex Staff, Pupils, Parents etc is not currently recorded within the Data Audit Log. Recommend a column titled "Categories of Data Subject" is added to fulfil Art30(1)(c).
Art.30(1)(c) …a description of the categories of personal data;	Yes	The categories of personal data are included in the column "**Data Label**" however I would strongly advise the title is changed to "**Categories of personal data**" to aid reference and external review.
Art.30(1)(d) …the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;	Yes	The categories of recipients are included in the column "**Who do we share data with**" however I would strongly advise the title is changed to "**Categories of recipients**" to aid reference and external review.
Art.30(1)(e) …where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country and the suitable safeguards;	To be established	Not present however yet to be established with the organisation if applicable. Action set for next termly update meeting to discuss data transfer audits completed by the organisation.
Art.30(1)(f) …where possible, the envisaged time limits for erasure of the different categories of data; Reference to the organisations control policy, sector specific or statutory guidance is acceptable.	Yes	The column "**How long is a data item kept /used for**" contains the elements required under Art30(1)(f). Note: Article 30(1)(f) does allow reference to an organisations data retention policy or statutory guidance if applicable. This can be useful if there are possible conditions on retention such as the current **moratorium on the destruction of child safeguarding records**.

Art.30(1)(g) …where possible, a general description of the technical and organisational security measures referred to in Article 32(1);	Yes	The column "where is the data kept" contains the information on security which would technically Art 30(1)(g) however the ICO may determine the current content is brief as it does not reference the security used for **website/cloud** storage i.e., encryption, dedicated user accounts, etc. or the security used for data transfers either internally or externally i.e., encrypted email, internal post, recorded mail etc. The combination of location and security measures in this column maybe confusing the inputter. Possibly consider separate columns to contain **location**, **transfer method** and **security measures** used.
Additional information		
There are several other provisions in the UK GDPR and in the Data Protection Act 2018 (DPA 2018) where documentation is necessary, especially when you are a controller for the personal data being processed. While it is not always a requirement that such information is recorded alongside (or linked from) the record of your processing activities, the ICO think that doing so makes good business sense. It can also help you demonstrate your compliance with other aspects of the Regulation.		
Information recommended by the ICO: *Source: ico.org.uk	Present: Yes/No	Notes/Recommendations:
The lawful basis for processing – one of more of the bases laid out in Article 6(1) of the UK GDPR.	Yes	Just for reference: Under the UK GDPR 6(1)(f) **Legitimate interests** is allowable for non-core functions of a public body or authority. For example, some activities may not be explicitly required under law (**legal obligation**) or a required core function of a public body (**Public Interest/ Public Task**) therefore your organisation may need to use another lawful basis. **Legitimate interests** maybe useful for activities such as advertising events at the school, organising a school performance or PTA fund raising event, sharing personal data of a staff member to seek legal advice etc.

The additional conditions for the processing of special categories, or criminal offence personal data. – one of more of the conditions laid out in Article 9 & Article 10 of the UK GDPR.	Yes	The column "**Legal basis for collection B***" does technically contain the information recommended by the ICO to fulfil the requirements of Article 9 and Article 10 of the UK GDPR but I would advise that the title be changed to "Art 9 & Art 10 Additional conditions for processing special category and criminal offence data" for ease of reference and external review.
Special category data or criminal conviction and offence data – in the UK, the DPA 2018 sets out several conditions for the processing of special category or criminal conviction and offence data. If you process special category data under a condition which requires an appropriate policy document, you must document the following information as part of your processing activities:		
The condition for processing you rely on in the DPA2018, as set out in Parts 1-3 of Schedule 1.	No	To provide a good perception of compliance with the ICO it is recommended to review and include if not recorded elsewhere within the organisation's compliance records.
• Whether the personal data is retained and erased in line with the accompanying policy document you must – if not you must detail the reasons why.	No	To provide a good perception of compliance with the ICO it is recommended to review and include if not recorded elsewhere within the organisation's compliance records.
If applicable, the legitimate interests for the processing – these are the interests pursued by the organisation or a third party if processing under the lawful basis Article 6(1)(f) of the UK GDPR. The ICO also recommends a link to the legitimate interest assessment.	N/A	Not currently applicable as the organisation does not currently process information under the Legitimate interest's lawful basis. Will only be required if the organisation decides to use the Legitimate interest lawful basis and it is not recorded elsewhere within the organisation's compliance records.
If using Article 6(1)(a) Consent, the link to the source of the consent. i.e., Form, website portal or script used in a telephone call.	Yes	The column "**If Consent where is the record of consent stored?**" contains the information required, however for best perception, it is advised to link to the location if possible.

The rights of the individuals regarding the processing. e.g., access, rectification, erasure, restriction, data portability, and objection. The rights vary depending on the lawful basis for processing. Your documentation can reflect these differences.	No	To provide a good perception of compliance with the ICO it is recommended to review and include if not recorded elsewhere within the organisation's compliance records.
If applicable, the existence of automated decision-making, including profiling. In certain circumstances you will need to tell people about the logic involved and the envisaged consequences.	No	To provide a good perception of compliance with the ICO it is recommended to review and include if not recorded elsewhere within the organisation's compliance records.
If applicable, the source of the personal data. This is relevant when you do did not obtain the personal data directly from an individual. This will also determine which type of privacy notice is required i.e., Article 13 (direct form the data subject) or Article 14 (a source other than the data subject).	No	To provide a good perception of compliance with the ICO it is recommended to review and include if not recorded elsewhere within the organisation's compliance records.
Details of processor/s and a link to their contract or written instruction. if a controller uses a processor to carry out a particular processing activity, a written contract or other legal act must be in place. Both controllers and processors can use their record of processing activities to link to the relevant contract documents.	No	To provide a good perception of compliance with the ICO it is recommended to review and include if not recorded elsewhere within the organisation's compliance records.
The format and location of personal data. recording where personal data is stored will help you locate information more easily when an individual exercises the right of access to their personal data (e.g., manual records held in HR file, electronic records held on cloud server, electronic records held by data processor).	No	To provide a good perception of compliance with the ICO it is recommended to review and include if not recorded elsewhere within the organisation's compliance records.

Indication of, and link to, completed Data Protection Impact Assessments (DPIAs) Your organisation must carry out a DPIA when what you are doing with personal data is likely to result in a high risk to individuals' rights and freedoms, particularly when new technologies are involved. You can use your record of processing activities to help flag when a DPIA is required, to keep a track of its progress, and to link to the completed report.	No	To provide a good perception of compliance with the ICO it is recommended to review and include if not recorded elsewhere within the organisation's compliance records.
Indication of data breach incidents, and a link to completed Personal data breach reports, if not recorded elsewhere within your compliance records. One of the requirements regarding personal data breaches is that they must be documented. It is up to you to decide how to do this, but we think it is useful to mark any breaches against your record of processing activities, while also linking to the full breach documentation. This can help you monitor which processing activities the breaches relate to and identify any patterns or potential areas of concern.	No	To provide a good perception of compliance with the ICO it is recommended to review and include if not recorded elsewhere within the organisation's compliance records.
Review completed by:	Data Rose CIPP/E of DHR Consultancy School Data Protection Officer	

Appendix 5 – College Town Primary ISMS Self Audit

Stage:	Description:	Target Date:	Notes/Resources:	Evidence:
1	**Consider an accreditation scheme for your organisation:** Cyber essentials is a self-certified scheme created by the National Cyber Security Centre department of the Government Communications Head Quarter (GCHQ). An additional element (Cyber Essentials Plus) is available which includes an external audit. ISO 27001 is an in-depth certification for organisations providing hosted services as a product or an organisation using a large amount of hosted or critical services within their IT.	Complete	Due to the size and setting of the school there are no current requirements for any specific accreditation. The school is considering the cyber essentials accreditation but is awaiting adequate funds and resources which have been impacted by the recent pandemic. The school will review the accreditation from April 2022 but in the meantime, they will follow the principles of security and utilise the free resources and guidance provided on the **NCSC.gov.uk** and the **ico.org.uk** websites.	
2	**Review if you need to appoint a Chief Information Security Officer (CISO):** A **chief information security officer** (**CISO**) is the senior-level manager responsible for establishing and maintaining the organisational vision, strategy, and program to ensure information assets and technologies are adequately protected	Complete	Due to the size of the setting the school has delegated the role of ensuring the security of the school information assets and technologies between the School IT co-ordinator and the curriculum managed services engineer designated to the school by the managed service provider.	Include the description of the role of the school IT Co-ordinator and the section from the Curriculum support providers SLA detailing the responsibilities of the assigned curriculum engineer.

Stage:	Description:	Target Date:	Notes/Resources:	Evidence:
3	**Create a risk management regime.** Embed an appropriate risk management regime across the organisation. This should be supported by an empowered governance structure, which is actively supported by the board and senior managers. Clearly communicate your approach to risk management with the development of applicable policies and practices. These should aim to ensure that all employees, contractors and suppliers are aware of the approach, how decisions are made, and any applicable risk boundaries.	Complete	The school has adapted materials provided by the local authority, the National Cyber Security Centre and the Information Commissioners Office to create a number of materials to identify, raise awareness and reduce data processing risks within the school including: • Data Protection Impact Assessment Policy • Data Security & Breach Management Policy • E-Safety and Data Security Policy • Data Security Framework • Staff Do's & Don'ts Handouts • Preventing Common Mistakes training video for SLT members • Avoiding Common Mistakes in Processing training video for all staff. • The impact of insufficient Technical & Organisational measures training video for all staff. • Secure handling of SEND training video for all staff in a SEND role or with SEND responsibilities.	[add links to the policies and videos listed once saved to your school network].
4	**Secure configuration** Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.	Ongoing	Evidence could be sourced from your curriculum or admin support providers of evidence such as server or workstation build sheets etc. **Possibly consider how you:** • control image creation and builds including control documents and records; and • control/plan remedial fix's and patch deployment. **Other resources:** https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/secure-configuration	

Stage:	Description:	Target Date:	Notes/Resources:	Evidence:
5	**Network security** By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation). Your organisation's networks almost certainly span many sites and the use of mobile or remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.	Complete	The school has adapted materials provided by the local authority, the National Cyber Security Centre and the Information Commissioners Office to create a number of materials to raise awareness of password security, clear desk clear screen and working remotely including: • E-Safety and Data Security Policy • Data Security Framework • Staff Do's & Don'ts Handouts • Preventing Common Mistakes training video for SLT members • Avoiding Common Mistakes in Processing training video for all staff. • The impact of insufficient Technical & Organisational measures training video for all staff.	[add links to the policies and videos listed once saved to your school network].
6	**Managing user privileges** If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as 'least privilege'.	Ongoing	Evidence could be sourced from your curriculum or admin support providers of evidence such as user creation sheets, permission review logs etc. **Possibly consider how you:** • review existing user or group privileges; and • control the creation of new user/group privileges or the limiting of user/group privileges. **Other resources:** https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/managing-user-privileges	

Stage:	Description:	Target Date:	Notes/Resources:	Evidence:
7	**User education and awareness** Users have a critical role to play in their organisation's security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture.	Complete	The school has adapted materials provided by the local authority, the National Cyber Security Centre and the Information Commissioners Office to create a number of materials to raise awareness and promote good practice including: • Staff Do's & Don'ts Handouts • Preventing Common Mistakes training video for SLT members • Avoiding Common Mistakes in Processing training video for all staff. • The impact of insufficient Technical & Organisational measures training video for all staff.	[add links to the policies and videos listed once saved to your school network].
8	**Incident management** All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact. You should identify recognised sources (internal or external) of specialist incident management expertise.	Complete	The school has adapted materials provided by the local authority, the National Cyber Security Centre and the Information Commissioners Office to create a number of materials to create a clear process of managing incidents within the school including: • E-Safety and Data Security Policy • Data Security Framework • Data Security & Breach Management Policy • Risk identification grids	[add links to the policies and videos listed once saved to your school network].

Stage:	Description:	Target Date:	Notes/Resources:	Evidence:
9	**Malware prevention** Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by developing and implementing appropriate anti-malware policies as part of an overall 'defence in depth' approach.	Complete	The school has adapted materials provided by the local authority, the National Cyber Security Centre and the Information Commissioners Office to create a number of materials to address possible scenarios where malware could enter into the schools' network such as phishing attacks, unprotected or out of date software etc. including: • E-Safety and Data Security Policy • Data Security Framework • Avoiding Common Mistakes in Processing training video for all staff. • Preventing Common Mistakes training video for SLT members	[add links to the policies and videos listed once saved to your school network].
10	**Monitoring** System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.	Ongoing	Evidence could be sourced from your curriculum or admin support providers of evidence such as real time monitoring with alert emails etc. **Possibly consider how you:** • monitor all systems, network traffic and user activity. **Other resources:** https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/monitoring	

Stage:	Description:	Target Date:	Notes/Resources:	Evidence:
11	**Removable media controls** Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.	Ongoing	Evidence could be sourced from your curriculum or admin support providers of evidence such as server group policy or anti-virus endpoint configuration to control removeable media. **Possibly consider how you:** • control/restrict the use of removeable media – endpoint security etc; • assess the appropriate use of removeable media; and • encrypt removable media containing sensitive or confidential information. **Other resources:** https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/removable-media-controls	
12	**Home and mobile working** Mobile working and remote system access offers great benefits, but exposes new risks that need to be managed. You should establish risk-based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers. Train users on the secure use of their mobile devices in the environments they are likely to be working in.	Complete	The school has adapted materials provided by the local authority, the National Cyber Security Centre and the Information Commissioners Office to create a number of materials to raise awareness, set expected standards and reduce data processing risks when working remotely from the school, including: • E-Safety and Data Security Policy • Data Security Framework • Staff Do's & Don'ts Handouts • Preventing Common Mistakes training video for SLT members • Avoiding Common Mistakes in Processing training video for all staff.	[add links to the policies and videos listed once saved to your school network].